

UNIVERSITY OF CALIFORNIA

Los Angeles

The Ethics of Social Media Policy:
National Principles of Justice, Security, Privacy and Freedom Governing Online Social
Platforms in Russia, China and The United States

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy
in Information Studies

by

Morten Bay Christensen

2018

© Copyright by

Morten Bay Christensen

2018

ABSTRACT OF THE DISSERTATION

The Ethics of Social Media Policy:
National Principles of Justice, Security, Privacy and Freedom Governing Online Social
Platforms on Russia, China and The United States

by

Morten Bay Christensen
Doctor of Philosophy in Information Studies
University of California, Los Angeles, 2018
Professor Leah A Lievrouw, Chair

As social media have become a primary mode of expression and communication for large parts of the world's population, social media platforms have also become vulnerable to less desirable actions. These include using social media for information warfare, recruiting and radicalizing potential terrorists or collecting data and information about users for purposes they have not consented to. The demand for an ethical discussion of social media policy at the national level is growing, and this study seeks to address that challenge. The study is an exploration of applied ethics in the context of information and technology policy. It addresses issues in information, media and technology ethics, applying a specific ethical theory to three cases. These three cases consist of Russian, Chinese and U.S. policies that relate to social media in a national information security or cybersecurity context, and which exist within the information and technology policy

categories. Each of these three cases represent a specific type of social media policy. The Russia case is an offensive social media strategy within foreign policy, the China case is a broad, domestic social media policy and the U.S. policy is a very narrow social media policy within the larger, national security domain that has substantial consequences for privacy and freedom rights nonetheless. First, the case policies are analyzed through Schön and Rein's frame-critical policy analysis method, which deconstructs the policy and adds to it the historical and cultural backgrounds that lends a broader perspective to the policy, and thereby, a more thorough understanding of its intended purpose and expected outcomes. Second, the now much more broadly unfolded policies are analyzed through the lens of political philosopher John Rawls' theories of justice and fairness to ascertain their compliance with Rawls' deontological ethics. Through this applied exercise, the validity of Rawlsian deontology as an ethical compass for information and technology policy is established. The findings are finally crystallized into an ethics test, The Rawls Test for social media policy.

The dissertation of Morten Bay Christensen is approved.

Jean-François Blanchette

Jonathan Furner

John D. Villasenor

Leah A Lievrouw, Committee Chair

University of California, Los Angeles

2018

Table of Contents

Table of Contentsv

List of figures viii

List of appendices..... viii

Glossary of terms ix

Abbreviations xiii

Acknowledgementsxvi

Biography and publication highlightsxix

Chapter 1: Introduction 1

 Research design..... 14

 Method of policy analysis..... 16

 Data collection22

 Chapter overview and summary of findings24

Chapter 2: Social media ethics and an introduction to John Rawls31

 Five categories that critique social media ethics.....31

 Meet John Rawls37

 The works of John Rawls39

 Rawlsian concepts and their inspiration40

 Rawls’ critics.....59

 Rawls in information and technology literature.....65

Chapter 3: Disinformation campaigns on social media	69
Background	69
Rhetorical Frame	81
Action Frame.....	95
Cultural background	111
Russia’s interventionist information security policy and the Rawlsian Frame.....	123
Chapter conclusion	137
Chapter 4: Policies of Control, Surveillance and Oppression on Social Media	139
Background	139
Rhetorical Frame	161
Action Frame.....	170
Cultural background	197
China’s policy frames and the Rawlsian Frame.....	214
Chapter 5: Violations of privacy rights on social media in the name of national security	235
Background	237
Rhetorical Frame	268
Action Frame.....	280
Cultural background	301
The DHS and the Rawlsian Frame	327
Chapter conclusion	352

Chapter 6: The Rawls Test – Discussion and Conclusion.....	355
Summary of findings and responses to research questions	355
Developing a Rawlsian ethics test for social media policy	365
Into the future.....	390
Appendix A: List of Interviewees with biographies	396
Esha Bhandari	396
Susanne Chan.....	396
Dr. Yubo Kou.....	397
Dr. Martin Libicki	397
Henrik Moltke	398
Dr. Margaret E. Roberts.....	399
The Hon. Adam Schiff.....	399
Dr. Margo Schlanger	400
Dr. Rebecca Slayton	400
Bibliography	402

List of figures

Figure 1: One of the Facebook ads presented during the October 31 – November 1, 2017 congressional hearings.....	103
Figure 2: Three tweets from Russian trolls.....	106
Figure 3: The international, submarine telecommunications cable landings in China in February 2018.....	146
Figure 4. Registered number of illegal or inappropriate behavior to the CAC.....	184

List of appendices

Appendix A: List of Interviewees with Biographies.....	398
---	-----

Glossary of terms

Active Measures: A tactic developed by the KGB during the Soviet era in which actions are taken to manipulate beliefs and attitudes, often through disinformation tactics, with the purpose of achieving strategic advantages. Known as “aktivnyye meropriyatiya” in Russian.

Applied Ethics: The application of ethical theories to real-world areas of practice. Examples include business ethics, marketing ethics, medical ethics or, as in the case of this dissertation information ethics and technology ethics.

Confucianism: A belief system based on the writings of the Chinese philosopher and scholar popularly known as Confucius. His teachings include a system of virtue ethics, writings on art and poetry as well as practical life guidelines.

Consequentialism: A form of ethics that evaluate actions, policies or laws based on their expected consequences or outcomes, often judging by the probability of those consequences or outcomes.

Contractarianism: The idea of letting an (most often imaginary) social contract between citizen and citizen, as well as between government and citizen, determine the rights and responsibilities of all the parties to the contract. The terms of the social contract are agreed to by all parties willingly and without regard to prior positions and sets the norms for the social cooperation that the parties commit to uphold by participating.

Communitarianism: A morality approach that prioritizes community over the individual from an ethical standpoint. The most recent communitarian theories emerged as a reaction to the resurgence of deontology and contractarianism led by John Rawls in the 1970s, as neo-

communitarians did not believe the latter theories adequately addressed the human need for community and social interaction.

Disinformation: Typically, misleading information seeded into communication channels for political or strategic purposes. Perfected as counter-intelligence tool by the KGB under the term “dezinformatsiya”.

Ethics: The philosophy of morality. The term is often used to indicate a set of moral theories or theories of morality set within a certain domain.

Information Ethics: Ethics that focus on how the creation, collection, organization, classification, distribution, use and processing of information relates to questions of moral conduct in social groups and society as a whole.

Information Policy: The umbrella term for the practice and/or study of making, implementing and adhering to policies that govern or guide the creation, collection, organization, classification, distribution, use and processing of information.

Lawful Permanent Resident: In the U.S., a person who resides legally in the United States without any limits to the length of their stay but is not a U.S. citizen. Also known as a “Green Card Holder”.

Misinformation: Wrongful or misleading information that is not necessarily communicated with the intent to mislead.

Morality: A code or heuristic for the “good” or doing what is “right” that may emerge from reasoning or from societal or religious norms.

National Security: Protecting a nation from attack or other dangers, (here understood as also including internal or domestic threats to the entire nation) by keeping armed forces and guarding state secrets.

Naturalization: In the U.S., the process of becoming a citizen of the United States.

Paternalism: The policy or practice on the part of people in positions of authority of restricting the freedom and responsibilities of those subordinate to them in the subordinates' supposed best interest.

Policy: A course or principle of action adopted or proposed by a government, party, business, or individual.

Social Media: A collective term for typically digital media forms that enable social networking, content sharing, peer-to-peer- as well as broadcast-type communications, use of rich media and the ability construction of an alternate identity (or avatar), most often using the Internet of mobile networks.

Technology ethics: Ethical theories concerned with the morality of distribution, use and social impact of technology in society.

Deontological Ethics: A category of ethical theory which prioritizes rules such as laws or norms over expected consequences of an action, law or policy, calling on the duty or obligation of citizens to adhere to those rules in order to act morally. Thus, deontological ethics are often referred to as “duty-based” ethics.

U.S. Person: A person, corporation, estate or organization with legal right to residence in the United States.

Utilitarianism: A consequentialist form of ethics originally based on conceptions of pleasure and pain. The whether an action, law or policy is right or wrong is contingent on whether it maximizes or minimizes pleasure or pain. Later, utilitarianism took on a more tangible form, where actions, laws or policies were judged by how many beings (for some thinkers, only humans) would benefit or suffer from the consequences.

Virtue ethics: Normative ethical theories that emphasize virtues of the person and the mind as determinants of the “good”.

Abbreviations

ACLU = American Civil Liberties Union

CAC = Cyberspace Administration of China

CBP = Customs and Border Patrol

CLAIMS = Computer - Linked Application Information Management System

CLGSI = Central Leading Group for Internet Security and Informatization (China)

CLGPIW = Central Leading Group for Propaganda and Ideological Work (China)

CNCERT/CC = China National Computer Emergency Response Team & Coordination Center

CNCI = Comprehensive National Cybersecurity Initiative

CPC = Communist Party of China

DHS = Department of Homeland Security

DNI = Director of National Intelligence

DPI = Deep Packet Inspection

DOD = Department of Defense

DOJ = Department of Justice

DNS = Domain Name System

ECHR = European Convention on Human Rights

EFF = Electronic Frontier Foundation

EPIC = Electronic Privacy Information Center

EO = (Presidential) Executive Order

FDNS-DS = Fraud Detection and National Security Data System

FEMA = Federal Emergency Management Agency

FISA = Foreign Intelligence Surveillance Act

FISC = Foreign Intelligence Surveillance Court

FSB = Federal Security Bureau (Russia)

FOIA = Freedom of Information Act

GCHQ = Government Communication Headquarters (United Kingdom)

I2F = Intelligence and Information Fusion

IC = Intelligence Community

ICA = Intelligence Community Assessment

ICE = Immigration and Customs Enforcement

INA = Immigration and Naturalization Act

ISP = Internet Service Provider

IP = Internet Protocol

KGB = Komitet Gosudarstvennoy Bezopasnost – former Soviet intelligence service

MAU = Monthly Active Users

MGT = Modernizing Government Technology Act

MIIT = Ministry of Industry and Information Technology (China)

NDAA = National Defense Authorization Act

NSL = National Security Letter

NSA = National Security Agency

NIISO = National Immigration Information Sharing Office

LP = *The Law of Peoples* by John Rawls

OP = Original Position

Patriot Act = U.S.A. PATRIOT Act of 2001

PII = Personally Identifiable Information

RT = Russia Today

SAPPRFT = State Administration of Press, Publication, Radio, Film and Television (China)

SIIO = State Internet Information Office (China)

SIGINT = Signals Intelligence

STOA = Science and Technology Office of Assessment (European Union)

TCP = Transport Control Protocol

TSA = Transportation Security Administration

TSP = Terrorist Surveillance Program

URL = Uniform Resource Locator

USCIS = United States Customs and Immigration Service

US-CERT = United States Computer Emergency Readiness Team

VPN = Virtual Private Network

Acknowledgements

There are many people without whom this dissertation would never have been possible, and even more who undeservingly suffered my distraction as well as physical and mental absence while I have undertaken this endeavor. To all of them, I am eternally grateful.

First and foremost, I must thank Kirsten Mogensen, who personally, and by inviting me to participate in an academic conference at Stanford University in 2010, gave me the confidence that I was even qualified enough to pursue a Ph.D. Thanks also to Mette Høybye for similar encouragement. The further encouragement I received from Henrik Søndergaard and Martin Høybye during that time was also invaluable in convincing me that I could achieve this goal.

Very warm thanks go to all the interviewees who were kind enough to share their knowledge and time so generously for this dissertation. During my time at UCLA, I have received invaluable inspiration, encouragement and support from many Ph.D. colleagues at the Department of Information Studies, and I would in particular like to thank: Dr. Kathy Carbone, Natascha Chtena, Dr. Marika Cifor, Kristin Cornelius, Dr. Roderic Crooks, Dr. Morgan Currie, Seth Erickson, Dr. Pat Garcia, Randy Illum, Dustin O'Hara, Britt Paris, Bernie Randles, Dr. Rob Montoya, Dr. Stacy Woods, for being amazing, fun and most of all inspiring and admirable colleagues whose work has served as aspirational motivation for me. Among my colleagues, special thanks go to Dr. Diana Ascher for invaluable support, particularly during the first part of this journey, Dr. Amelia Acker for convincing me that the Information Studies Department at UCLA was the right place for me, and to Dr. Colin Doty, Irene Pasquetto and Jennifer Pierre for great collaborations over the years – and for being around during one emergency incident in particular, for which I also owe Andrew Vanschooneveld and Dr. Safiya Noble a great debt. I

also want to thank Dr. Noble for influencing my thinking in a very positive way during her time at the department.

Great thanks also go to Dr. Bradley Fidler and Dr. Andrew Schrock, whose friendships and academic advice played a big part in getting me through to the end. The same goes for Dr. Leonard Kleinrock and Dr. Michael Suman of the Computer Science and Communication Studies departments who have been supportive in more ways than one over the years. When it comes to support, I must also thank Susan Abler, Michelle Maye, Jane Bitar and Pia Svenson, those student affairs and department managers at the Information Studies and Communication Studies departments without whom I would never have understood how to navigate the American university system. I also owe quite a big thanks to Dr. Amy Mulherin for helping me through the process mentally.

I also wish to thank the entire faculty at the Department of Information Studies at UCLA for being so inspirational, helpful and approachable and fun (Yes, I'm looking at you, Doctors Leazer, Becker and Posner). Special thanks go to Michelle Caswell for putting me on the path to the RAND summer associate program where I found the inspiration for this dissertation (I also owe Dr. Isaac Porche III of the RAND Corporation a huge thanks for that). From the faculty, I am particularly indebted to Dr. Ramesh Srinivasan and Dr. Christine Borgman, not only for early meetings that convinced me that the program was for me, but for their continued support through all six years I was in it. Dr. Johanna Drucker literally changed my life and brought me back from the philosophical abyss of over-rational data-driven determinism by introducing me to new materialisms and systems theory, and I cannot thank her enough for that. During the later years,

Dr. Sarah Roberts has been an incredible inspiration and motivator for me, and I want to thank her wholeheartedly for being the kind of academic I aspire to be.

I must convey an even deeper gratitude to the members of my doctoral committee whose spirited advice has been crucial to my process, but also for their own work: Dr. Jean-François Blanchette for making me think about the materiality of bits, Dr. Jonathan Furner for showing me the intersection between philosophy, information and media studies and Dr. John Villasenor whose work connected all of the above with the real world of technology that I have spent so much time in professionally.

But more than any faculty member, I must convey my deepest, sincerest gratitude and thanks to Dr. Leah Lievrouw for being my advisor for six years and sticking with me during my crazier moments. Dr. Lievrouw's kindness and friendship has been as essential to the completion of this project as her advice. There have some been very difficult times during my time as a Ph.D. student and had it not been for Dr. Lievrouw, I would likely have given up somewhere along the way. I owe the completion of this dissertation to her.

Finally, big thanks from the bottom of my heart to those close friends and family members who I have neglected for six years while pursuing this quest: Kim, Dana, Kayla and Martin, Lara and Claus, Christy and Thomas, Kaela and Jeppe, Michelle, Sarah, Anne Mette and Lars, Christian and Stine, Lotte and Lars, Elizabeth and René, Helen and Dad, and the rest of my friends and family members in the U.S., Scotland, Sweden and Denmark.

Biography and publication highlights

Morten Bay is a Danish-American award-winning technology scholar, writer and consultant. He is expected to receive a Ph.D. degree from UCLA in June 2018.

Bay has spent the last two decades researching emerging technologies and their impact on Western societies from both commercial and academic viewpoints. His current research focuses on the ethics of social media and how technology impacts democracy, social justice and the economy overall.

His pre-UCLA research spawned five books published in his native Denmark, one of which, 'Generation Network', earned him the Future Award from the Danish Academy of Strategic Foresight. He has also received awards from UCLA, Stanford University and the Society for the History of Technology. His most popular book, 'Homo Conexus', was translated into English and released internationally in 2012. Alongside his research, Morten Bay has worked as a journalist, writing feature articles and op-eds for American media outlets such as Slate, Vice and U.S. News & World Report. He covers technology and U.S. politics for major Danish media outlets, including Denmark's biggest news organization, Politiken. He appears regularly as an expert on both technology-related and U.S. political affairs in European media.

Bay, who relocated permanently to California in 2008, is also in high demand as a strategic consultant and a public speaker. His long client list includes tech giants such as Microsoft, Apple, Oracle and eBay as well as media and communications companies including NBC, PBS, Saatchi and Saatchi, MTG, Time/Warner and the national broadcasters in Sweden, Norway and Denmark.

He has also been involved in several European technology startups, among them the continent's first legal music download service in 2000. Bay also created Europe's first music download service for smartphones in 2004, three years before the iPhone was released, and pioneered online recommendation engines on the continent by creating the first of its kind based on micro-segmentation in 2005.

As a policy consultant on technology and emerging media platforms, Bay has advised agencies under the Department of Health and Human Services as well as the U.S. Army and DARPA under the Department of Defense. In Europe, he has done policy work with the parties in the European and Danish parliaments.

Peer-reviewed Publications

Bay, M. (2018) The Ethics of Psychometrics in Social Media: A Rawlsian Approach. In Proceedings of the 51st Hawaii International Conference on System Sciences.

Bay, M. (2017) Rawls on Privacy – social cooperation in the presence of unbreakable encryption. First Monday. February.

Bay, M. (2017) What is “Internet?” The case for the proper noun and why it's important Internet Histories, August 2017.

Bay, M. (2017) Conversations with a Pioneer: Paul Baran in His Own Words. Internet Histories, August 2017

Bay, M. (2016) What is Cybersecurity? In search of an encompassing definition for the post-Snowden era. French Journal of Media Research, 6/2016. Paris.

Bay, M. (2010) Who Are the Tech Press Darlings? An Empirical Study of Coverage of Innovation-Driven Tech Companies in US Newspapers. Innovation Journalism. Vol. 7 no. 7. November.

Chapter 1: Introduction

If ethics and policy-making were Facebook users, their relationship status would be set to “It’s complicated”. In the traditional understanding of the term, ethics are what we use to contain the effects of any institutional policy, the frame that keeps the policy from having an impact in places where it shouldn’t. We may have rational, economic arguments for a given policy. We may have political motivations. We may have the best bricks in the world to build our policy house from. But any corporate, organizational, public or political policy will always have boundaries, it cannot be all-encompassing. And that’s where ethics come in. Yes, sometimes the boundaries are set by budgets or the weather or resource availability. But none of those elements are infinite. Choices must be made, options must be prioritized because of the limitations of those policy components. These choices will always be done according to some kind of ethical rule set. Even if we choose not to apply ethics to a policy process, we have made an ethical choice. Even if our ethical choice emerges from a lack of deliberation and reason and is completely irrational, even if we decide to act according to instinct and rationalize it post-hoc, the process is still an expression of a certain set of ethics, materialized through action rather than through intentional reasoning. On an institutional level you can read any policy brief and find a similar expression of the ethics behind it, which may again reveal a multitude of information about the cultural characteristics, history and mindset of the society in which the policy brief embarks on its inevitable mission of making an impact, whether insignificant or massive.

The relationship between ethics and policy-making is particularly close, but also complex, when it comes to information. As information and the technology that enables it has become

intrinsic to society in both a financial, social and political sense, information policy and information ethics now concerns everyone. These two areas of study are now at the center of how democracies function, how wars are fought, how citizens express themselves and how their rights are upheld. Information policy, and its frame of information ethics impact how we work, how we define quality of life and how we create our own identities. At the highest level of abstraction, perhaps only environmental and political ethics and are currently as important for our survival as the ethics that inform information and technology – and by extension, the public, organizational or corporate policies we enact in that context.

During the time it took to complete this dissertation and the prior coursework it required, several events gave me first-hand experience of the power and importance of information ethics and the policies that follow them. These experiences motivated me to conduct the study at hand.

When Edward Snowden made his revelations about methods used by the NSA in the summer of 2013, I was one year into the Ph.D. program which has resulted in this dissertation. While others were shocked over what Snowden revealed, I was shocked that others were shocked. Government surveillance of every form of electronic communications has happened ever since they were invented, and several whistleblowers before Snowden had come forth with tangible evidence of surveillance systems similar to those Snowden made public. Only very few technical abilities and the names had been changed. The Patriot Act was 11 years old, and the American people had gone through six elections since its passing in which they could have voted out the presidents, senators and representatives who supported it. They did not. Furthermore, Internet users worldwide had now been sharing many of the same data they were worried about

government agencies collecting with strangers and private companies via their social media profiles and registered memberships of streaming services, e-commerce sites and e-mail services.

These services, along with information technology companies following the Big Data trend emerging at the time, would even brag in their marketing about their abilities to use this data to give the consumer more convenient user experiences. It was not as if the notion of personal data being collected and used all over the place was a secret, if you were paying just a modicum of attention. But the summer of 2013 was a slow one, news-wise. President Obama had been re-inaugurated as president and was continuing to rebuild the economy in the U.S. while facing staunch opposition from the Republican-led Congress, but things were generally chugging along in a somewhat normal fashion that summer. Until the Snowden story hit and took over all the headlines. And all of a sudden, everyone was a critic of government data collection methods. The debate that followed the Snowden revelations was frustrating to me, as it reflected the growing division in the U.S.: On one side, you had those who would insist on the right to privacy as an absolute that covered all data and information attributable to the person, and who did not think that government agencies, particularly those involved in law enforcement and national security, had any business collecting data on U.S. persons. On the other side, some voices would claim that without data collected for national security and law enforcement purposes, society as we know it would dissolve into chaos, and the U.S. would be taken over by foreign powers before we knew it. (It is important to note that I use the term “national security” in this dissertation as not simply meaning protection against external threats to the nation, but also internal threats, i.e. the individual being protected against implications of violent insurgencies or

military coups etc. A previous paper included a more in-depth discussion of how the term “security” can be viewed in the light of a new era of cyberwarfare.¹⁾

My frustration over the divisiveness and lack of reasonable discourse in the debate led to this dissertation. In its essence, the public debate following Snowden’s revelations was a re-hashing of an old one: Balancing personal liberty with the interests of the nation. Philosophers have struggled with this at least since Plato wrote *The Republic* around 360 BC.² Yet, perhaps it really was time to take up that debate again, considering that the modern world was perceived as being in transition from industrial to information society, and that the production of data, even by the individual, was growing at a phenomenal rate. The latter was particularly the case because of the emergence and popularity of social media platforms for communication.

To me, the ongoing debate at the time had become toxic because of the Snowden revelations, and the divisiveness was making any common ground that could lead to reasonable policies infertile. Thus, the motivation for the study described in this dissertation was to create a framework within which such a debate would become reasonable, productive discourse as a foundation for policy-making. As I wrote earlier, ethics inform policy-making, whether we like it or not. It is almost impossible to come to the policy-making process in a purely technocratic way and not bring our values with us to the table. And so, the debate over personal liberty versus national security policies is also an ethical one

¹ Morten Bay, “What Is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era,” *French Journal For Media Research* Special Is, no. 6 (2016): 1–28.

² Plato and Benjamin (trans.) Jowett, “The Republic by Plato,” The Internet Classics Archive |, 2008, <http://classics.mit.edu/Plato/republic.html>.

But policy, particularly public policy, is about bringing the abstract to the concrete. Making real changes in people's lives from otherwise intangible ideals. To make my study useful, I therefore chose to ground it in one area in which the debate over personal liberty versus national security was becoming a factor that was growing in importance: Social media. In the summer of 2015, as I was developing my dissertation proposal, it became clear that social media had been weaponized by terrorist groups such as ISIS and that Russia was commencing an information warfare campaign targeting the U.S., largely based on the same social media platforms. These activities had ramped up since 2014, and the thought occurred to me that the above-mentioned debate would likely turn to social media as both ISIS and Russia progressed in their efforts to weaponize the platforms. Three events following this realization showed that the notion I had in the summer of 2015 had been correct:

First, the San Bernardino terror attack in December 2015 showed how social media could play a role in radicalization of people living in the U.S.³, and how social media-enabling devices such as a smartphone could become a central object of study for law enforcement and national security agencies in this regard. When the FBI asked Apple to break the encryption on an iPhone used by one of the suspected terrorists, Apple refused, leading to a revival of the debate over what kind of power, government agencies should be able to wield over the individual's ability

³ Robert Windrem, "Terror in the Family: When Radicalization Begins at Home," NBC News, 2015, <https://www.nbcnews.com/news/us-news/terror-family-when-radicalization-begins-home-n481816>; Adam Nagourney, Salman Masood, and Michael S. Schmidt, "Killers Were Long Radicalized, F.B.I. Investigators Say," New York Times, 2015, <https://www.nytimes.com/2015/12/08/us/fbi-says-san-bernardino-assailants-were-radicalized.html?mtref=www.google.com>; Marie Wright, "Domestic Terrorism, Cyber-Radicalization, U.S. College Students.," *Forensic Examiner*, 2011, 10–18, <https://issuu.com/acfei.media/docs/fallwinter2011>.

and desires to keep their personal information private through encryption. I have published a study on this matter elsewhere.⁴

The second event was the U.S. presidential election in 2016, and the months preceding it, in which it became very clear to those of us studying Russia's information warfare efforts that they had employed social media tactics in an attempt to influence, and perhaps disrupt and even change the outcome of the election.

The third event was the debate in the aftermath of the election, in which social media platforms would admit to having been blind to the Russian influence campaign and news about methods used by consulting companies such as Cambridge Analytica shocked people in the same manner that the Snowden revelations did. I have also published on the ethicality of these methods elsewhere.⁵ The public seemed particularly shocked over the revelations from February and March 2018 that Facebook's own rules allowed Cambridge Analytica researchers to gather data about more than 50 million Facebook users between 2014 and 2015 by using a network effect from a base of 270,000 users who had given consent for data collection.⁶

While others debated the scandals, joined the public outcry or scrambled to contain any damage done, I decided to step back and take in a grander perspective. From a distance, I saw a

⁴ Morten Bay, "The Ethics of Unbreakable Encryption: Rawlsian Privacy and the San Bernardino iPhone," *First Monday* 22, no. 2 (2017).

⁵ Morten Bay, "The Ethics of Psychometrics in Social Media: A Rawlsian Approach," in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

⁶ Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *The New York Times*, 2018, <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>; Matthew Hindman, "This Is How Cambridge Analytica's Facebook Targeting Model Really Worked — According to the Person Who Built It," *Nieman Lab*, 2018, <http://www.niemanlab.org/2018/03/this-is-how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it/>.

clear need to talk about social media in a larger context. Others are already doing great work on the economic, racial, gender- or sexuality-based inequities that live within the social media realm. I felt that my contribution could be of another sort, at a more philosophical level. I wanted to ask, not “*Why* social media?”, but, accepting that social media now make up a dominant information infrastructure that is critical to how many people experience democracy, work, education and social life, “*How should* social media...?”

Though media ethics is an established discipline, much of its literature does not take into account the crucial, participatory aspects of social media and thus, I felt that a dissertation concerned with social media ethics might be a good contribution to the information ethics literature. But a long literature review and some well-argued ethical theory doth not a dissertation-worthy study make. I therefore decided to conduct a study in which ethics were applied to matters of consequence. And that meant engaging with information policy. Since, as I wrote earlier, information policy is intrinsically linked to information ethics, it seemed natural to study how ethical theory applies to information policies. But, because of the pressing events that happened during the course of my Ph.D. education, it was simply not possible for me to aim low. I had to look at information policies at the national level. Fortunately, this was an area that was reasonably unexplored when it came to social media, so I could likely make a good contribution. Less fortunately for the world, but fortunately enough for my process, the world had served up three national social media policies that were having a substantial impact on international relations and security. Russian operatives had taken information warfare to a new level and weaponized social media in the process. China had implemented new cybersecurity laws that focused on suppressing freedom of speech through actions on social media. And in the U.S.,

national policy changes and a massive increase in certain social media information-gathering activities signaled a shift in strategy that looked more like China than a Western democracy.

With these three cases almost casting themselves in the role of independent variables, I now needed an ethical yardstick to use for sizing them up and finding the dependent variable. Between the two dominant political ethics theories in the post-cold war era, consequentialism and deontology, I chose to focus on the latter. The main reason for this is that consequentialism, and particularly its sub-theory of utilitarianism, is already the preferred choice in national information policy, at least in the West. The world already knows what that looks like. But only a handful of scholars have taken on the task of applying modern contractarianism or deontology to information and technology policy, and even fewer have made that journey at the national level. Thus, it became the overall mission for this study to explore whether a deontological approach might also be viable as an ethical framework to discuss the above-mentioned, pressing issues within. The most important theorist for modern contractarianism and deontology in political philosophy also happens to be perhaps the most influential thinker when it comes to freedom, justice and fairness in the last half century – John Rawls. With their focus on how to construct a fair society, Rawls’ theories - and the criteria embedded within them – seemed perfectly suited as “yardsticks” to compare these national policies to.

But why Rawls? And why now? The choice of John Rawls may seem oddly retrospective or even retrogressive. But it is intended to be the opposite. The entire concept of applied ethics is, after all, based to some degree on the assumption of cognitively active actors, i.e. that those faced with moral decisions are capable of making them by employing anywhere from almost none to all-encompassing amounts of reasoning. As will be discussed further along in this text,

varying ethical theories require different amounts of reasoning in the decision-making situation, but all of them are based on some sort of deliberation which is not chaotic and irrational. Yet, in recent decades, irrationality has been widely acknowledged as part of the human decision-making process. The rise of behavioral economics since the 1980s, and the integration of psychological research into economic science and decision-making theory⁷ has brought forth such compelling arguments for cognitive biases in decision-making that it makes ethical reasoning in a decision-making process seem almost quaint. Add to that the sociological aspect presented by Beck⁸ and Giddens⁹ that structural stressors in society further impede the individual's ability to make purely reason-based decisions, because the structure forces the individual to navigate life through a series of risk-minimizing or -averting decisions. Or the angle coming from communications/media and information studies scholars that both noise as well as technology-enabled filtering simultaneously make it difficult to obtain the information from which reason-based decisions can be made¹⁰ In the communication subfield of persuasion

⁷ Daniel Kahneman, Jack L Knetsch, and Richard H Thaler, "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias," *Journal of Economic Perspectives*, 1991, <https://doi.org/10.1257/jep.5.1.193>; Richard H. Thaler, "Behavioral Economics: Past, Present, and Future," *American Economic Review*, 2016, <https://doi.org/10.1257/aer.106.7.1577>; Cass R. Sunstein, "Nudging: A Very Short Guide," *Journal of Consumer Policy*, 2014, <https://doi.org/10.1007/s10603-014-9273-1>; Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica*, 1979, <https://doi.org/10.2307/1914185>.

⁸ Ulrich Beck, "Risk Society: Towards a New Modernity," *Nation*, 1992, <https://doi.org/10.2307/2579937>.

⁹ Anthony Giddens, "The Consequences of Modernity," *The British Journal of Sociology*, 1991, <https://doi.org/10.2307/591454>.

¹⁰ David Bawden and Lyn Robinson, "The Dark Side of Information: Overload, Anxiety and Other Paradoxes and Pathologies," *Journal of Information Science* 35, no. 2 (2009): 180–91, <https://doi.org/10.1177/0165551508095781>; Miriam J. Metzger and Andrew J. Flanagin, "Credibility and Trust of Information in Online Environments: The Use of Cognitive Heuristics," *Journal of Pragmatics* 59 (2013): 210–20, <https://doi.org/10.1016/j.pragma.2013.07.012>;

theory as well as in political communication, it has been a known factor for decades that individuals rarely change their attitudes immediately because of direct communication, and much less because of reasoning¹¹. When an individual makes a moral decision, it is much more likely to be the result of an ingrained heuristic than of a process of deliberation. Even such a deliberation may have occurred, it is likely to have been impacted by cognitive bias.

However, ethics are not about what we do. They are not about what we *can* do. They are about what we *should* do. Ethics are prescriptive, not descriptive. This doesn't mean that the *norms* in an ethical theory are necessarily prescriptive, and Rawls' work provides a good example of this. He is mostly concerned with securing the fairness and justice of *the process* of creating norms, rather than simply prescribing norms and arguing for them. Rawls' whole theory is based on the thought experiment of the original position, precisely to avoid influence from cognitive biases. His imaginary "veil of ignorance" exists solely as a tool to reduce such biases as much as possible when deciding on how society should be structured. But Rawls never claimed that it was possible to be completely objective and reasonable in decision-making. Furthermore, as can be read below, he emphasized that many of his principles were only implementable at the macro-level. For example, Rawls never intended his Maximin principle to be implemented in personal decision-making and was very emphatic about it in his writing.

Eli Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think* (The Penguin Press, 2011).

¹¹ David Gold et al., "Personal Influence: The Part Played by People in the Flow of Mass Communications.," *American Sociological Review*, 1956, <https://doi.org/10.2307/2088435>; Daniel Katz, "The Functional Approach to the Study of Attitudes," *Public Opinion Quarterly*, 1960, <https://doi.org/10.1086/266945>; William J. McGuire, "Personality and Attitude Change: An Information-Processing Theory," in *Psychological Foundations of Attitudes*, 1968, <https://doi.org/10.1016/B978-1-4832-3071-9.50013-1>.

The present study is an analysis of national policies, which reside at the macro-level where Rawls' theories also belong. The important work on decision-making cited above usually addresses the micro-level, the level of the individual. However, from the point of social psychology, many of the scholars above have also addressed how cognitive biases in decision-making can impact groups such as collectives of voters, and certainly impacts decision- and policy-makers with high levels of influence – they are human after all.

This raises the question: Even though we accept irrationality as part of personal decision-making processes, should we accept them in decisions taken on behalf of society? In the legislative processes? In the enforcement of laws? And if so, how much irrationality will we tolerate? Who gets to set the limits of the irrational in the democratic process? It seems fair to assume that no-one is interested in pervasive, complete and utter irrationality in the democratic process, since that would take away the expectation that a representative you elect will actually represent you in office, it would make political coalitions impossible due to the lack of trust, it would create an unpredictability in the political leadership which impedes the building and maintenance of international alliances and it would create a deep mistrust in law enforcement and public institutions.

At the time of writing, the United States is in fact experiencing all of the above, precisely because the acceptance of irrationality in the democratic process. The election of Donald Trump and the actions and policies he and his administration have subjected the American voters to are

characterized by a high degree of cognitive bias in the voters who elected him¹² (which is partially what Chapter 3 is about), and, according to some, in the president himself.¹³

It seems that Western democracies are at a stage of “peak irrationality”. It is visible in the rise of right-wing nationalism in Europe over the past two-three decades. Considering its not-too-distant past, some observers find it hard to find the logical reasoning why the continent would let such a thing happen.¹⁴ The ‘Brexit’ vote in the United Kingdom is seen by some as an example of the same.¹⁵ And in the United States, there’s President Trump. This dissertation is written in the expectation that once the political pendulum once swings away from this political trend at some point in the coming years, reason will also re-expand its role in democratically deliberative processes. Rawls, being the last century’s strongest voice in one of reason-based schools of thought, deontological contractarianism, may find a new audience. Perhaps this is why there are already signs of a renewed interest in Rawls. Though it should not be viewed as an absolute

¹² Andrew Guess, Brendan Nyhan, and Jason Reifler, “Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 U.S. Presidential Campaign,” 2018, <https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf>; Briony Swire et al., “Processing Political Misinformation—Comprehending the Trump Phenomenon,” *Royal Society Open Science*, 2017, <https://doi.org/10.1098/rsos.160802>.

¹³ Bandi Lee, *The Dangerous Case of Donald Trump: 27 Psychiatrists and Mental Health Experts Assess a President.*, *The Dangerous Case of Donald Trump: 27 Psychiatrists and Mental Health Experts Assess a President.*, 2017; Joyce Ann Mercer, “The Dangerous Case of Donald Trump: A Case Study in Contested Ethics and the Public Uses of Professional Expertise,” *Pastoral Psychology*, 2018, <https://doi.org/10.1007/s11089-018-0810-8>.

¹⁴ Marcel Lubbers and Marcel Coenders, “Nationalistic Attitudes and Voting for the Radical Right in Europe,” *European Union Politics* 18, no. 1 (2017): 98–118, <https://doi.org/10.1177/1465116516678932>; Ulrike M. Vieten and Scott Poynting, “Contemporary Far-Right Racist Populism in Europe,” *Journal of Intercultural Studies* 37, no. 6 (2016): 533–40, <https://doi.org/10.1080/07256868.2016.1235099>.

¹⁵ Zack Beauchamp, “Brexit Was Fueled by Irrational Xenophobia, Not Real Economic Grievances - Vox,” *Vox.com*, 2016, <https://www.vox.com/2016/6/25/12029786/brexit-uk-eu-immigration-xenophobia>; Brendan Donnelly, “A Chaotic Brexit Is Still a Possibility,” *LSE Brexit*, 2017, 1–4.

representation of reality, a simple Google Trends consultation shows that the search query “John Rawls” with the Google qualifier “American philosopher” started trending upward again after a 14-year decline in early 2016, as the Trump and Brexit campaigns gained steam.¹⁶

In other words, this dissertation looks ahead, positioning itself within a relatively new and, until recently, small set of literature applying Rawls to technology. Scholars on the same mission, as I will show in Chapter 2, show how Rawls’ theories can be used to address different challenges related to a wide range of technologies. The present study concentrates on policies regulating social media as an online technology. To lay the groundwork for future, similar inquiries, as the pendulum swings back towards reason, this dissertation asks questions like:

Could Rawls provide a reasonable justification for the Russian influence campaign on social media during the 2016 presidential election in the U.S.? Or would it show why it was unjust? What would Rawls say to China’s national policy of social media surveillance and censorship? And would Rawls argue for or against the new social media data collection practices implemented by the Department of Homeland Security?

The following examines these national policies through a Rawlsian lens: Are they fair? Are they just? Do they respect the rights of the citizens for whom they apply? Do they make the citizen more or less free? To that end, a research design had to be found which could unpack the policies in full and expose them to the application of Rawlsian ethics.

¹⁶ Google Trends, “John Rawls,” Google Trends, 2018, <https://trends.google.com/trends/explore?date=all&geo=US&q=%2Fm%2F0x3r3>.

Research design

My proposal for this dissertation originally had a broader scope, looking at ethics in cybersecurity policies as information policy writ large. As I went through the process of finding the right cases to study, however, it quickly became clear that a narrower focus was needed. At the same time, cybersecurity scholars were beginning to consider social media as an essential part of national cybersecurity, not least because of how ISIS used social media both strategically and tactically. As the cases mentioned above impressed themselves on me, it became apparent that social media was the right aspect of cybersecurity to focus on.

Research Questions

The questions mentioned above now went through a process of specification in order to become research questions. The purpose of the first three questions was to unpack the policies involved in the three cases I had chosen to study, and how they related to Rawls. The fourth questions and its sub-questions would provide the foundation for the ethical exploration on which I was about to embark:

RQ1: What national security policies encompassing social media platforms exist at present in Russia, China and the US?

RQ2: What is the balance of state security measures versus citizens' rights in each of the three sets of policies and their implementation?

RQ3: To what extent do these existing policies reflect Rawls' conceptions of liberty, justice as fairness and the Law of Peoples?

RQ4: Given what we know from RQ3, from a Rawlsian perspective:

- Under what circumstances should citizens be entitled to national security from the state on social media platforms?
- Which liberties can a state ethically require a citizen to surrender on social media to achieve national security?
- Which methods can states employ to protect citizens from misuse of their social media data without compromising Rawlsian justice as fairness?

Structure

The structure of these questions provides a scaffolding for the research design. For each case, the policies under analysis would have to be teased apart and their components examined in order to provide answers to RQ1, RQ2 and RQ3 for each case. The cases would each get a chapter dedicated to them, whereas the exploration of RQ4 would happen in the final discussion, based on the findings in the other research questions. The last subquestion almost begs for a theoretical deliverable – an ethical test applicable to national policies which govern social media. Such a test would be a distillation of everything that had been shown to that point in the dissertation, and thus represent the findings as both a framework for discussion and a concrete fairness evaluation tool for policymakers. The Rawls Test for social media ethics would thus be a fitting outcome of the study, if the findings supported its validity.

Method of policy analysis

To take apart and analyze the policies, one method presented itself as particularly suitable for the study, since the goal of the latter was to build a framework for discussion of matters of national interest.

The Frame Reflection theory of Schön and Rein

Schön and Rein's Frame Reflection method is intended as an instrument of mediation, a theoretical tool to be used when what they call "policy controversies" seem intractable. Frame reflection was introduced by Schön and Rein¹⁷, but has been further developed by several scholars¹⁸As a method, it has seen implementations in a multitude of analyses in as many different policy areas¹⁹

¹⁷ Donald A Schon and Martin Rein, *Frame Reflection: Toward the Resolution of Intractable Policy Controversies* (Basic Books, 1995); Martin Rein and Donald Schön, "Frame-Critical Policy Analysis and Frame-Reflective Policy Practice," *Knowledge and Policy* 9, no. 1 (1996): 85–104, <https://doi.org/10.1007/BF02832235>.

¹⁸ Mieke Verloo, "Mainstreaming Gender Equality in Europe. A Critical Frame Analysis Approach," *The Greek Review of Social Research* 117, no. B' (2005): 11–34, <https://doi.org/10.1063/1.3033202>; Merlijn van Hulst and Dvora Yanow, "From Policy 'Frames' to 'Framing': Theorizing a More Dynamic, Political Approach," *American Review of Public Administration* 46, no. 1 (2016): 92–112, <https://doi.org/10.1177/0275074014533142>.

¹⁹ Sanda Kaufman and Janet Smith, "Framing and Reframing in Land Use Change Conflicts," *Journal of Architectural and Planning Research* 16, no. 2 (1999): 164–80; O. A. Ogunseitan, "Framing Environmental Change in Africa: Cross-Scale Institutional Constraints on Progressing from Rhetoric to Action against Vulnerability," *Global Environmental Change* 13, no. 2 (2003): 101–11, [https://doi.org/10.1016/S0959-3780\(03\)00004-9](https://doi.org/10.1016/S0959-3780(03)00004-9); Jörg Michael Dostal, "Campaigning on Expertise: How the OECD Framed EU Welfare and Labour Market Policies - And Why Success Could Trigger Failure," *Journal of European Public Policy*, 2004, <https://doi.org/10.1080/13501760410001694255>; Arjen E. Buijs, "Public Support for River Restoration. A Mixed-Method Study into Local Residents' Support for and Framing of River Management and Ecological Restoration in the Dutch Floodplains," *Journal of Environmental Management* 90, no. 8 (2009): 2680–89, <https://doi.org/10.1016/j.jenvman.2009.02.006>; Esther Prins, "Framing a Conflict in a Community-University Partnership," *Journal of Planning Education and Research*, 2005, <https://doi.org/10.1177/0739456X04270370>; Falk Daviter, "Policy Framing in the European Union," *Journal of European Public Policy* 14, no. 4 (2007): 654–66, <https://doi.org/10.1080/13501760701314474>; Minah Kang and Jiho Jang, "NIMBY or NIABY? Who Defines a

Schön and Rein suggest the old virtue of “walking a mile in the other person’s shoes” as a foundation for this mediation. Their method suggests building policy frames consisting not just of the interests that the conflicting parties bring to the policy discussion, but also the cultural and historical background that gave rise to those interests, and the values inherent in them. The method is aimed specifically at conflicts involving competing policies, which is what Schön and Rein refer to as “controversies”. The “controversy” in question can concern competing policy solutions to a particular issue or competing views on implementation of a particular policy. In both cases, Schön and Rein describe these policy controversies as “symbolic contests over the social meaning of an issue domain, where meaning implies not only what is at issue, but what is to be done”.²⁰ Frame reflection is thus not only a technique for policy analysis on a theoretical level, but also on an actionable/practical level. This broadly makes the techniques and modes of analysis in frame reflection highly applicable to the dissertation research proposed here, but it also would serve the latter well in a narrower sense.

Frame reflection is the use of framing as an analytical, meaning-deriving tool. Schön and Rein present four types of frames in the most abstract sense:

A frame can be seen as a scaffolding (an inner structure), a boundary that sets off phenomena from their contexts (like picture frames), a cognitive/ appreciative schema of

Policy Problem and Why: Analysis of Framing in Radioactive Waste Disposal Facility Placement in South Korea,” *Asia Pacific Viewpoint* 54, no. 1 (2013): 49–60, <https://doi.org/10.1111/apv.12007>; Øyvind Ihlen, Tine Ustad Figenschou, and Anna Grøndahl Larsen, “Behind the Framing Scenes: Challenges and Opportunities for NGOs and Authorities Framing Irregular Immigration,” *American Behavioral Scientist* 59, no. 7 (2015): 822–38, <https://doi.org/10.1177/0002764215573254>.

²⁰ Schon and Rein, *Frame Reflection: Toward the Resolution of Intractable Policy Controversies*, 29.

interpretation (an idea that one finds in Piaget, Vickers, Bartlett, as well as Davidson, whom we quote), or a generic diagnostic/prescriptive story (as in our view of problem framing, and also in the writings of Paul Ricoeur and other hermeneuticists)²¹

All of these definitions of frames are applicable to the process of frame reflection, and more specifically, frame-critical policy analysis (see below). However, Schön and Rein are very specific about the constructivist nature of this type of analysis:

Regardless of whether we see the frames at work in policy controversies as strong narratives or as schemas of interpretation, these frames are not self-evident. If we wish to study them, we must *construct* them, which is to say that from some evidence we must infer interpretations about belief and meaning and implications for action to deal with coping and facing.²²

Frame reflection and more specifically, the sub-component of frame-critical policy analysis are thus both descriptive and interpretive analysis tools, in which the properties of a particular object of study (in this case named the *policy object* by Schön and Rein²³) are presented, but also contextualized and interpreted. The frame, then, is a specific, interpretive view of the entirety of a policy object, its properties and its context.

²¹ Rein and Schön, “Frame-Critical Policy Analysis and Frame-Reflective Policy Practice,” 88.

²² Rein and Schön, 90.

²³ Rein and Schön, 93.

By making interpretation central to frame-critical policy analysis, Schön and Rein acknowledges that this type of analysis is prone to be characterized by subjectivity. They call this epistemological problem the “relativist trap”²⁴ as the process of constructing frames will undoubtedly be shaped relative to the separate frame in which the analyst exists. Schön and Rein do not attempt to solve this by forcing objectivity upon frame construction but offer methodological strategies which may at least diminish the impact of subjectivity on the end result. First and foremost, they argue that the analyst must strive to consider and step out of his or her own frame when constructing frames surrounding a policy object, in order to solve a frame conflict without simply replacing or merging the frame in question with his or her own.

Frame-critical policy analysis and independent criteria

By not simply presenting competing policies as narrow representations of interest, but as rich narratives that paint a fuller picture of the situation, Schön and Rein argue that it is easier to understand and sympathize with the competing party’s position. And because the policy components have been taken apart and contextualized, Schön and Rein suggest that commonalities are easier to find as part of the mediation and eventual solution of the conflict.

But more specifically – and highly applicable to this dissertation proposal - they also present a strategy that relies on adherence to an external set of values:

The second strategy would resolve frame conflicts by appealing, not to a shared perception of fact, but to consensual, logically independent criteria for evaluating frames and choosing

²⁴ Schon and Rein, *Frame Reflection: Toward the Resolution of Intractable Policy Controversies*, 41.

among them. For example, disputants might evaluate their respective frames by reference to a common criterion of utility²⁵

It is possible, then, in the process of frame-critical analysis, to reference a third, independent set of criteria when comparing two different frames. This does not remove relativism from the equation, as subjectivity still enters into the construction of frames, but it does lessen the impact of any subjectivity in the choice between two (or more) frame in terms of policy implementation. Also, it can be argued that any major flaws in the construction of the frames due to the bias of the analyst could become more apparent when an independent reference point is entered into the picture, aiding the analyst in the process of becoming aware of his or her own frame.

To put it another way, the “independent criteria” could very well be the “yardstick” mentioned earlier, i.e. Rawls’ theories. The application of Schön and Rein’s method would thus focus on the Frame-critical analysis method and then apply the independent criteria in the shape of Rawlsian ethics.

More concretely, frame-critical policy analysis entails the construction of two policy frames, a Rhetorical Frame and an Action Frame. The Rhetorical Frame contains those policy elements that have entered into the discourse. It is how the policy is being spoken about by those proposing it, those touched by it, or those reporting on it in different venues. Schön and Rein suggest that the rhetoric surrounding the policy, when observed from an outsider’s point of view, will often reveal more about the policy’s intentions, values, sociocultural conditions and

²⁵ Schon and Rein, 43.

historical context than its proposers and proponents ever could do alone. Thus, by building a frame solely based on this rhetoric, these elements can be separated from any consequences of implementation of the policy. These are instead dealt with in the Action Frame which is where the real-world expressions of the policy are found. In this frame, it becomes visible what the policy looks like when real people, real money and real problems are involved. Here, the challenges of policy implementation come to the fore in a separate frame, which is mostly free of any lofty intentions or hopes for the success of the theory. It is in the Action Frame that we see what a policy looks like when it enters the political debate and when it transcends from policy to law. It is here we see what the results of implementing the policy are – or could be in future implementation of the policy somewhere else. Of course, this is equally revealing as the Rhetorical Frame, but the two are distinct so that the main purpose of frame-critical analysis is fulfilled: Disassembling the policy into its components, separating them, studying them and most importantly, putting them into context in order to fully understand the policy as a sum of its parts.

Rhetorical Frames and Action Frames in each chapter

For each case, this research design thus includes a construction of Rhetorical Frame and an Action Frame, which is then compared and contrasted theoretically with a Rawlsian Frame, which I shall construct by introducing Rawls and his theoretical ethics concepts in Chapter 2. In addition to the Rhetorical Frame, the Action Frame and the Rawlsian Frame, a background for the frames is provided at the beginning of each chapter. The purpose is to give an impression of the general conditions from which the policies have emerged, as Schön and Rein's frame criteria dictate. Furthermore, after the construction of the Rhetorical and Action Frames in each chapter,

I will provide an even deeper dive into the national, cultural dimensions that might be impacting or shaping the policies. It is in these Cultural Background sections that the more unexpected perspectives on the policies can be found, i.e. what it is in the national tradition and culture of the country in question that paves the way for the emergence of the policy?

With all these components in place within the frames, the examination of the policies becomes fairly comprehensive, which is necessary for the ensuing ethical discussion based on Rawls' principles.

Data collection

The data in this study consist of official policy documents and public statements about the policies as well as expert interviews.

Documents and public statements

In my proposal, I gave a rather expansive list of sources for documents relating to the cases I had yet to choose. As my focus narrowed to solely examining national social media policies, the document sources also narrowed down to the official publications of the countries in question, which made the process much easier. I had expected the collection of documents from Russia and China to be made difficult by language barriers and general, national secrecy. However, this turned out not to be the case. Both Russia and China have publicized English versions of their current national information strategy (in the case of Russia) and cybersecurity and information strategies (in the case of China). When data collection began in late 2016, early 2017, Russia had yet to publish their documents in English, as the directives had only recently been decided upon

by the Kremlin. But a translation was provided on the official website of the Russian Federation before that phase of the data collection ended. China officially provides English translations of most of their national policy and strategy documents.

To verify that there were no discrepancies between the national and the international version of these documents, I compared machine-translated versions of every official, public document I used to the translated version. In the cases where these documents came from official websites, I made sure to use a VPN to simulate that I was downloading the document within the borders of the countries in question. This way, I would be as certain as possible that the document I received was the same as the one available that country's own citizens. I found no substantial, meaning-altering discrepancies in any of the cases and thus moved forward with the officially provided translations.

Interviews

The selection of interviewees for the expert interviews happened through a process involving several modes of selection. Some were selected through a snowball effect. For example, Margo Schlanger was suggested by Esha Bhandari, and Margaret E. Roberts was suggested by a scholar who was scheduled for an interview, but whose most recent work turned out to be irrelevant to this study. Others were selected through a process resembling convenience sampling, i.e. Congressman Adam Schiff happens to be the congressman representing the district in which I live, which meant that I was fortunate enough to have relatively easy access to the ranking member of the House Intelligence Committee. There are two Danes among the interviewees, Thomas Elkjer Nissen and Henrik Moltke, and having lived in Denmark most of my life, those interviews may have seemed like convenience choices. However, though I was slightly

acquainted with Moltke before the interview phase began, both were chosen on the merits of their work. Elkjer Nissen became known to me when high-level RAND Corporation analyst working with the U.S. Army handed me his book a part of the study I did as a summer associate at RAND in 2015. The person who handed me the book did not know I grew up in Denmark. The remaining experts were chosen because of their renown and the actual work they have done in their fields of study. A full list of interviewees can be seen in Appendix A.

Chapter overview and summary of findings

In the chapter immediately succeeding this one, I will introduce John Rawls' main theoretical concepts. First, however, a short review of other work that has related Rawlsian principles to technology or information ethics and policy is provided. Then, Rawls' main principles and concepts are listed. I have only selected those that are relevant to this study, however, as Rawls' work was quite expansive, and fathomed many concepts and theoretical elements that, though very capturing and interesting, are better discussed elsewhere. I also provide a review of the positions of Rawls' main opposing discussants with regards to freedom concepts, Robert Nozick and Amartya Sen. Following that is an overview of the consequentialist/utilitarian thinkers who have critiqued Rawls' contractarianism and represented the staunchest opposition to it. Absent here are Rawls' notions of privacy and those scholars who have explored them. I have placed a review of those in Chapter 5, as it relates to the main topic discussed there. A review of communitarian opposition to Rawls can also be found in Chapter 5 for the same reason.

In Chapter 3, I present the first case, which is the Russian influence campaign waged on American social media during the 2016 U.S. presidential election cycle. This is an example of how an offensive, national information strategy can include social media as part of an aggressive foreign policy. The chapter begins with the relatively recent historical background that informs the policies underlying the strategy, i.e. the disinformation strategies and campaigns used by the KGB during the cold war. Next, I describe the details of the current disinformation strategy as we know them and show how it corresponds with both the national information strategy of the Russian Federation, the so-called Gerasimov doctrine and the rhetoric used by both President Putin and others in public statements. A perspectivization based on a journey even further back in Russia's history and a very cautious review of scholars who have tried to define a Russian "character" shows a culture in which deception is sometimes seen as virtuous, which stands in stark contrast to typical American values. The value discussion then leads into the discussion of Russia's policies as they contrast with Rawlsian ethics. I find in Rawls a strong argument against using such tactics, both because of the *reciprocity principle* presented in his work on international justice, and because of how such tactics impedes the access to information that Rawlsian principles dictate is a right for everyone as part of a fair, democratic process.

In Chapter 4, I turn towards case number two. Whereas the Russia case in Chapter 3 represents an offensive, outwardly-facing strategy for foreign policy objectives, the China case is an example of how social media regulation play a part of a larger, domestic policy. The chapter begins with an overview of social media in China and the isolationist stance taken by the Chinese government with regards to the Internet in general. I continue by showing how, after a period of gradually loosening its grip on online media and communication overall, the Chinese

government is now again clamping down on dissent and attempts at mobilization on social media. Under Xi Jinping, China has also returned to a normative, value-based censorship strategy that is reminiscent of the era of Mao. The Rhetorical Frame is built from, among other sources, speeches by Xi. The Action Frame analyzes the current legislation and stated policies governing social media as well as enforcement actions taken in China with a particular focus on the new cybersecurity legislation that was enacted in 2016 and became active law in 2017. The law puts unprecedented pressure on providers of social media services to ensure that their users comply with the law and stay within the government's often vaguely stated and socially normative guidelines. The Cultural Background section shows how more than two millennia of Confucianism impacts online user behavior and why, in spite of the efforts of some parts of the population to mobilize protests and fight the government's suppression of free speech, the majority of China's more than 700 million Internet do not try to circumvent the "Great Firewall" and seem to generally tolerate conditions that would be completely unacceptable to a Western Internet user. More broadly, the adherence to Confucianism also allows for the kind of paternalism the Chinese government is exhibiting. When challenging the Chinese policy frames with the Rawlsian Frame towards the end of the chapter, it becomes clear that China's social media policy is in violation of a number of Rawlsian principles, including his opposition to paternalism. The question is also asked if China's status as (in words of the Chinese government) a developing country, can be considered "burdened" by its historical, economic and sociocultural conditions, which would make China subject to a different set of Rawlsian principles. However, it is shown that even if this is the case, China does not live up to the transparency conditions and

requirements for consulting the people that Rawls argues must be in place in lieu of a fair democracy.

In Chapter 5, after looking at a broad, outwardly-facing, national social media strategy in Russia and then narrowing the focus slightly by examining an inward-facing domestic policy in China, I zoom in even further on a particular social media policy in the U.S. It is really two sets of policy and legislation, but I refer to it as a “dual policy” because it impacts the social media privacy of the same group of people through similar means and is implemented and enforced by the same government agency. The dual policy targets a much smaller population than the policies in Chapter 3 and 4, but it also distinguishes itself by using social media to reach outside the confines of the Internet. The policy object in question consists of, on the one hand, the DHS policy of searching electronic devices belonging to U.S. citizens (and lawful permanent residents) at the country’s borders with social media activity included in the search parameters, and on the other hand, the USCIS’ permanent registration and archiving of naturalized citizens’ social media handles and activities. This chapter is thus focused on the inseparable relationship between free speech and privacy, and I initiate the analysis by showing how the U.S. government has likely used social media as a source for intelligence collection about individuals since these media platforms first emerged. First, the electronic surveillance system known as ECHELON was expanded to possibly include information from early social media platforms, and with the passing of the Patriot Act after the 9/11 attacks, social media became an essential part of this intelligence-gathering process, increasing the risk of the government accessing personal information about the individual that may not be relevant to any investigation, This concerns about such risks were further substantiated by the Snowden revelations in 2013, which, for a

while, led the government to reconsider and heighten the supervision of the data and information collection practices of its agencies, at least until the San Bernardino terror attack occurred in 2015, after which the pendulum swung back again.

The Rhetorical Frame in this case includes the public defenses of the dual policy by the Department of Homeland Security, as well as an analysis of the information-relevant parts of the National Security Strategy of the Trump administration. The latter, similarly to the equivalent policy announcements from Russia and China analyzed in chapters 3 and 4, employs vague language so open to interpretation that it gives the government considerable wiggle room to define policies more intrusive than previously seen. The implementation of these policies, with a focus on the aforementioned dual DHS policy, is then analyzed in the Action Frame.

For the cultural-historical background, I examine what privacy has actually meant in an American sense over the last century. With its close ties to freedom of speech, I study the place privacy holds in the core American value set, if there such a value set exists. I show how privacy has been tied to an absolutist conception of liberty that has spawned the individualism that emerged alongside neoliberalism, and how some scholars have claimed that it is this individualism, with roots in the American revolution, that gives meaning to the term “American exceptionalism”. In the context of this policy analysis, a paradox now emerges: How can privacy-breaching policies as intrusive as the dual policy analyzed here emerge in a nation so firmly based on the value of individual liberty?

But as it turns out, the purported historical grounding of America as a nation based on individualist ideals may very well be misguided. There is substantial evidence that shows that if there is such a thing as an “American character” or a common value set across the many cultures

making up the United States, it is dominated by local communalism, i.e. adherence to local community values over the needs of the individual. Towards the end of the chapter, I consider the possibility that the election of Donald Trump may not only show that local communalism is alive and well, but that it has been inflated so much rhetorically that it has now become tribalism. In such an environment, the dual policies do not seem paradoxical at all.

From this vantage point I bring Rawls into the picture. Because Rawls was so focused on liberty and justice, it quickly becomes apparent that the dual policy violates his principles. Not only does it suffer from a similar lack of processual transparency as can be seen in the China case (and any such similarity should worry any supporter of open democracies), but it also falls short of complying with two core, Rawlsian principles: universality and maximin. Another growing similarity with China is the paternalism inherent in the rhetoric surrounding the dual policy, and I show how this is at odds with Rawls' concept of a fair democracy.

Chapter 6 is mainly concerned with a summation of how the findings chapters respond to the research questions. As mentioned, RQ1, RQ2 and RQ3 are all answered within each case. The chapter then continues with a discussion aimed at responding to RQ4. Here, I sum up the Rawlsian arguments as they have been presented in the discussions at the end of the findings chapters, that is, how Rawls' principles work in these specific social media policy contexts, to answer RQ4's first two subquestions. The chapter ends with the presentation of The Rawls Test for social media policy ethics. The test has been constructed using the findings in the dissertation and Rawlsian criteria as they manifest themselves with regard to social media and by presenting it and arguing for it, I simultaneously present a response to the third subquestion in RQ4.

As I conclude the dissertation in Chapter 6, I offer my thoughts on how future research may continue on from what the work I have presented here. But more importantly, I argue that the findings of this dissertation show that Rawls' deontological contractarianism is a viable foundation for ethical policymaking in technology and may even have practical benefits in speeding up the process by reducing the so-called "law lag".

Overall, I hope this dissertation will contribute in a meaningful way to the discourse on information and technology ethics, which is currently undergoing somewhat of a renaissance. By applying ethics to concrete policies, I also believe the findings in this dissertation can show the dangers of choosing the wrong, national policy for an information and communication infrastructure as integral to contemporary living as social media have become.

Chapter 2: Social media ethics and an introduction to John Rawls

In this chapter I will provide an overview of basic background knowledge needed to proceed into the findings of this dissertation. Each case analyzed will have its own background description, but the following are the essentials needed to understand Rawls as well as the current state of social media analysis from an ethical standpoint. First, however, I will present a brief, and by no means exhaustive, overview of critical social media literature that is focused on ethical issues, divided into five categories. Then, an introduction to the concepts and theories of John Rawls will follow, along with an overview of his main critics, including the utilitarianists with whom Rawls spent a lifetime trading philosophical punches. Finally, I will show how Rawls currently appears in literature related to technology and information.

Five categories that critique social media ethics

This dissertation would not be very useful if there was already a vast amount of literature on its subject. Though the ethics of national social media policies writ large have not been subject to much analysis – and particularly through a Rawlsian lens – a substantial body of work exists that analyzes the consequences for social media of broader policies or consists of ethical analyses of particular practices on social media. This literature includes a number of topics that can be divided into at least five separate categories:

1. Ethical evaluation and critiques of the conduct and business models of social media companies

This category contains critical analyses and normative judgments that situate social media corporations and their actions within socioeconomic and socio-technological contexts, often through a critique of social media as expressions of neoliberalism and/or late capitalism. These include critiques of personal data collection on social media for both commercial or political purposes,²⁶, research²⁷, and national security²⁸, algorithmic bias contributing to inequalities²⁹,

²⁶ Christian Fuchs, “Written Evidence - University of Westminster - Communication and Media Research Institute & Westminster Institute for Advanced Studies,” 2017, <http://westminsterresearch.wmin.ac.uk/20505/1/73970.pdf>; Christian Fuchs et al., *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, vol. 16 (Routledge, 2013); Alexandra Mateescu et al., “Social Media Surveillance and Law Enforcement,” 2015, http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf; Danah Boyd and Kate Crawford, “CRITICAL QUESTIONS FOR BIG DATA Provocations for a Cultural, Technological, and Scholarly Phenomenon,” *Communication & Society* 15, no. 5 (1986): 545–662, <https://doi.org/10.1080/1369118X.2012.678878>.

²⁷ Michael Zimmer, “‘But the Data Is Already Public’: On the Ethics of Research in Facebook,” *Ethics and Information Technology* 12, no. 4 (2010): 313–25; Jacqueline Lorene Bender et al., “Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment,” *Journal of Medical Internet Research* 19, no. 4 (April 6, 2017): e104, <https://doi.org/10.2196/jmir.7029>; Anders Albrechtslund, “Online Social Networking as Participatory Surveillance,” *First Monday*, 2008, <http://journals.uic.edu/ojs/index.php/fm/article/view/2142/1949>.

²⁸ David Lyon, “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique,” *Big Data & Society* 1, no. 2 (2014): 2053951714541861; Geoff Dean, Peter Bell, and Jack Newman, “The Dark Side of Social Media: Review of Online Terrorism,” *Pakistan Journal of Criminology* 3/4 (2012): 191–210, <http://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=89690880&site=ehost-live>; Thomas E Nissen, *The Weaponization of Social Media: Characteristics of Contemporary Conflicts* (Copenhagen, Denmark: Royal Danish Defence College, 2015); Bryce Clayton Newell and Joseph T. Tennis, “Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs” (Rochester, NY, October 2013), <http://papers.ssrn.com/abstract=2345468>.

²⁹ Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (NYU Press, 2018); Jenna Burrell, “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms,” accessed April 4, 2018, <https://doi.org/10.1177/2053951715622512>; Tarleton Gillespie, “Algorithmically Recognizable: Santorum’s Google Problem, and Google’s Santorum Problem,” *Information, Communication & Society* 20, no. 1 (January 2, 2017): 63–80, <https://doi.org/10.1080/1369118X.2016.1199721>; Tarleton Gillespie, “The Relevance of Algorithms,” *Media Technologies: Essays on Communication, Materiality, and Society* 167 (2014).

inequality-contributing/unfair hiring practices and work conditions³⁰, and how social media fit into the political discourse of late capitalism.³¹

2. Critique of global socioeconomic conditions as a consequence of the emergence of social media

In contrast to the first category, the analyses here are focused on the global effects of social media writ large, not just the conduct of corporations. This includes explorations of social media's impact on global economic conditions and balances of power.³² Analyses of how cultural differences and inequalities of access on the international level can be found in global and local social media platforms also belong in this category.³³

³⁰ Sarah Roberts, "Commercial Content Moderation: Digital Laborers' Dirty Work," in *Intersectional Internet: Race, Sex, Class and Culture Online*, ed. Safiya Noble and Brandesha Tynes (Peter Lang, 2016), <http://ir.lib.uwo.ca/commpub/12>; Lilly Irani, "The Hidden Faces of Automation," *XRDS: Crossroads, The ACM Magazine for Students* 23, no. 2 (December 15, 2016): 34–37, <https://doi.org/10.1145/3014390>; Alessandro Acquisti and Christina M. Fong, "An Experiment in Hiring Discrimination Via Online Social Networks," *SSRN Electronic Journal*, July 17, 2012, <https://doi.org/10.2139/ssrn.2031979>; Statista, "Global Social Media Ranking 2018 | Statistic," Statista.com, 2018, <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>; Patricia Sánchez Abril, Avner Levin, and Alissa Del Riego, "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee," *American Business Law Journal* 49, no. 1 (March 1, 2012): 63–124, <https://doi.org/10.1111/j.1744-1714.2011.01127.x>.

³¹ Daniel Trottier and Christian Fuchs, *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and Youtube*, vol. 16 (Routledge, 2014); Christian Fuchs, "Social Media and Capitalism," *Analysis*, 2011; Robert W Gehl, *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism* (Temple University Press, 2014); Yarimar Bonilla and Jonathan Rosa, "# Ferguson: Digital Protest, Hashtag Ethnography, and the Racial Politics of Social Media in the United States," *American Ethnologist* 42, no. 1 (2015): 4–17; Brian D Loader and Dan Mercea, "Networking Democracy? Social Media Innovations and Participatory Politics," *Information, Communication & Society* 14, no. 6 (2011): 757–69; Nikita Carney, "All Lives Matter, but so Does Race," *Humanity & Society* 40, no. 2 (May 13, 2016): 180–99, <https://doi.org/10.1177/0160597616643868>.

³² Ramesh Srinivasan, *Whose Global Village?: Rethinking How Technology Shapes Our World* (NYU Press, 2017); Arne Hintz, "From Media Niche to Policy Spotlight: Mapping Community-Media Policy Change in Latin America," *Canadian Journal of Communication*, 2011; Michael L. Best, "The Internet That Facebook Built," *Communications of the ACM* 57, no. 12 (November 26, 2014): 21–23, <https://doi.org/10.1145/2676857>.

³³ E. Gabriella Coleman, "Ethnographic Approaches to Digital Media," *Annual Review of Anthropology* 39, no. 1 (October 21, 2010): 487–505, <https://doi.org/10.1146/annurev.anthro.012809.104945>; Sandra Ponzanese, *Gender*,

3. The ethics of social media as media.

This category is mostly rooted in the communication, information and media studies realms and observes social media more narrowly as platforms for the exchange of information and content. showing how social media are contributing to a less truthful or less ethical news environment³⁴. This is also where critiques of the roles social media play in political communication can be found.³⁵

Globalization, and Violence: Postcolonial Conflict Zones (Routledge, 2014); Muchazondida Mkonu, “Sustainability and Indigenous Tourism Insights from Social Media: Worldview Differences, Cultural Friction and Negotiation,” *Journal of Sustainable Tourism* 24, no. 8–9 (September 19, 2016): 1315–30, <https://doi.org/10.1080/09669582.2016.1177066>.

³⁴ Martin. Hirst and Martin, *News 2.0: Can Journalism Survive the Internet?* (Allen & Unwin, 2011), <http://dro.deakin.edu.au/view/DU:30041209>; Alfred Hermida, “Tweets and Truth,” *Journalism Practice* 6, no. 5–6 (October 2012): 659–68, <https://doi.org/10.1080/17512786.2012.667269>; Sharon Rider and Michael A. Peters, “Post-Truth, Fake News: Viral Modernity and Higher Education,” in *Post-Truth, Fake News* (Singapore: Springer Singapore, 2018), 3–12, https://doi.org/10.1007/978-981-10-8013-5_1; Chei Sian Lee and Long Ma, “News Sharing in Social Media: The Effect of Gratifications and Prior Experience,” *Computers in Human Behavior*, no. 28 (2012), <https://doi.org/10.1016/j.chb.2011.10.002>; Ruth A. Harper, “The Social Media Revolution: Exploring the Impact on Journalism and News Media Organizations,” *Inquiries - Social Sciences, Arts and Humanities*, 2010.

³⁵ Guess, Nyhan, and Reifler, “Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 U.S. Presidential Campaign”; Hunt Allcott and Matthew Gentzkow, “Social Media and Fake News in the 2016 Election,” *Journal of Economic Perspectives—Volume* 31, no. 2—Spring (2017): 211–36, <https://doi.org/10.1257/jep.31.2.211>; Cass R Sunstein, *# Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, 2018); Philip N Howard et al., “Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?,” 2017, <http://275rzy1ul4252pt1hv2dqyuf.wpengine.netdna-cdn.com/wp-content/uploads/2017/07/2206.pdf>.

The category also contains work on social media's role in access to information³⁶ and methods used in social media advertising.³⁷

4. Social media as commercial or cultural products

Here, social media is understood mostly as an instrument of communication and information retrieval within an organization or an institution. This category including analyses of using social media in education and within a business³⁸, and how unequal access to the hardware platforms that social media exist on may become a social problem³⁹

³⁶ Richard Fletcher and Rasmus Kleis Nielsen, "Are People Incidentally Exposed to News on Social Media? A Comparative Analysis," *New Media & Society*, August 17, 2017, 146144481772417, <https://doi.org/10.1177/1461444817724170>; Seth Flaxman, Sharad Goel, and Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly* 80, no. S1 (January 1, 2016): 298–320, <https://doi.org/10.1093/poq/nfw006>; Pariser, *The Filter Bubble: How the New Personalized Web Is Changing What We Read and How We Think*.

³⁷ A-Reum Jung, "The Influence of Perceived Ad Relevance on Social Media Advertising: An Empirical Examination of a Mediating Role of Privacy Concern," *Computers in Human Behavior* 70 (May 1, 2017): 303–9, <https://doi.org/10.1016/J.CHB.2017.01.008>; Bay, "The Ethics of Psychometrics in Social Media: A Rawlsian Approach"; Christian Fuchs, *Social Media: A Critical Introduction* (Sage, 2017).

³⁸ Stefania Manca and Maria Ranieri, "Facebook and the Others. Potentials and Obstacles of Social Media for Teaching in Higher Education," *Computers & Education* 95 (April 1, 2016): 216–30, <https://doi.org/10.1016/J.COMPEDU.2016.01.012>; Abu Elnasr E. Sobaih et al., "To Use or Not to Use? Social Media in Higher Education in Developing Countries," *Computers in Human Behavior* 58 (May 1, 2016): 296–305, <https://doi.org/10.1016/J.CHB.2016.01.002>; Thomas Aichner and Frank Jacob, "Measuring the Degree of Corporate Social Media Use," *International Journal of Market Research* 57, no. 2 (March 1, 2015): 257–76, <https://doi.org/10.2501/IJMR-2015-018>.

³⁹ Jen Schradie, "The Trend of Class, Race and Ethnicity on Social Media Inequality," *Information, Communication & Society* 15, no. 4 (May 2012): 555–71, <https://doi.org/10.1080/1369118X.2012.665939>; Leo Van Audenhove et al., *Social Inequalities, Media, and Communication: Theory and Roots* (Lexington Books, 2016); Eran Fisher, "Class Struggles in the Digital Frontier: Audience Labour Theory and Social Media Users," *Information, Communication & Society* 18, no. 9 (September 2, 2015): 1108–22, <https://doi.org/10.1080/1369118X.2015.1018300>; Philip M. Napoli and Jonathan A. Obar, "The Emerging Mobile Internet Underclass: A Critique of Mobile Internet Access," *The Information Society* 30, no. 5 (October 20, 2014): 323–34, <https://doi.org/10.1080/01972243.2014.944726>.

5. Social media, identity and media psychology.

Related to media effects and similar studies of reception psychology, this category includes analysis of the effects of social media addiction⁴⁰, how social media may be breaking down other social structures⁴¹ and critiques of how social media affect the users, both on a neurological and psychological level⁴²

The above review is a good indication of the wide spectrum of work being done in the critical analysis of social media writ large. These critiques and analyses often touch upon normative aspects and adds meaning and social context to the much larger body of work that e.g. provides empirical evidence of the graphs and network structures that underpin social media or studies social media as applied communication and/or marketing theory. While the latter are respectable endeavors within their fields, they do not contribute much to the larger, macro-level issues discussed in this dissertation. The critical analyses in the above review do, of course, but most often in a narrower manner, focused on a specific topic or dimension of social media practice or

⁴⁰ Daria J. Kuss and Mark D. Griffiths, “Online Social Networking and Addiction—A Review of the Psychological Literature,” *International Journal of Environmental Research and Public Health* 8, no. 9 (August 29, 2011): 3528–52, <https://doi.org/10.3390/ijerph8093528>.

⁴¹ Sherry Turkle, “Alone Together” (New York: Basic Books, 2011); José Van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press, 2013); Alex Rosenblat and Luke Stark, “Uber’s Drivers: Information Asymmetries and Control in Dynamic Work,” *SSRN Electronic Journal*, July 30, 2015, <https://doi.org/10.2139/ssrn.2686227>.

⁴² José van Dijck, “‘You Have One Identity’: Performing the Self on Facebook and LinkedIn,” *Media, Culture and Society* 35, no. 2 (2013): 199–215, <https://doi.org/10.1177/0163443712468605>; Luke Stark and Kate Crawford, “The Conservatism of Emoji: Work, Affect, and Communication,” *Social Media + Society* 1, no. 2 (September 22, 2015): 205630511560485, <https://doi.org/10.1177/2056305115604853>; Paul J Zak, “The Neuroscience of Trust Management Behaviors That Foster Employee Engagement,” Level Five Executive, 2017, <https://levelfiveexecutive.com/wp-content/uploads/2017/03/hbr-neuroscience-of-trust.pdf>.

conduct on the corporate or the consumer side. What I am attempting here, is to provide a larger context, to discuss how social media *is* embedded in our societal structure vis-à-vis how it *should* be embedded. Since national policies regarding social media are among the main societal components that dictate the latter, I have chosen them as my objects of study. Such a choice of study object demands a theoretical and ethical source that is equally wide-ranging and structure-oriented on a societal level. And this is why I have chosen John Rawls' work as the theoretical foundation for this dissertation.

Meet John Rawls

John Rawls has been called the most important political philosopher in the 20th century. Whether that is true or not, Rawls did leave behind a compelling set of philosophical works which have influenced political thought since the early 70s. Many links between the convictions of contemporary politicians and Rawls' work have been made, and particularly President Barack Obama seems to have studied Rawls.⁴³ This is somewhat unsurprising, since Rawls still had a big presence as a professor at Harvard University when Obama studied there in 1988-1991.

John Bordley Rawls was born and grew up in Baltimore, MD. He achieved a Ph.D. degree at Princeton in 1950, having studied under Norman Malcolm, who was heavily influenced by Wittgenstein. This kept Rawls from venturing too far into metaphysics, and most likely

⁴³ Alan Haworth, "Obama's Debt to Rawls?," Practical Ethics, 2012, <http://blog.practicaethics.ox.ac.uk/2012/11/obamas-debt-to-rawls/>.

influenced his very tangible and constructive approach to political philosophy.⁴⁴ Throughout the fifties and sixties, Rawls' political philosophy took shape through a series of papers and lectures attempting to ground the modern Anglo-American philosophy tradition in realizable concepts, rather than choosing an epistemological or ontological route. This culminated in 1971's *A Theory of Justice*, a magnum opus in which Rawls provides an almost complete societal model with strong roots in moral philosophy. His main objective is to describe – and provide a path to – a society in which justice prevails at all levels and in all institutions. This raises the demand for a definition of justice as more than a mere instinctual notion of fairness. Accordingly, Rawls manages to establish the fairness concept in depth and apply it societal justice. He does this by modernizing an old philosophical concept: the social contract, as described by, among others, Jean-Jacques Rousseau and John Locke.

As the capitalism of late-modernity began to shift its shape in the late 60s, Rawls observed a clear preference for utilitarianism in Western societies. He saw utilitarianism's maximization of good for the biggest number of people as unjust and thereby immoral, as he felt it carried in it the potential for marginalization of the few. If one is to believe the work done by Thomas Piketty⁴⁵, this is exactly what capitalism in the post-industrial society is doing by letting capital income grow faster than wage income. If Piketty is right, utilitarianism has been taken to a dysfunctional extreme. He contends that the post-industrial version of utilitarianism is influenced

⁴⁴ Henry S. Richardson, "John Rawls," Internet Encyclopedia of Philosophy (Internet Encyclopedia of Philosophy Pub), accessed April 4, 2018, <http://www.iep.utm.edu/rawls/>.

⁴⁵ Thomas Piketty, "Capital in the Twenty-First Century: A Multidimensional Approach to the History of Capital and Social Classes," *British Journal of Sociology* 65, no. 4 (2014): 736–47, <https://doi.org/10.1111/1468-4446.12115>.

by one of free-market libertarianism's central tenets: maximization for the many happens as a consequence of maximization for the few who possess the means of maximization. Except, as Piketty points out, the so-called rising tide that lifts all boats never seems to come in. The result of attempting to maximize good for the many by maximizing good for the few is instead a gradual marginalization of the few, as Rawls suspected. But, as Piketty points out, because this version of utilitarianism has been left to its own device for decades, the marginalized few have become the marginalized many. More than ever, it would seem, we need Rawls' ideas of fairness and equality.

The works of John Rawls

In *A Theory of Justice*⁴⁶, Rawls introduces most of the concepts and theories relevant to this paper, and the overview it provides. However, Rawls would revisit his theories many times over the subsequent years of his career until his death in 2002. These revisits occurred in order to both augment and reiterate his general theory. In *Political Liberalism*⁴⁷, Rawls fleshes out in more detail, how his theory of justice would actually be implemented in terms of political institutions and a concrete, real societal structure. Particularly, he takes on the notion of legitimacy, and how the institutions in the societal structure are held accountable for justice.

Until that point, Rawls had primarily focused on establishing one society. But as globalization spread, Rawls began to think about societies in the plural. What would a just,

⁴⁶ John Rawls, "A Theory of Justice" (Cambridge Mass.: Harvard University Press, 1971).

⁴⁷ John Rawls, *Political Liberalism* (Columbia University Press, 2005).

global society look like? How can just societies interact with those characterized by injustice? This is the topic of *The Law of Peoples*⁴⁸, in which a longer version of a 1993 article by the same name was published, combined with another article from 1997, “The Idea of Public Reason Revisited”. In 1999, many of Rawls’ singular articles and papers were made available in *Collected Papers*⁴⁹ Rawls’ final work was *Justice as Fairness: A Restatement*⁵⁰, published a year before his death. Here, Rawls revisits *A Theory of Justice* and restates many of its principles – with some modifications. It also serves as shorter and more accessible summation of Rawls’ lifework, including his responses to some of his most vehement critics.

Rawlsian concepts and their inspiration

The social contract

As mentioned above, Rawls’ observation of late-modern capitalism’s utilitarian tendency to marginalize the few particularly takes shape in the 1960s. It is probably no coincidence that this was a time when the US was engaged in the Vietnam war, itself a symbol of how marginalization of the few (and eventually the many) happens as a result of taking the utilitarian approach. Rawls instead reaches back to pre-capitalist societal models in order to find a fair vision for contemporary capitalism. His overarching mission is to redefine the social contract. The French-Genevan philosopher Jean-Jacques Rousseau had found himself in similar situation as Rawls,

⁴⁸ John Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"* (Harvard University Press, 2001).

⁴⁹ John Rawls, *Collected Papers*, ed. Samuel Freeman (Cambridge Mass.: Harvard University Press, 1999).

⁵⁰ John Rawls, *Justice as Fairness: A Restatement* (Harvard University Press, 2001).

only 200 years prior. Rousseau's works on inequality, leading to *Of The Social Contract, or Principles of Political Right*, was highly influential on the political activists who would eventually topple the French monarchy in 1789 and establish the Republic of France. Rousseau is regarded as the main thinker of the French revolution because of this.⁵¹

Rousseau's concept of a social contract is very concrete. He argues for abandoning total freedom in order to achieve what he calls *civil freedom*. The first, in Rousseau's view, is a property of *the state of nature*, a concept which was in effect introduced by Hobbes (calling it "the natural condition of mankind") and Locke. However, this starting point is pre-civilization, pre-society, a state of anarchy, or at least an existence governed only by the laws of nature. Rousseau argues that this may be ultimate freedom in principle, because no restrictions are put on humans, but it is also an untenable state, as goods will only be distributed through conflict. This, according to Rousseau, is not actual freedom, because one is not free from conflict nor the rules of nature. He presents civil freedom as an alternative, where some personal liberties are sacrificed in order to enable uninhibited expression of the rest of the liberties. Civil society, he claims, is the only forum in which morality and rationality can be expressed freely. But how to determine which liberties to give up and surrender to the regulation of society? This is where Rousseau presents the social contract as a solution. This imaginary contract is the "agreement" the members of a society negotiate within themselves to distribute power and enact regulation. Democracy grows out of the social contract as a method for this negotiation, and it is the nature

⁵¹ Christopher Bertram, "Jean Jacques Rousseau," Stanford Encyclopedia of Philosophy (Stanford University, 2017), <https://plato.stanford.edu/entries/rousseau/>.

of the social contract, which determines the distribution of societal goods – or at least how to determine the latter⁵²

This type of social contract theory is older than Rousseau’s work, however. Even Plato has Socrates debate the subject in *Crito* and *Republic*. Socrates stipulates the social contract indirectly by asserting that it is one’s choice to live in Athens, but if one chooses so, one must abide by the rules set by the rest of Athens through a democratic process.⁵³ Next in the historical line of major social contract philosophers is Thomas Hobbes, who lived through the English civil war and saw Oliver Cromwell lead the Parliamentarians into a fight for a more powerful parliament and less centralized, monarchic power. Being a pragmatic, Hobbes does not choose sides. Instead, he states principally that authority and obligation should be in the hands of individuals looking out for their self-interest – but as equals. Pragmatically, however, he wants the monarchy to still be in place to maintain order. The principle is a long-term goal. Hobbes was influenced heavily by the scientific revolution at the time, and thus rejected divine influences overall⁵⁴. But it took John Locke’s⁵⁵ later work to completely clear the social contract model of any religious influence. Like Hobbes, Locke works from the assumption that without civilization, the human race is left to live in a hypothetical state of nature, as described above.

⁵² Bertram.

⁵³ Plato and Jowett, “The Republic by Plato.”

⁵⁴ Stewart Duncan, “Thomas Hobbes,” Stanford Encyclopedia of Philosophy (Stanford University, 2017), <https://plato.stanford.edu/entries/hobbes/>.

⁵⁵ Patrick Connelly, “John Locke,” The internet encyclopedia of philosophy (Internet Encyclopedia of Philosophy Pub), accessed April 4, 2018, <http://www.iep.utm.edu/locke/>.

Whereas Hobbes assumes an anarchic, conflict-driven state of nature, Locke's state of nature introduces morality. Locke ascribes *a priori* morality to humans, and though his state of nature is pre-political and pre-civilization, it is not pre-moral. Morality keeps humans from unconstructive behavior, Locke argues. Thus, his state of nature is one where humans are completely free, with the only exception being the liberty to do immoral, harmful things to each other.

Locke also accepts that in the state of nature, humans are social: families are bound to each other, and this bondage is stronger than any will of the individual between them. Locke considers this a completely natural state of being. Although the characteristics of Locke's natural state is up for debate, his conjecture is important, because it provides the moral incentive for civilization and the creation of society: The social contract does not just emerge from pragmatism, it is also the most morally acceptable way of constructing a society, because it is a contract agreed upon by individuals with a natural morality. Locke is said to have had a profound influence on the founders of the United States, and in particular Thomas Jefferson.⁵⁶

This brings us back to John Rawls' revitalization of the social contract concepts of Rousseau, Hobbes and Locke.⁵⁷ Like Hobbes, Rawls argues for a very basic, natural state of being as the foundation from which society must rise. Like Locke, Rawls argues that morality must be part of the picture (although he leans towards Kantian morality of reason, rather than *a priori* morals), and like Rousseau, his aim is not hypothetical. He may employ hypotheticals to arrive at his goal, but Rawls' mission (like Rousseau's 200 years before him) is to create a

⁵⁶ Connelly.

⁵⁷ Rawls, "A Theory of Justice," VI, P. XVIII.

blueprint upon which an actual, functioning society can be based. It is somehow very fitting that Rawls embarks on his journey at a time of social injustice, as an American trying to construct a better system for America. As mentioned before, Locke’s work directly influenced, among others, Thomas Jefferson. Rousseau’s work influenced the French revolution and the establishment of a republic with a model that would become an inspiration for the founders of the United States. No wonder Rawls chose to look at the original inspirations for the American project in order to try to fix it.

The original position

Like Hobbes, Locke and Rousseau before him, Rawls assumes a “state of nature”. But for Rawls, it is more of a tool than an assumed state of pre-political being. He calls it the *original position* (OP)⁵⁸ In the OP, humans have not yet determined the rules that will make society “well-ordered” (which is another of Rawls’ concepts – see below). They are free – and most importantly, rational – beings, aware of the benefits of societal organization. Like Locke, Rawls attributes morality to humans in the original position, but it is not an *a priori* morality. Rather, it is the result of the line of reasoning which drove Immanuel Kant to establish the *categorical imperative*, first formulated thus: “Act only according to that maxim whereby you can at the same time will that it should become a universal law without contradiction”⁵⁹ Kant arrives at this “golden rule”-style formulation through a series of arguments which are not relevant here.

⁵⁸ Rawls, 18.

⁵⁹ Immanuel Kant, “Groundwork for the Metaphysic of Morals (1785),” *Practical Philosophy*, 2005, 18, <https://doi.org/10.4324/9780203981948>.

But it is important to note that Rawls assumes this morality as inherent in humans in the OP. Humans in the OP are aware of the fact that their actions must be of such a nature that anyone could act in the same manner without inflicting harm or applying discrimination. They are reasonable beings, and reasonable beings will always arrive at the categorical imperative when trying to be moral, a truly Kantian view of morality, which Rawls adopts for the humans in his OP. It is not that humans always act this way, but in the process of establishing a society built upon reason, in the original position, they are compelled to act morally by their own reason⁶⁰ Another side of this is Rawls' version of *public reason*. The concept is also present in the work of some of Rawls' biggest influencers: Hobbes, Kant and Rousseau. With the concept of *public reason*, Rawls elevates Kant's categorical imperative from the action of the individual to the justification of, e.g., regulation by the masses. By the principle of public reason, any decision which affects society, must be justified by reasoning that all the individuals in society can get behind⁶¹ That does not mean that all individuals must agree with the decision or that there must be unanimous consensus for justice to be in place. But it does mean that everyone must be able to accept the reasoning itself as being consistent and logical. Or to put it in a Kantian perspective: The reasoning behind a decision or rule which affects all who are also eligible to impact the rule or decision, must be universally applicable, or it may be deemed unjust.⁶²

⁶⁰ Rawls, "A Theory of Justice," 251.

⁶¹ Rawls, *Political Liberalism*, 31.

⁶² Rawls, "A Theory of Justice," 92.

The OP is a hypothetical tool. But Rawls bridges this hypothetical state and the empirically perceived reality by considering the concept of justice. His mission is to create a *just* society, not just an arbitrary societal model. He builds the aforementioned bridge by coupling reason-based morals with justice. Justice must be moral, otherwise it serves no purpose in an attempt to build a just society. Or to put it another way, the humans in the OP already act according to reason-based morals because they are reasonable. But the way this morality is becomes situated in the structure of a society is by expressing it as justice.

The veil of ignorance

If Rawls has contributed anything to popular discourse in the shape of terms and concepts, it is the veil of ignorance. The term is now used in many other contexts than the construction of a moral and just society. But for Rawls, it is the most essential instrument in use when creating a just society. The veil of ignorance is applied to humans in the OP as they attempt to establish manifest social norms and rules. Rawls argues that for the latter to be just and moral, one must not be able to consider any pre-existing situations, conditions or positions. When establishing society's main principles of function, it cannot matter whether the humans in the OP come from a position of wealth or poverty, nor can it matter which level of education they have. It cannot matter what their physical attributes are, both for reasons of equality in gender, race and sexual preferences, but also in a more basic sense: a large, strong person's possession of strength cannot be part of the equation. And so, Rawls suggests looking at the construction of society's

institutions through a veil of ignorance, so that humans in the original position are ignorant of any attributes or possessions which might otherwise make a difference in a state of nature⁶³

Justice as Fairness

Rawls' final book revisits *A Theory of Justice*. In it, he not only updates many of the principles set forth in his magnum opus, but he also focuses the attention given to his work on the principle which also gives the book its title: *Justice as Fairness*. Intuitively, justice seems to inhabit fairness and vice versa, but for Rawls, this is not necessarily the case. He instead *defines* justice as fairness, with fairness understood as the upholding of moral decisions and regulations by *just institutions*. These just institutions are put in place during the process (or with the tools) described above. Rawls also wrote a paper with the title *Justice as Fairness*, a 1985 article that had the following subtitle: *Political, Not Metaphysical*.

From the present discussion, the subtitle's meaning should be obvious: Rawls does not believe in a metaphysical morality from which we can establish the rules and norms that should shape our society. For him, it is a question of extracting morality from reason and the political exercise of arguing from the OP with observations through the veil of ignorance. Rawls uses the article to flesh out further what this means. He does that by introducing two additional concepts: the principles of justice as fairness. Here, Rawls breaks down his concept of justice into two principles:

1. First principle: The liberty principle, and

⁶³ Rawls, 12.

2. Second principle: The equality principle, which has two subdivisions:
 - a. Fair equality of opportunity
 - b. The difference principle⁶⁴

First Principle. The first principle is clearly inspired by Rousseau, in the sense that liberty is elevated to the highest order, but there are still limitations: “Each person is to have an equal right to the most extensive basic liberty compatible with a similar liberty for others”⁶⁵ – the last few words being the restricting factor which eventually leads to the social contract. Because of this restriction, Rawls keeps these “basic liberties” to the minimum required to participate in a just society and thereby adhere to the social contract: The right to vote, to run for office, to assemble, to free speech, liberty of conscience, as well as freedom of property and freedom from arbitrary arrest. These basic liberties echo many principles set forth in other normative lists of rights or liberties such as the UN Human Rights Charter or the US Constitution and Bill of Rights.

There are crucial and intentional omissions from the list. It is not a basic liberty to be able to own *certain* types of property, most notably means of production: “Liberties not on the list, for example, the right to own certain kinds of property (e.g., means of production) and freedom of contract as understood by the doctrine of laissez-faire are not basic; and so they are not protected by the priority of the first principle”⁶⁶ Rawls’ mentioning of “the doctrine of laissez-faire” is a

⁶⁴ Rawls, *Justice as Fairness: A Restatement*, 42.

⁶⁵ Rawls, “A Theory of Justice,” 25.

⁶⁶ Rawls, *Collected Papers*, 260.

clear rejection of libertarianism, as advocated by Rawls' academic adversary and long-time friend, Robert Nozick (more on that later).

When Rawls stops short of advocating for the basic right to own means of production and freedom of contract, it is not just a Marxian influence. It is also for logical reasons: The basic liberties are essential for the individual's societal participation and adherence to the social contract. But an individual's right to own and employ means of production, or his or her right to enter into contracts other than the social contract, are not *essential* to societal participation, and are therefore omitted. Elsewhere, Rawls also attributes two *moral powers* to individuals who fulfill their obligations as citizens through participation in upholding of the social contract. These two moral powers are the capacity for the sense of justice and the capacity for the conception of the good. The latter leads into a larger discussion of reason-based Kantian morals and their influence on Rawls which is not within the scope of this paper. The former is a capacity that is inherent in Rawls' humans in the OP – they are reasonable, and therefore able to argue for moral justice through reason. Now of course, these humans are hypothetical beings, but they serve as good illustrations, or maybe even ideal notions of how Rawls sees a citizen's ability (moral power) to recognize justice - through reasoning towards morality.

Second Principle. Fair equality of opportunity is a principle establishing a liberty of pursuit of opportunity. Without fair equality of opportunity in institutions of society, not only are these institutions not just institutions, the individual's liberty to pursue any opportunity on equal terms as those of her or his peers is also inhibited. This type of restriction of opportunities is exactly what the veil of ignorance is supposed to root out. It should be noted; that Rawls distinguishes *fair* equality of opportunity from *formal* equality of opportunity. The latter is merely the

statement of intention of equality, the former is the actual application of justice as fairness in equality of opportunities.

The *difference principle* is where Rawls becomes normative and positions himself on the political spectrum. This principle is the most contested by economists and political philosophers of all of Rawls' statements. It stipulates that "Social and economic inequalities are to be arranged so that they are to be of the greatest benefit to the least-advantaged members of society".⁶⁷ Rawls argues that through reason, humans in the OP looking through the veil of ignorance could not come to any other conclusion than the difference principle. But in theory, and as stated by many of Rawls' detractors (see below), it cannot be disregarded that humans in the OP may *not* find the difference principle to be undeniable, even when looking through the veil of ignorance. Rawls argues for the difference principle with reason as his weapon, but the result still seems more normative than necessarily logical. It is also with the difference principle in mind that Rawls can truly be called an egalitarian. The difference principle is a principle of equal liberty, because it levels the playing field and thus creates liberty of opportunity for *everyone*, at least within the frame of a well-ordered society with just institutions.

Maximin

From the difference principle, Rawls derives the concept of maximin in moral decision-making. Some scholars conflate the maximin and the difference principle⁶⁸ but there is an important

⁶⁷ Rawls, *Justice as Fairness: A Restatement*, 43.

⁶⁸ Anna Lauren Hoffman, "Beyond Distributions and Primary Goods: Assessing Applications of Rawls in Information Science and Technology Literature since 1990," *Journal of the Association for Information Science and Technology* 68, no. 7 (2017): 1601–18, <https://doi.org/10.1002/asi.23747>; Olatunji A Oyeshile, "A Critique of the

difference. Rawls described his principles of justice as having “an analogy”⁶⁹ with the maximin rule in his 1971 original of *A Theory of Justice*, but in a later edition, it was changed to the principles and the maximin rule having a “relation”.⁷⁰ In either case, it is clear that sees the difference principle as separate from, but related to, maximin. The difference principle deals specifically with the conditions under which inequalities can be decided upon in the construction of the basic structure of a just and fair society. Maximin is an ethical tool for Rawls, who emphasizes that it can be used to decide in questions emerging at a higher level of abstraction (and thus shouldn’t necessarily be used for every-day decision making.) “The maximin rule tells us to rank alternatives by their worst possible outcomes”, he writes, “we are to adopt the alternative the worst outcome of which is superior to the worst outcomes of the others”.⁷¹ It is important to note the choice of the words “worst *possible* outcomes” (emphasis mine), as this plays into the utilitarian critique of Rawls that I describe below. Utilitarians will often use the risk-averse choice of the least bad outcome against Rawls, arguing that taking a small risk is worth a substantially useful outcome. These arguments, as I show below, are often made through examples with outcomes that reasonable individuals would not consider *possible* outcomes, even without resorting to probability calculations. Maximin is certainly a more risk-averse strategy,

Maximin Principle in Rawls’ Theory of Justice,” *Humanity & Social Sciences Journal* 3, no. 1 (2008): 65–69, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.607.5171&rep=rep1&type=pdf>.

⁶⁹ Rawls, “A Theory of Justice,” 152.

⁷⁰ John Rawls, *A Theory of Justice - Revised Edition* (Belknap Press, 1999).

⁷¹ Rawls, “A Theory of Justice,” 152–53.

but as mentioned, Rawls only recommends applying it in high-concept or high-stake situations, not in everyday decision-making.

Primary goods

From Rawls' two principles of justice another list emerges. But this list is not so much a "menu" of liberties that should be available to everyone. Rather, it is a list of goods needed in order for (or at least useful for) citizens to be able to exercise the two *moral powers*⁷² which makes them just, reasonable and equal participants in a just society. Rawls calls these *primary goods* (not to be confused with *public goods*, which is dealt with below.) These are the primary goods⁷³:

- The basic rights and liberties;
- Freedom of movement, and free choice among a wide range of occupations;
- The powers of offices and positions of responsibility;
- Income and wealth;
- The social bases of self-respect: the recognition by social institutions that gives citizens a sense of self-worth and the confidence to carry out their plans.

Note that these are not basic liberties, i.e., it is not morality which dictates that they must be made available to all. The basic liberties are instead part of the list of primary goods of which some or all are essential to the participation in a just society. This is where Rawls also allows for the ownership of means of production. Primary goods are those that are *available* for those who

⁷² Rawls, *Justice as Fairness: A Restatement*, 18.

⁷³ Rawls, 58.

wish to pursue them, but except for “the basic rights and liberties,” an individual cannot claim that he or she is morally *entitled* to them. But as mentioned, it is through one or more of these primary goods that a citizen can express his or her adherence to the social contract. According to Rawls, the pursuit of primary goods in a way that is just and reasonable, is part of (and enabled by) living in a well-ordered society.

Well-ordered societies

This is a good opportunity to present Rawls’ concept of well-ordered societies. A well-ordered society for Rawls is basically a society built around the principles described above. This may seem trivial. The concept takes on more meaning, however, when Rawls extends his thinking to international politics, as he does in *The Law of Peoples*. In order for the *international* society to be well-ordered, and for the societies/peoples participating in the international society to also be internally well-ordered, they must adhere to the following eight principles:

- Peoples are free and independent, and their freedom and independence are to be respected by other peoples.
- Peoples are to observe treaties and undertakings.
- Peoples are equal and are parties to the agreements that bind them.
- Peoples are to observe the duty of nonintervention (except to address grave violations of human rights).

- Peoples have a right of self-defense, but no right to instigate war for reasons other than self-defense.
- Peoples are to honor human rights.
- Peoples are to observe certain specified restrictions in the conduct of war.
- Peoples have a duty to assist other peoples living under unfavorable conditions that prevent their having a just or decent political and social regime.⁷⁴

These principles may seem to be very obvious and almost naïve, but what Rawls provides is a rational argument for each of them - with a solid foundation in logic and reason-based morality - rather than letting them stand as mere normative statements. It is one of the achievements that makes Rawls such an important contributor to political philosophy: We do not need to rely on emotional, religious or otherwise normative notions of morality in order to understand why these principles must be in place.

Achieving a situation in which a society – local or international - is organized according to principles of reason, just political discourse within just institutions, and where public reason dominates is a state Rawls calls *reflective equilibrium*.⁷⁵ It is a sort of utopic nirvana which Rawls never expresses hope of achieving. Rather, he describes the journey towards reflective equilibrium as the iterative development that members of well-ordered societies must go through in order to achieve Rawls' notion of *distributive justice*⁷⁶ – the philosophical concept of how

⁷⁴ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 37.

⁷⁵ Rawls, "A Theory of Justice," 20.

⁷⁶ Rawls, 4.

justice is actually disseminated in society. For the members of a well-ordered society, reflective equilibrium is a state where every decision and action are grounded in reason and justice. This is also how Rawls wishes to secure stability. His concept of *overlapping consensus* addresses the matter by once again assuming rationality as a basis for morals. If, as he suggests, reason-based moral is the normative guide for a society, if its institutions are just, if public reason is in place, and if there some prevalence of reflective equilibrium among the citizens, then everyone should be able to agree on the fundamentals – but maybe for different reasons. As an example, an atheist may support freedom of religion because it is part of freedom of expression and thought, while a Muslim supports freedom of religion out of self-interest. In both cases, they would have arguments and support of a decision based on reason, but their motivations would be different. That is *overlapping consensus*⁷⁷, and for Rawls, this ensures stability, since there is agreement on the reason-based fundamentals. This is once again a display of the Kantian influence on Rawls – morality stems from reason, first and foremost.

Ideal vs non-ideal theory

Rawls is well aware that the above principles are ideals. He distinguishes between the ideal world he describes and the non-ideal world he lives in⁷⁸ but his mission is to create a theory of justice which can transfer its principles from one to the other. He sees this transfer as happening in four stages, as society builds its (just) institutions. This four-stage sequence⁷⁹ is a gradual

⁷⁷ Rawls, *Justice as Fairness: A Restatement*, 42.

⁷⁸ Rawls, “A Theory of Justice,” 8.

⁷⁹ Rawls, *Political Liberalism*, 289.

unveiling of the veil of ignorance, the first stage being observing through the veil from the original position. The second stage can be seen as constitutional: The veil is lifted enough for the parties to get an understanding of actual political culture and economic development in the environment observed, and from there, they create a constitution which applies the two principles of justice to these conditions. At the third stage, the veil is lifted even further, and can be seen as the legislative/regulatory stage. It is at this point laws and regulations are fleshed out, but still with the stated mission to uphold the two principles. Finally, at the fourth stage, the veil is completely lifted, and the criteria created in the two former stages are realized and put into action by the institutions of society, which can now be seen as just.

Rawls characterizes his model as a “realistic utopia” spurred on by political philosophy. He writes: “By showing how the social world may realize the features of a realistic utopia, political philosophy provides a long-term goal of political endeavor, and in working toward it gives meaning to what we can do today”.⁸⁰

Rawls on power

When it comes to the distribution of power and monopoly of force in society, Rawls again leans on the reasonable citizen and the Kantian notion that reason will always lead to the categorical imperative. He writes: “Our exercise of political power is fully proper only when it is exercised in accordance with a constitution the essentials of which all citizens as free and equal may

⁸⁰ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 28.

reasonably be expected to endorse in the light of principles and ideals acceptable to their common human reason”⁸¹

In other words, he once again asserts that, despite the motivations and despite whatever expression of self and self-interest any citizen has, all citizens must be able to support the reasoning behind society’s implemented institutions and principles. This also applies to power, where “free and equal” citizens can be “expected” to “endorse” the reasoning behind the distribution of power. This is yet another critique of utilitarianism from Rawls. Institutions of power/force in society may be maximized to protect and serve the biggest amount of people possible, but for Rawls, that’s not good enough. Even the marginalized few must be able to endorse the reasoning behind (and at best the manifestation of) public institutions of power. Note that the power distribution in question here is strictly *public*.

The ideal Rawlsian society will not need to consider private distribution of power, since its institutions and regulations already ensure that power from wealth, for example, is distributed (and acted upon) fairly, and the veil of ignorance ensures that the playing field is leveled before categories of non-public power are allowed to grow.

Rawls on Public Goods

A societal theory, including political economy, would not be complete without a discussion of public goods. Rawls’ theory of justice is no exception, although he stresses that his mission is not to advocate for one economic system over another based on its efficiency or growth potential, but solely judge it by its justness. By excluding ownership of means of production from the basic

⁸¹ Rawls, *Political Liberalism*, 137.

liberties, Rawls manages to take a centrist position, in which the balance of public vs private ownership can only be judged on whether a certain position on the spectrum between two extremes enables justice as fairness for the citizens or not.⁸² Rawls calls out laissez-faire capitalism as unjust (see above), but elsewhere he also sees exaggerated nationalization of the means of production as equally unjust.⁸³

Rawls acknowledges the need for public goods and presents principles which distinguish them from private goods (ownership of which, unlike ownership of means of production ARE protected by the basic liberties). These principles are clearly inspired by Samuelson's theory of public goods, as Rawls states that public goods must be characterized by indivisibility and being public in nature. Rawls' notion of "indivisibility" is comparable to Samuelson's notion of rivalry, i.e., non-rival goods being impossible to partition into pieces of exclusive ownership. Being "public in nature" is analogous to Samuelson's excludability factor.⁸⁴ To be public, according to Samuelson, a good must be non-exclusive, available to the entire public. From Rawls' viewpoint, this means that a public good is only just (and actually public) if all citizens have equal access to it "in the same amount". Rawls uses national defense as an example. For national defense to be just, it must be non-rival (for the citizens – which it is, since the "amount" of defense is not necessarily the same as the number of tanks, soldiers or drone attacks), and non-

⁸² Rawls, "A Theory of Justice," 266.

⁸³ Rawls, *Justice as Fairness: A Restatement*, 138.

⁸⁴ Rawls, "A Theory of Justice," 267.

exclusive (which it is, since every citizen is principally protected by a national defense system. If they are not, it is an unjust system built without the veil of ignorance.)

Rawls' critics

Nozick

Rawls' most famous opponent was his Harvard colleague and friend Robert Nozick, who wrote *Anarchy, State and Utopia* as a direct response to *A Theory of Justice*. Nozick argues from a libertarian standpoint, that it does not make sense to call Rawls' difference principle just at all.

For Nozick, the existence of the principle itself is unjust, since it infringes on humans' right to voluntary exchange⁸⁵ By the latter, Nozick means the free acquisition and (re)selling of private goods. As a libertarian, Nozick finds any interference with this process to be a restriction of the liberty of humans⁸⁶, and it is unimportant whether voluntary exchange results in wealth for the individual or not – it is the fact that society agrees on a restriction of the individual's liberties, which bothers Nozick. It is not that Nozick wishes for an anarcho-liberal “state of nature” instead of civilized and regulated society, but rather he argues for the *minimal state*⁸⁷

Nozick argues that the only state apparatus that can be justified is a state that only guards the very basic structures of society such as “the narrow functions of protection against force, theft,

⁸⁵ Robert Nozick, *Anarchy, State, and Utopia*, vol. 5038 (New York: Basic Books, 1974), 151.

⁸⁶ Nozick, 5038:Preface ix.

⁸⁷ Nozick, 5038:297.

fraud, enforcement of contracts”⁸⁸ Nozick also criticizes the entitlement aspect of Rawls’ difference principle. He states that there is no reasonable or just argument for why the least well-off are entitled to receive benefits from a redistribution of wealth. He accepts that social cooperation has benefits, inspired by John Locke, but does not accept that reason dictates entitlement *qua* social cooperation. Nozick eventually inches closer to Rawls in the sense that he admits that some wealth concentrations (such as those that are brought about by crime or repression of populations) are unjust and immoral. His argument, though, is that those wealth concentrations would always be a result of involuntary and unjust exchanges.

Sen

Another source of critique of Rawls comes from Amartya Sen, also one of Rawls’ Harvard colleagues. As late as in 2009, he published *An Idea of Justice*, in which he puts forth a coherent critique of Rawls, as a sort of summation of earlier writings. Sen devotes an entire chapter of the book to the critique of Rawls, which can be summed up in three main points:⁸⁹

First, Sen latches on to Rawls’ distinction between ideal and non-ideal theory, claiming that if – as in non-ideal theory – there isn’t necessarily consensus on principles of justice, Rawls’ entire theory falls apart. Sen argues that the non-ideal determines the ideal in terms of theory, and if not, the ideal theory has no meaning. Second, Sen expresses a severe skepticism towards Rawls’ four-step sequence and the transfer from the ideal to the non-ideal, in the sense that he does not

⁸⁸ Nozick, 5038:Preface ix.

⁸⁹ Sebastiano Maffettone, “Sen’s Idea of Justice versus Rawls’ Theory of Justice,” *Indian Journal of Human Development* 5, no. 1 (2011): 119–32.

take Rawls' assumption, that the parties from the OP will automatically behave according to the rules they themselves have set, for granted. Third, Sen finds it implausible that the parties in the OP would actually be guided by reason, and thinks it is much more likely that they will be guided by "parochial beliefs" as they establish the institutions and structure of society.⁹⁰

Sen additionally criticizes Rawls for applying resourcism in the sense that his focus is completely on the just distribution of resources within a fair societal structure. Sen finds this to be focusing too much on means rather than ends – more on resources than human beings. This is in line with Sen's general theory of citizens' *capabilities* being the yardstick with which we measure the justness and quality of a government or state⁹¹

Sen also replaces Rawls' veil of ignorance with an "impartial spectator" thought experiment, which meets the challenge of parochial beliefs as mentioned above and takes a slightly more utilitarian stance in the sense that he leaves it up to a population to continuously discuss the maximization of good.⁹²

Consequentialists, utilitarianists, economists and communitarians

Unsurprisingly, utilitarianists have been critics of Rawls' theories, just as he has been of theirs. Perhaps just as unsurprisingly, many of these critiques have come from economists. Kenneth Arrow was among the first to critique Rawls after *A Theory of Justice* was published. Arrow

⁹⁰ Amartya Sen, "The Idea of Justice: A Response," *Philosophy and Social Criticism* 41, no. 1 (2015): 71, <https://doi.org/10.1177/0191453714553501>.

⁹¹ Amartya Sen, "Economic Development and Capability Expansion in Historical Perspective," *Pacific Economic Review* 6, no. 2 (2001): 179–91, <https://doi.org/10.1111/1468-0106.00126>.

⁹² Sen, "The Idea of Justice: A Response."

finds that Rawls does not argue convincingly for what Arrow calls *asset egalitarianism*, i.e. that all assets and skills in society can be pooled and distributed according to principles of justice. Arrow argues that the *productivity principle*, “that an individual is entitled to what he creates”, is so “widely and unreflexibly held”⁹³ that he has had trouble explaining to students that this is not self-evident. Arrow further criticizes Rawls’ principles for being at a level of abstraction that makes them vulnerable to real-life challenges. He argues against maximin, saying it would, for example, allow medical procedures “which serve to keep people barely alive but with little satisfaction and which are so expensive as to reduce the rest of society to poverty”.⁹⁴ Arrow, seemingly ignoring the veil of ignorance concept, also point to structural inequalities “due to biological and cultural inheritance”⁹⁵ as working against Rawls’ egalitarianism.

In another contemporaneous critique against Rawls, John Harsanyi approached Rawls’ theories from the viewpoint of utilitarianism, which, according to Harsanyi, “up to now in its various forms were virtually the only ethical theory proposing a reasonably clear, systematic, and purportedly rational concept of morality”.⁹⁶ A number of European 18th- and 19th century philosophers would likely disagree politely with this statement. Harsanyi lauds Rawls’ use of the original position but writes that its usefulness “crucially depends on it being combined with a

⁹³ Kenneth J Arrow, “Some Ordinalist-Utilitarian Notes on Rawls’s Theory of Justice,” *The Journal of Philosophy* 70, no. 9 (1973): 251, <http://www.jstor.org/stable/2025006>.

⁹⁴ Arrow, 251.

⁹⁵ Arrow, 252.

⁹⁶ John C. Harsanyi, “Can the Maximin Principle Serve as a Basis for Morality? A Critique of John Rawls’s Theory,” *American Political Science Review* 69, no. 02 (June 1, 1975): 594, <https://doi.org/10.2307/1959090>.

satisfactory decision rule.” He then targets the same concept as Arrow: “Unfortunately, Rawls chooses the maximin principle”, which according to Harsanyi “cannot fail to have highly paradoxical implications”.⁹⁷ He goes on to argue that the maximin principle would have a person living in New York City decline an advantageous job offer in Chicago and take a less advantageous job in New York City instead – merely because the worst possible outcome of the flight to Chicago would be to crash and die, and the least worst outcome would be to stay in New York and live, even with a boring job. Harsanyi does not take Rawls’ criteria that outcomes must be *possible* as understood by reasonable individuals into account in his critique of maximin.

Further, Harsanyi responds to a prior critique of him from Rawls by asserting that his model of utilitarianism (which incorporates the von Neumann-Morgenstern utility functions from game theory⁹⁸) does not merely rely on a calculation of risk but employs a balancing of risk versus utility when making moral decisions, with a focus on the utility aspect. Harsanyi advocates the Bayesian school of thought (which he claims was dominant at his time of writing), which proposes expected-utility maximization for decision rules under uncertainty. He proposes that an individual’s evaluation of a given choice would be based on how high the average utility level is for society as a whole, and for the individual. In some cases, the individual will choose morally, i.e. where the average utility level is highest for society, and in other cases, a choice will be made that favors the individual’s own interests, because the average utility level is higher for the individual than for society. As mentioned, Harsanyi uses the von Neumann-Morgenstern

⁹⁷ Harsanyi, 594.

⁹⁸ John C. Harsanyi, “Normative Validity and Meaning of von Neumann-Morgenstern Utilities,” *Studies in Logic and the Foundations of Mathematics* 134, no. C (1995): 947–59, [https://doi.org/10.1016/S0049-237X\(06\)80083-2](https://doi.org/10.1016/S0049-237X(06)80083-2).

utility function theory to describe the individual's perception of the outcomes. If the outcomes are impossible to know, Harsanyi argues that the same probability should be assigned to all the outcomes when calculating average utility level. I shall return to this towards the end of the dissertation when making the case for why a Rawlsian approach is more ethical than the utilitarian approaches currently favored for decision-making in the tech industry.

Jonathan Baron⁹⁹, believes Rawls' theories are rooted too deep in what Baron calls "moral intuitions" which makes the theories prone¹⁰⁰ to failure because they could "leave us with a normative model that does not allow us to criticize and improve our intuitions"¹⁰¹ and instead, a utilitarian model is called for. Most utilitarian critiques of Rawls resemble those presented by Harsanyi and Baron¹⁰², but others are more conciliatory, either merging utilitarian systems with Rawls' conceptions of justice and good or showing how utilitarianism can provide the same kinds of justice and fairness as Rawls' contractarian deontology¹⁰³

⁹⁹ Jonathan Baron, "Nonconsequentialist Decisions," *Behavioral and Brain Sciences* 17, no. 01 (March 4, 1994): 1, <https://doi.org/10.1017/S0140525X0003301X>.

¹⁰⁰ Baron.

¹⁰¹ Baron, 22.

¹⁰² Hare, "Rawls' Theory of Justice," *The Philosophical Quarterly*, 1973, <http://www.ditext.com/hare/rawls1.html>; Leonard Choptiany, "A Critique of John Rawls's Principles of Justice," *Ethics* 83, no. 2 (January 19, 1973): 146–50, <https://doi.org/10.1086/291872>.

¹⁰³ William R. Shadish, Thomas D. Cook, and Donald T. Campbell, *Experimental and Quasi-Experimental Designs for Generalized Causal Inference* (Boston: Houghton Mifflin, 2002); Dennis C. Mueller, Robert D. Tollison, and Thomas D. Willett, "The Utilitarian Contract: A Generalization of Rawls' Theory of Justice," *Theory and Decision* 4, no. 3–4 (1974): 345–67, <https://doi.org/10.1007/BF00136654>; Will Kymlicka, "Rawls on Teleology and Deontology," *Philosophy & Public Affairs* (Wiley), accessed April 4, 2018, <https://doi.org/10.2307/2265243>; Thomas M Scanlon, "Rawls' Theory of Justice," accessed April 4, 2018, http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=5241&context=penn_law_review.

Finally, Rawls has also been met with criticism from communitarians who see Rawls as representing an overly individualistic view. A thorough review of this criticism can be found towards the end of Chapter 5, where it serves a purpose more meaningful to the discourse in this dissertation.

Rawls in information and technology literature

A full literature review of the field of ethics related to technology, information and data would take up too much space in this dissertation, as would a full review of how ethics and national security policy are related more broadly. Furthermore, such reviews would likely include too much material that is irrelevant to the argument I am presenting here. Instead, I will now focus on the literature which includes Rawlsian perspectives with regard to information and technology.

Based on her dissertation work, Anna Lauren Hoffman has provided an admirably comprehensive review of literature that uses Rawls in an information technology context.¹⁰⁴ She proposes four broad categories of work:

- (i) Rawls as a figurehead or representative of contemporary Western philosophy, in particular, social contract theory; (ii) Rawls as an oppositional figure, that is, as representative of an argument or position to be resisted; (iii) Rawls as an authority for a particular normative concept, such as the idea of procedural justice or the priority of

¹⁰⁴ Hoffman, "Beyond Distributions and Primary Goods: Assessing Applications of Rawls in Information Science and Technology Literature since 1990."

liberty; and (iv) Rawls as method, that is, as a method for reasoning about and arriving at moral rules or principles.¹⁰⁵

I find this classification highly useful, and since (iii) is the most pertinent to the concepts explored here, I will focus on that and proceed to give an overview of literature that fits within it. Rawls is used as an authority for a normative concept in different ways, but in most cases, his work is applied very concretely. A number of papers by computer scientists creating computational models and applications for legal reasoning or risk assessment have used Rawlsian principles.¹⁰⁶

Other scholars point to different Rawlsian concepts of equity and equality (such as the original position, the veil of ignorance, the difference principle and the maximin method) to argue for fair distribution of computing resources¹⁰⁷.

¹⁰⁵ Hoffman, 1605.

¹⁰⁶ Thomas F Gordon, “The Pleadings Game; Formalizing Procedural Justice,” in *Proceedings of the Fourth International Conference on Artificial Intelligence and Law*, 1993, 10–19, <https://doi.org/10.1145/158976.158978>; Ronald E. Leenes, “Burden of Proof in Dialogue Games and Dutch Civil Procedure,” in *Proceedings of the 8th International Conference on Artificial Intelligence and Law - ICAIL '01*, 2001, 109–18, <https://doi.org/10.1145/383535.383549>; Guido Governatori et al., “Variants of Temporal Defeasible Logics for Modelling Norm Modifications,” in *Proceedings of the 11th International Conference on Artificial Intelligence and Law - ICAIL '07*, 2007, 155, <https://doi.org/10.1145/1276318.1276347>; John Zeleznikow et al., “Bargaining in the Shadow of the Law-Using Utility Functions to Support Legal Negotiation,” in *Proceedings of the 11th International Conference on Artificial Intelligence and Law*, 2007, 237–46; Arno R Lodder and Aimée Herczog, “DiaLaw: A Dialogical Framework for Modeling Legal Reasoning,” in *Proceedings of the 5th International Conference on Artificial Intelligence and Law*, 1995, 146–55, <https://doi.org/10.1145/222092.222225>.

¹⁰⁷ Jon Crowcroft and Philippe Oechslin, “Differentiated End-to-End Internet Services Using a Weighted Proportional Fair Sharing TCP,” *ACM SIGCOMM Computer Communication Review* 28, no. 3 (1998): 53–69, <https://doi.org/10.1145/293927.293930>; Božidar Radunović and Jean Yves Le Boudec, “A Unified Framework for Max-Min and Min-Max Fairness with Applications,” *IEEE/ACM Transactions on Networking* 15, no. 5 (2007): 1073–83, <https://doi.org/10.1109/TNET.2007.896231>.

In a similar fashion, these principles are used by some to argue for equity/equality in access to technology and/or information¹⁰⁸ The above-mentioned work by Hoffman belongs in this group, as she critiques Google Books from a sociotechnical standpoint, using Rawls to point out issues relating to justice, equality and self-respect within the service. Á propos equity/equality, Lievrouw and Farb¹⁰⁹ make an important distinction between the two, proposing the use of the former when discussing larger issues of fairness and justice, and limiting the use of the latter for situations where the discussion revolves around something of which equal amounts can actually be distributed. They point to Rawls and, in particular his long-time discourse partner Amyarta Sen, for conceptualizations of equity versus equality. Van den Hoven and Rooksby¹¹⁰

¹⁰⁸ Don Fallis, "Social Epistemology and Information Science," *Annual Review of Information Science and Technology* 40 (2006): 475–519; Don Fallis, "Information Ethics for Twenty-First Century Library Professionals," *Library Hi Tech* 25, no. 1 (2007): 23–36; Don Fallis and Dennis Whitcomb, "Epistemic Values and Information Management," *Information Society* 25, no. 3 (2009): 175–89, <https://doi.org/10.1080/01972240902848831>; Peter Drahos, "A Philosophy of Intellectual Property, Dartmouth," *Aldershot, UK and Brookfield, US*, 1996; Utpal Bose, "An Ethical Framework in Information Systems Decision Making Using Normative Theories of Business Ethics," *Ethics and Information Technology* 14, no. 1 (2012): 17–26, <https://doi.org/10.1007/s10676-011-9283-5>; Alistair Duff, "Neo-Rawlsian Co-Ordinates: Notes on A Theory of Justice for the Information Age," *International Review of Information Ethics* 6 (2006): 12, <http://fiz1.fh-potsdam.de/volltext/ijie/07243.pdf>; Thomas B. Hodel-Widmer, "Designing Databases That Enhance People's Privacy without Hindering Organizations," *Ethics and Information Technology* 8, no. 1 (2006): 3–15, <https://doi.org/10.1007/s10676-006-9105-3>; M J Wolf and F S Grodzinsky, "Good/Fast/Cheap: Contexts, Relationships and Professional Responsibility During Software Development," in *Proceedings of the 2006 ACM Symposium on Applied Computing*, 2006, 261–66, <https://doi.org/http://doi.acm.org.library.capella.edu/10.1145/1141277.1141339>; H Misra, "E-Governance and Millennium Development Goals: Sustainable Development Perspective in Rural India," in *ACM International Conference Proceeding Series*, 2012, 354–64, <https://doi.org/10.1145/2463728.2463796>; Kay Mathiesen, "The Human Right to a Public Library," *Journal of Information Ethics* 22, no. 1 (2013): 60–79, <https://doi.org/10.3172/JIE.22.1.60>.

¹⁰⁹ Leah A. Lievrouw and Sharon E. Farb, "Information and Equity," *Annual Review of Information Science and Technology* 37, no. 1 (January 31, 2005): 499–540, <https://doi.org/10.1002/aris.1440370112>.

¹¹⁰ Jeroen Van den Hoven and Emma Rooksby, "Distributive Justice and the Value of Information: A (Broadly) Rawlsian Approach," in *Information Technology and Moral Philosophy*, ed. Jeroen Van Den Hoven and John Weckert (New York: Cambridge University Press New York, NY, 2008).

have made one of the most compelling arguments for considering information a Rawlsian primary good alongside liberty, health etc., but in the following chapters, I will rely mostly on Rawls' own statements with regard to fair access to information needed for democratic participation and social cooperation. Some authors have discussed normative concepts through Rawls related to the Internet and its applications specifically.¹¹¹ There has also been work done on how Rawls' writings on civil disobedience applies to the digital realm¹¹²

Introna¹¹³ and Palm¹¹⁴ both use Rawls in discussions of surveillance, with a focus on the workplace. Several other scholars have used Rawls in a privacy/surveillance context, but because this is so intrinsic to the discussions in this dissertation, I will provide a more in-depth review of this literature in Chapter 5.

¹¹¹ T Hausmanninger, "Controlling the Net: Pragmatic Actions or Ethics Needed?," *International Review of Information Ethics* 1, no. 6 (2004): 19–28, http://container.zkm.de/ijie/ijie/no001/ijie_001_04_hausmanninger.pdf; Johnny Hartz Søraker, "The Role of Pragmatic Arguments in Computer Ethics," *Ethics and Information Technology* 8, no. 3 (2006): 121–30, <https://doi.org/10.1007/s10676-006-9119-x>; Bay, "The Ethics of Psychometrics in Social Media: A Rawlsian Approach."

¹¹² Kristin R. Eschenfelder, Robert Glenn Howard, and Anuj C. Desai, "Who Posts DeCSS and Why?: A Content Analysis of Web Sites Posting DVD Circumvention Software," *Journal of the American Society for Information Science and Technology* 56, no. 13 (2005): 1405–18, <https://doi.org/10.1002/asi.20234>; Bay, "The Ethics of Unbreakable Encryption: Rawlsian Privacy and the San Bernardino iPhone."

¹¹³ Lucas D. Introna, "Workplace Surveillance, Privacy and Distributive Justice," *ACM SIGCAS Computers and Society* 30, no. 4 (2000): 33, <https://doi.org/10.1145/572260.572267>.

¹¹⁴ Elin Palm, "Securing Privacy at Work: The Importance of Contextualized Consent," *Ethics and Information Technology* 11, no. 4 (2009): 233–41, <https://doi.org/10.1007/s10676-009-9208-8>.

Chapter 3: Disinformation campaigns on social media

This chapter contains a case study of an offensive and aggressive foreign policy in the shape of information warfare operations on social media. The case studied is the influence campaign waged by Russian operatives in connection with the 2016 Presidential election in the United States. As described above, the method involves defining the policy frames (Rhetorical / Action) that constitutes the policy in frame-critical methodology terms. First, I shall present how Russia's policy in this matter has emerged through these two types of frames, and second, I will discuss how the policy frames interact with the Rawlsian Frame.

Background

On September 11, 2014, residents of St. Mary's Parish in Louisiana began receiving disturbing text messages around 8:30 in the morning: "Toxic fume hazard warning in this area until 1:30PM. Take shelter. Check Local Media and columbiachemical.com." Twitter was flooded with messages about a powerful explosion that had happened at the Columbian Chemical (with an n) plant in Centerville, not too far from St. Mary's Parish. Calls began coming in to the local Homeland Security and Emergency Preparedness office – who had no knowledge of such an explosion. A YouTube video claimed that ISIS had claimed responsibility for the attack. A screenshot of CNN's homepage with the Louisiana explosion in the headline began to circulate. Obviously, local residents who had their Twitter and Facebook accounts as well as their text apps on their mobile phones flooded with this content, began to panic. But no explosion had occurred. It was merely an elaborate prank, played by the Russian influence campaign operatives at the

Internet Research Agency in St. Petersburg.¹¹⁵ This was one of the early attempts at disruption, degrading trust in the authorities and spreading a general sense of fear, distrust and chaos performed by the same Russian operatives who would later move to influence the U.S. presidential election in 2016. It was a trial run for what was to come two years later.

At the time of writing, the Russian influence campaign of 2016 has been part of the news cycle for more than a year and has been the subject of congressional inquiries, intelligence agency investigations and caught the attention of special counsel Robert Mueller in his investigation of the Trump campaign's ties to Russia. The latter led to the Department of Justice indicting 13 Russian citizens on counts of conspiracy to defraud the United States and commit bank or wire fraud. The indictments represented an acknowledgment that the U.S. now officially believed that Russian operatives attempted to interfere with the 2016 elections. The events has led to further attention being paid to the advertising practices of social media platforms such as Facebook, who would first admit to letting Russian operatives post false advertisements on the platform and later would concede that their former advertising practices had given data collection companies the ability to collect information about at least 87 million people, though the data collectors had only obtained direct consent from less than 300,000 users.

These events have pushed the world's largest social media platform into a crisis in which its market value has dropped substantially and attitudes have turned against it. Throwing a tech giant like Facebook off balance and having some amount of impact on a U.S. presidential election are not small tasks. That both were accomplished by a small group of people in St.

¹¹⁵ Adrian Chen, "The Agency," The New York Times Magazine, 2015, <https://www.nytimes.com/2015/06/07/magazine/the-agency.html>.

Petersburg, Russia without ever setting foot in the United States is hard to believe. But it becomes easier to believe when venture back into Russian history and look at its centuries-long tradition for political deception, a craft honed especially during the Soviet era. I shall return to the cultural aspects that inform the Russian disinformation and deception tactics after constructing the Rhetorical and Action Frames for this aggressive, offensive foreign policy for social media. But to truly unpack the motivations behind the implementation of such a policy, I will now relay a history of these tactics as we have observed them in recent years, collectively known as “Active Measures”

A history of Active Measures

“Disinformation has always played a part in Soviet policy” the Soviet defector Ilya Dzhirkvelov wrote in 1987.¹¹⁶ Dzhirkvelov was one of the KGB’s most senior disinformation operatives and his memoirs, along with the work of Lawrence Bittman¹¹⁷ and the Mitrokhin archive¹¹⁸ are seen as some of the most authoritative sources on Soviet disinformation tactics during the Cold War by, among others, independent military researchers¹¹⁹, the intelligence community¹²⁰, the U.S.

¹¹⁶ Milad Dehghani and Mustafa Tumer, “A Research on Effectiveness of Facebook Advertising on Enhancing Purchase Intention of Consumers,” *Computers in Human Behavior* 49 (2015): 597–600, <https://doi.org/10.1016/j.chb.2015.03.051>.

¹¹⁷ Ilya Dzhirkvelov, *Secret Servant My Life with the KGB and the Soviet Elite* (London: Collins, 1987), 301.

¹¹⁸ Ladislav Bittman, “The Use of Disinformation by Democracies,” *International Journal of Intelligence and CounterIntelligence*, 1990, <https://doi.org/10.1080/08850609008435142>.

¹¹⁹ Vasili Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officers Handbook* (Routledge, 2013).

¹²⁰ Jeremy Azrael, “The KGB in Kremlin Politics,” 1989.

Army¹²¹ and the U.S. Navy¹²² According to Dzirkhvelov, disinformation was already a widely used strategy, but became more pervasive in 1947, when the Information Committee was set up by Soviet leadership:

The Committee organized a disinformation service, known as the Fifth Information Directorate, headed by Colonel Grauer. Its business was the preparation of disinformation material and the spreading of false rumors aimed at destabilizing the position of unwanted regimes and governments. Later it was given additional functions, such as the organization of sabotage, the incitement of disorder and other actions to undermine the stability of countries in the West and the Third World. Today, every KGB *rezidentura* includes a representative of this department.¹²³

A *rezidentura* was the representation of the KGB present at Soviet embassies across the globe (Dzirkhvelov writes this in 1987, before the end of the cold war, when the KGB was still active). Note that the Fifth Information Directorate, though working with the KGB, was set up by the Central Committee of the Soviet Union, and thus carried out disinformation orders coming directly from Soviet leadership. The KGB had its own disinformation group, known as Department D, located in the First Chief Directorate of the Soviet intelligence service. Likewise,

¹²¹ Thomas Boghardt, "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence* 53, no. 4 (2009).

¹²² Daniel T. Bolger, "Book Review: Guerrilla Warfare and Counterinsurgency: U.S.-Soviet Policy in the Third World.," *Parameters - US Army War College Quarterly*, no. June (1990).

¹²³ Boleslaw A Boczek, "Resource Rivalry in the Third World," 1984.

there was a disinformation group working within the Soviet Foreign Ministry and several groups were working inside news agencies such as TASS and Novosti. These groups were independent from the KGB organizationally, but worked in coordination with them and the Central Committee. Prior to 1947, the Soviet Union also engaged in disinformation campaigns and information warfare, and even before its formation, during World War I, information warfare was a factor:

Going back to the time around World War I, these information operations were centered around radio and correspondents for newspapers. Back then, people had blind faith in newspaper and saw newspaper editors as being at the same level as high-level elected officials, making the ability to influence much larger.¹²⁴

With the proliferation of electronic mass media that happens in the 1950s, and 1960s, however, the Soviet Union identified a way to proliferate disinformation in a more decentralized manner. Both Barron¹²⁵ and Dzhirkvelov trace the establishment of Department D to 1959.

Thomas Elkjer Nissen, a military analyst at the Danish Defence College, is the author of *#TheWeaponizationOfSocialMedia*, one of the few textbooks on social media warfare that has since been added to syllabi at several U.S. military school. In an interview for this dissertation, Nissen says Russian influence campaigns are “cleansed of all ideology”, in contrast to the

¹²⁴ Dzhirkvelov, *Secret Servant My Life with the KGB and the Soviet Elite*, 301.

¹²⁵ Thomas Elkjer Nissen, “Interview, May 31” (Copenhagen, Denmark, 2017).

original emergence of Active Measures, which was directly motivated by, in Dzhirkvelov's words, the "heating up" of the "ideological struggle" with the West:

Counter-propaganda alone could not produce the desired ideological and political results; we needed new kinds of campaign against bourgeois ideology and its attacks on the socialist system. Active measures were to be taken to anticipate political and ideological acts... We would have not only to reply to the West's anti-Soviet attacks as we had done in the recent past, but to take steps to manipulate public opinion in the West, primarily in the United States, in matters of domestic and foreign policy.¹²⁶

From Disinformation to Active Measures: Taking down Franz Josef Strauss

More deliberate, strategic disinformation campaigns were now put in place, which, according to Dzhirkvelov had an early success in the resignation of the German Defense Minister, Franz-Josef Strauss, in 1962. The Strauss resignation is analogous to contemporary situations caused by Russian Active Measures and serves as a prime example of not only the how the Soviet Union viewed the ideological struggle at the time, but also of how they viewed mass media as an instrument as powerful as conventional weapons of armed conflict.

Alexei Adzhubei was the editor-in-chief at *Izvestia* in the 1960s, but he was also General Secretary Khrushchev's son-in-law, and a close advisor of the Soviet leader¹²⁷ In 1960, Dzhirkvelov had a conversation with Adzhubei about the emergence of West Germany as a power factor in Europe, particularly as a threat to the Soviet Union's allies in East Germany.

¹²⁶ John Barron, "KGB," in *The Penguin Book of Lies*, ed. Hodder and Stoughton (Penguin, 1974), 420–23.

¹²⁷ Dzhirkvelov, *Secret Servant My Life with the KGB and the Soviet Elite*, 288.

Adzhubei said “the Soviet leaders considered that the most dangerous people in West Germany were Strauss, the Minister of Defence, and the press magnate Axel Springer, because one had the weapons and the other the mass media”. Thus, the Soviet leadership considered the media as an equal or almost-equal threat to their dominance in Eastern Europe as conventional weapons. Adzhubei went on to describe two strategies in which the Soviet Union’s influence on Germany could be increased. One was through the potential reunification of East and West Germany, through which Khrushchev apparently saw an opportunity to draw West Germany closer to the Soviet Bloc ideologically, as a reunification would mean an influx of East German communist influencers into the West German political infrastructure. Prior to 1960, Khrushchev was apparently ready to support a reunification on certain terms because of this.

The other strategy, which ended up being attempted, was to influence both the West German decision-makers and the country’s populace through information operations, thereby drawing them closer to their East German neighbors, and ideologically closer to the Soviet Union. This strategy entailed “distancing West Germany from the United States”.¹²⁸ One operation conducted as part of this strategy was the *Spiegel* affair that eventually led to the above-mentioned resignation of West German Defense Minister Franz-Josef Strauss.

Dzhirkvelov describes how he was approached by Boris Ponomarev regarding a visit to Moscow by a group of West German journalists planned for May 1961. Ponomarev was the head of the International Department of the Central Committee of the Communist Party of the Soviet Union, and in charge of coordinating with communist parties around the world, particularly in nations

¹²⁸ Jeanne Vronskaya, “Obituary: Alexei Adzhubei,” *The Independent*, 1993, <http://www.independent.co.uk/news/people/obituary-alexei-adzhubei-1499406.html>.

allied with the Soviet Union, and thus a very powerful figure in the Soviet leadership.

Dzhirkvelov was designated to play host to the West German journalists, which entailed attempts at influencing them. Ponomarev told Dzhirkvelov to relay a message to the journalists that despite any official, more diplomatic lines, “we regard Adenauer [Chancellor of West Germany at the time] as a politician whose days are numbered, and Strauss as a follower of Hitler and as a revanchist who is harming the whole of Europe by his actions.”¹²⁹ Later, this was followed up by Ivan Agayants, the head of the disinformation-focused Department D at the KGB, who ordered Dzhirkvelov to

...hint that we have information concerning Strauss’s connections with the American intelligence service. Tell them they recruited him when he was in prison and that he now receives huge sums of money for the services he rendered them. He is more concerned with increasing his personal fortune than with a peaceful future for Germany. If you are asked what proof you have, you can say that we even have *documentary* proof, but that you can produce it only on the condition that it will be published in the West German press without the source being revealed.¹³⁰

Dzhirkvelov’s message to the West German journalists was part of a larger KGB effort to discredit Strauss by alleging corruption and inappropriately close ties to the U.S. intelligence community. The strategy was successful in increasing the attention paid by the West German

¹²⁹ Dzhirkvelov, *Secret Servant My Life with the KGB and the Soviet Elite*, 293.

¹³⁰ Dzhirkvelov, 293.

press to Strauss' actions. On May 31st, 1961, only days after the West German journalists had visited Moscow, *Der Spiegel* reported that Strauss had recommended to U.S. Secretary of Defense Thomas Gates that a contract for building 5,424 apartments as housing for U.S. military personnel in Germany should be awarded to the company FIBAG. One of that company's largest shareholders was Hans Kapfinger, a close friend of Franz-Josef Strauss, and the article hinted at accusations of corruption. A government-led investigation later cleared Strauss of any wrongdoing (and the contract eventually went to a different company).

The relationship between Strauss and *Der Spiegel* was already strained because of a 1959 article, in which the West German Ministry of Defense's decision to purchase of 300 Lockheed F-104 "Starfighter" jets was questioned. The article pointed to the lack of documentation and reasoning given by the West German government in choosing the Lockheed jets over jets from the French company Dassault or Lockheed's American competitor, Grumman.¹³¹ Lockheed was suspected of offering large bribes to government officials around the world in exchange for similar contracts, something that the company later admitted to.¹³² These hints of corruption in *Der Spiegel* allegedly put Strauss personally at odds with the founder and editor-in-chief at *Der Spiegel*, Rudolf Augstein. Consequently, when *Der Spiegel* in October 1962 published an assessment of the German armed forces from the NATO high command which deemed the

¹³¹ Dzhirkvelov, 298.

¹³² Staff, "RÜSTUNGS-AUFTRÄGE: Kalifornische Preise," *Der Spiegel*, 1959, <http://www.spiegel.de/spiegel/print/d-42624035.html>.

forces only “partially ready”¹³³ to defend the country, Strauss reacted by claiming *Der Spiegel* had published classified information and had the article’s authors, Conrad Ahlers and Hans Schmelz arrested – alongside Rudolf Augstein. This was seen as an attack on the freedom of the press and caused massive outrage in West Germany, causing several elected officials to resign, not least Franz Josef Strauss himself. A year later, it also forced Chancellor Konrad Adenauer to resign before the end of his term.¹³⁴

The KGB saw the fall of Strauss and later Adenauer as one of their first big achievements using Active Measures. As with most information warfare, it is difficult to attribute a causal effect to their efforts, but as Dzhirkvelov writes:

Although there can be no doubt at all that the anti-Strauss campaign in *Der Spiegel* was launched on the basis of KGB-planted material, this, of course, does not imply any collaboration between the KGB and *Der Spiegel*, many respectable and politically impeccable publications fell victim to the KGB ‘active measures’ without knowing by whom they had been used.

An example of similar Active Measures in the U.S. Presidential Election of 2016

The events that led to Strauss’ resignation are analogous to events that occurred during the 2016 U.S. presidential election. Though not as high-ranking as Strauss, the Chairwoman of the Democratic National Committee, Debbie Wasserman-Schulz was forced to resign due to e-mails

¹³³ Staff, “SCANDALS: Lockheed’s Defiance: A Right to Bribe?,” *Time Magazine*, 1975, <http://content.time.com/time/subscriber/article/0,33009,917751-1,00.html>.

¹³⁴ Cristoph Gunkel, “50th Anniversary of the SPIEGEL Affair - SPIEGEL ONLINE,” *Spiegel Online*, 2012, <http://www.spiegel.de/international/germany/50th-anniversary-of-the-spiegel-affair-a-857030.html>.

published by DCLeaks and WikiLeaks who obtained them from Russian hackers allegedly working for the Russian state.¹³⁵ The DNC officials directly implicated in the e-mails were also forced to resign, although no criminal wrongdoings had taken place. Instead the controversy centered on the fact that some of the e-mails could be interpreted as if the DNC deliberately tried to work against the campaign of one of the Democratic Party's primary electoral candidates, Senator Bernie Sanders. The resignations thus came due to the public outrage that followed the publication of the e-mails, and the scandal added to a growing suspicion of corruption in the DNC and the Clinton campaign which was already circulating in the press. In this manner, Russian operatives, just as in the Strauss example, was able to proliferate information that didn't necessarily in itself incriminate anyone, but its suggestive power was enough to cause perceptions to shift and political disruptions to occur.

In the latter case, it is important to distinguish between the two types of interventions that Russia is accused of with regards to the U.S. presidential election in 2016. One is a specific cyberattack with the specific purpose of collecting useful intelligence. This is the so-called "DNC Hack", which originated as a spear-phishing attack on one of Hillary Clintons closest aides, John Podesta. By obtaining the password to Podesta's private e-mail account, the allegedly Russian-backed hacker groups known in the intelligence and cybersecurity communities as APT27 and APT28, or Fancy Bear and Cozy Bear, were able to make further penetrations into

¹³⁵ Gunkel.

the Democratic National Committee's e-mail systems and obtain the e-mails mentioned above.¹³⁶

This is separate from the influence operation that had been ongoing since 2014 and gained steam during the election in 2016. The content pulled from the DNC hack, as well as news stories generated from it, became an important part of the influence campaign, however. But they are still two different types of operations, one being a more traditional cyberattack and the other an information (warfare) operation. This chapter is focused on the latter.

The adoption of a foreign policy in which information warfare is waged is a serious matter. In the acrimonious atmosphere of the cold war, it was not surprising to see Active Measures being employed and acts of information warfare having a great impact. The U.S. would retaliate with equally effective means during that time, both the Soviet Union and the U.S. were very clear about their adversarial policies towards each other. Since the fall of the Soviet Union, there has been no such adversarial policies put forward that were directly targeting U.S. or Russian interests – until the influence campaign of 2016 and the events that preceded it, going back to the fake Columbian Chemicals explosion on September 11, 2014. Russia, with a GDP roughly the size of Italy's, cannot afford the retaliations that would follow an act of kinetic (i.e. physical) aggression targeting U.S. interests. You don't have to look far, however, to see the contours of a policy that attempts to portray Russia as a victim of cultural and political aggression that would justify aggressive tactics such as the influence campaign of 2016. In the

¹³⁶ Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

next section, I will exhibit examples of the political rhetoric that lays the foundation for such a justification, and the policy that emerges from it.

Rhetorical Frame

In this section, I will present three instances in which the policy emerges from a rhetorical standpoint in order to establish the Rhetorical policy frame.

Russia has not officially acknowledged its use of disinformation, on social media or elsewhere, as a political tool, nor has it officially recognized disinformation as a valuable or morally valid tactic. There are, however, instances in official policy documents that collectively create a space in which such a policy can exist, which in turn adds to the validity of the claims that constitute the action frames described below.

The Information Security Doctrine

One such instance is the official information security strategy of the Russian Federation, which was updated in 2016.¹³⁷ Officially named the *Doctrine of Information Security of the Russian Federation*, the document outlines mostly the defensive strategy for Russia's national information security interests, but there are elements that point to a more offensive strategy, and which can be interpreted as an opening towards Active Measures-type operations that include participation from private organizations and citizens.

¹³⁷ Office of the Director of National Intelligence.

An example is “societal mobilization”¹³⁸, a central part of the doctrine. In the strategy, the Russian Federation includes citizens and private organizations as part of the “institutional framework” that regulates the “information security system”:

V. Institutional Framework of Information Security

30. The information security system is part of the broader national security system of the Russian Federation. Information security is ensured through the combination of legislative, law enforcement, judicial, oversight and other activities of government bodies working in cooperation with local governments, organizations and citizens.

This first part of the description of the institutional framework is noteworthy for its absolute inclusion of the information security system in the national security system and the inclusion of “organizations and citizens” in the information security efforts. It is noteworthy, because this clause in no uncertain terms states that citizens and organizations cooperating with the government is part of the *national* information security effort. It can be read as a way to make sure the private sector does its part to secure information of vital national importance, but at the same time, it opens up for the type of collaborations that the U.S. intelligence community identified in the disinformation campaigns, e.g. non-state actors committing international hacking offenses in collusion with the Russian government.¹³⁹

¹³⁸ Russian Federation, “Doctrine of Information Security of the Russian Federation,” *The Ministry of Foreign Affairs of the Russian Federation*, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICk6BZ29/content/id/2563163.

¹³⁹ Olikier Olga, “Unpacking Russia’s New National Security Strategy,” Center for Strategic and International Studies, 2016, <https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy>.

The Russian Federation's involvement of private entities in its national information security strategy becomes even clearer in the doctrine's list of components in the "information security system":

The information security system includes the following actors: owners of critical information objects and organizations operating such objects; mass media and mass communications; monetary, foreign currency, banking and other financial institutions; telecommunication operators; information system operators; organizations that create and operate information and communications systems; organizations that develop, produce and operate information security means; organizations that provide information security services; organizations that provide education services in this sphere; public associations and other organizations and individuals involved in information security under the laws of the Russian Federation.¹⁴⁰

This clause includes almost every single element of civil society in Russia and merges the cyber- and information security spheres into one, something that is not necessarily an obvious choice, as there are differences between the two.¹⁴¹ The clause is a catch-all for computing technology, information systems, networks and people. This is not in itself decidedly controversial, but Russia distinguishes itself from other nations, however, by centralizing control:

¹⁴⁰ Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections."

¹⁴¹ Russian Federation, "Doctrine of Information Security of the Russian Federation."

32. The structure of the information security system is determined by the President of the Russian Federation.

In other words, the doctrine gives President Putin himself full control over the “structure” of the information security system, notably without defining what “structure” means in this case. But it does make it clear that the President of the Russian Federation has personal control over essential aspects of how almost any private entity enacts information security measures in Russia. Again, this justifies the type of collaboration with black hat hackers and other cybercriminals that some scholars believe are the active elements in Russia’s disinformation campaigns. It creates a space for offensive information- or cyberwarfare operations or counterintelligence activities conducted by private citizens as part of a larger, defensive information security strategy – directed by the president himself.

The doctrine does emphasize the right to legal information access for its citizens but does not define what constitutes legality in the cooperation between private entities and the state in the effort to uphold information security. In the doctrine, the Russian Federation also commits itself to the international rule of law when it comes to information security:

Information security activities of government bodies is based on the following principles:

- a. the legality of public relations in information sphere and the legal equality of all participants of such relations arising from the constitutional right of citizens freely to seek, receive, transmit, produce and disseminate information in any legal manner;
- b. constructive interaction between government bodies, organizations and citizens in dealing with information security tasks;

- c. maintaining a balance between citizens' demand for the free exchange of information and restrictions related to national security, including in information sphere;
- d. the adequacy of information security forces and means determined, inter alia, through constant monitoring of information threats;
- e. compliance with the universally recognized principles and norms of international law, international treaties to which the Russian Federation is a party and laws of the Russian Federation.

But at the same time, the doctrine emphasizes that the “universally recognized principles and norms of international law” mentioned in e. don’t really exist:

Given the current global distribution of resources required to ensure safe and steady functioning of the Internet, it is not possible to manage them jointly in a fair and trust-based manner. The absence of international legal norms regulating inter-State relations in the information space, as well as mechanisms and procedures for their application that would take into account the specifics of information technologies makes it difficult to create an international information security system designed to achieve strategic stability and equitable strategic partnership.

Russia thus distances itself from international cooperation on Internet governance in the doctrine, directly calling it impossible to establish a “fair and trust-based” governance. By doing so, it releases itself from any norms or sets of ethics promoted by the international community, again opening a space of justification for independent action based on its own rules and values.

In fact, values are an intrinsic part of the doctrine, which makes the doctrine an even more intriguing document, at least compared to other national security strategies of the same sort from other countries. Aligning perfectly with the Russian tradition of isolation and keeping outsiders at bay described further down in this text, the doctrine states:

There is a growing information pressure on the population of Russia, primarily on the Russian youth, with the aim to erode Russian traditional spiritual and moral values.

And:

There is a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation. Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented from performing their professional duties.

The doctrine does not provide evidence of either claim, nor does it define what Russian, traditional, spiritual and moral values are under threat. In conjunction with the control over the “structure” of the information system given to the President of the Russian Federation in the doctrine, it becomes possible for the government to define these values and threats without any contradiction. Russia thus also sees itself as a victim of what the west is accusing it of, and the doctrine furthers the image of Russia as being under threat from other states with regards to information security:

Intelligence services of certain States are increasingly using information and psychological tools with a view to destabilizing the internal political and social situation in various regions across the world, undermining sovereignty and violating the territorial

integrity of other States. Religious, ethnic, human rights organizations and other organizations, as well as separate groups of people, are involved in these activities and information technologies are extensively used towards this end. Information security in the sphere of strategic stability and equitable strategic partnership is characterised by the desire of individual States to use their technological superiority to dominate the information space.

The doctrine is not alone in perpetuating this notion among policymakers in Russia. Another important document in this regard is the so-called Gerasimov Doctrine.

The Gerasimov Doctrine

The article “The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations” published in 2013 the Russian military journal *Voyenno-Promyshlenny Kurier*¹⁴² is perhaps one of the most misunderstood and misquoted documents when it comes to understanding the elements of current, Russian national security strategies. It was written by Vasily Gerasimov, who at the time was Chief of the Russian General Staff, a position similar to heading the U.S. Joint Chiefs of Staff, but with much more authority and power.¹⁴³ Gerasimov’s thoughts on current conflict situations and military solutions thus carried a lot of weight, and perhaps that is why many overinterpreted the article.

¹⁴² Bay, “What Is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era.”

¹⁴³ Charles K Bartles, “Getting Gerasimov Right,” *Military Review*, no. January-February (2016), http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf.

Media misrepresentations of the article include a January 2018 segment of CBS news' 60 Minutes in which journalist Lesley Stahl interviews the editor-in-chief of the Russia Today (RT) TV news channel¹⁴⁴, articles in *POLITICO Magazine*¹⁴⁵, *Mother Jones*¹⁴⁶ and perhaps most influentially, in *The New Yorker*¹⁴⁷. The content of the article is usually referred to as defining "The Gerasimov Doctrine", which supposedly is a strategy adopted by Russia that includes so-called "Hybrid Warfare":

The article identified and urged the adoption of a Western strategy that involved military, technological, media, political, and intelligence tactics that would destabilize an enemy at minimal cost. The strategy, which came to be known as "hybrid war," was an amalgam that states have used for generations, but the text took on the status of a legend and is now known in international military circles as the Gerasimov doctrine.¹⁴⁸

The Gerasimov article thus impacted the discourse on Russian information warfare and their impact on the U.S. election in 2016. It likely also was very impactful among Russian military

¹⁴⁴ Bartles.

¹⁴⁵ Lesley Stahl, "RT's Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda," CBSnews.com, 2018, <https://www.cbsnews.com/news/rt-editor-in-chief-on-election-meddling-russian-propaganda-label/>.

¹⁴⁶ Molly K. McKew, "The Gerasimov Doctrine," *POLITICO Magazine*, 2017, <https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538>.

¹⁴⁷ Hannah Levintova, "The US Military Is Set to Meet With the Russian General Who Called For Cyberattacks Against the West," *Mother Jones*, 2018, <https://www.motherjones.com/politics/2018/01/the-us-military-is-set-to-meet-with-a-prominent-russian-booster-of-cyberattacks/>.

¹⁴⁸ Evan Osnos, David Remnick, and Joshua Yaffa, "Trump, Putin, and the New Cold War," *The New Yorker*, 2016, <https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war>.

strategists, but for completely different reasons – and this is why it deserves to be considered as part of the rhetorical frame. Since the publication of The New Yorker article, the idea that the so-called Gerasimov doctrine contains anything new in terms of Russian national security strategies or innovations in warfare has been rejected, even by scholars from the U.S. military and the American international relations research community. According to Bartles¹⁴⁹:

Probably the most misunderstood aspect of Gerasimov’s article is the idea of “indirect and asymmetric methods” that has been interpreted by the West as hybrid war. Of note, there is a general consensus in Russian military circles that hybrid war is a completely Western concept as no Russian military officer or strategist has discussed it, except to mention the West’s use of the term, or to mention the West’s use of hybrid warfare against Russia. The Russian military has been adamant that they do not practice a hybrid-war strategy. Moreover, there have been many Russian commentaries that state this concept is nothing new, that the aspects of hybrid war mentioned by Western analysts have been practiced since warfare began.

Bartles, as well as Giles¹⁵⁰, both argue that Gerasimov’s article mostly describes the *threat* to Russia, rather than Russia’s own intentions. When it was first published, Western analysts and media outlets put Gerasimov’s article in the context of Russia’s interventions in Ukraine and the Crimean Peninsula, but as the influence operations of the 2016 presidential election in the U.S.

¹⁴⁹ Osnos, Remnick, and Yaffa.

¹⁵⁰ Bartles, “Getting Gerasimov Right.”

became apparent, the narrative of Gerasimov as the mastermind behind Russia's information operations was once again promoted. But, as Thomas Elkjer Nissen of the Royal Danish Defence Academy stated: "I am of the persuasion that what we see emerge from the Russian Federation today is methodologically and doctrinally exactly the same as what we saw during the Cold War on the part of the KGB. The same techniques and methods are being used, and the same framework of concepts is being applied. They have just been brought into the 21st century through digitization, which makes them easier to carry out by several degrees. It has become much easier to erase the attribution chain, too, and more money is being invested in the efforts"¹⁵¹

Nissen is backed up by Giles, who writes, with direct reference to the misperception that what Gerasimov described in his article was a new strategy for Russia:

Nevertheless, the techniques and methods displayed by Russia in Ukraine have roots in traditional Soviet approaches. Since the end of the Cold War, Russia's military academics have displayed an unbroken and consistently developing train of thought on the changing nature of conflict and how to prevail in it, including – but certainly not limited to – the successful application of military power. As a result, despite modern technological enablers, Russia's intentions and actions throughout the Ukraine conflict have been recognizable from previous decades of study of the threat to the West from the Soviet Union.¹⁵²

¹⁵¹ Keir Giles, "Russia's 'New' Tools for Confronting the West," *Chatham House*, 2016, <https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf>.

¹⁵² Nissen, "Interview, May 31."

According to these researchers, we must look to the methods employed by the KGB during the Cold War to understand the actions taken by Russia in the present time, and this is perhaps the real lesson from the Gerasimov article. I shall continue down this avenue of inquiry in the following section on Action Frames, but first, it is necessary to include a third element in the rhetorical frame, and that is Russian state-sponsored or -controlled media.

RT

The two Russian news outlets that have the potential to influence the English-speaking world the most, is *RT* (formerly known as *Russia Today*) and *Sputnik*. Both distribute news about Russia, or from a Russian perspective, in English. They are popular destinations online¹⁵³, and were behind a large number of social media posts that went viral during the U.S. presidential election in 2016.¹⁵⁴ *Sputnik* is wholly owned and controlled by the Russian state and acts as a news agency (its parent company is *Rossiia Segodnya*, the news agency controlled by the Russian state)¹⁵⁵ but also runs news websites and radio broadcasts. *RT* is mostly focused on TV production and is available as a cable channel in many western countries. It can also be watched online on the website *RT.com*, which also functions as a separate news outlet. *RT* is independent

¹⁵³ Giles, “Russia’s ‘New’ Tools for Confronting the West.”

¹⁵⁴ Amanda Erickson, “If Russia Today Is Moscow’s Propaganda Arm, It’s Not Very Good at Its Job,” *The Washington Post*, 2017, https://www.washingtonpost.com/news/worldviews/wp/2017/01/12/if-russia-today-is-moscows-propaganda-arm-its-not-very-good-at-its-job/?utm_term=.0aa08dbd15f4.

¹⁵⁵ Nigel Inkster, “Information Warfare and the US Presidential Election,” *Survival - Global Politics and Strategy* 58, no. 5 (2016): 23–32, <http://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1231527?needAccess=true>.

but sponsored and supported by the Russian state¹⁵⁶ According to the European Council's media database MAVISE, its primary owner is the Russian Federation¹⁵⁷ It's editor-in-chief is Margarita Simonyan, who has been described by several sources as having close ties to Vladimir Putin.¹⁵⁸ Simonyan vehemently denies that Russia interfered in the 2016 election: "Continue to believe that Russian interference in American elections happened. In five years, you will know that it didn't...."¹⁵⁹, and particularly, that RT had anything to do with it, which has been reported by the U.S. intelligence community¹⁶⁰: "There's nothing illegal that we did. There's nothing murky. There's no weird activity that we're involved in. Nothing." In a similar fashion as the Gerasimov article and the information security doctrine, Simonyan presents a narrative that has Russia as the victim: "What they're doing is destroying our reputation. Should we do the same thing here in Russia to all the American media? They're all anti-Putin. Should we do that? Probably should, shouldn't we? ...Should we close American media in Russia because they're all anti-Putin and they wage campaigns against him every single day?"¹⁶¹

¹⁵⁶ Sputnik, "About Us - Sputnik International," Sputniknews.com, accessed February 4, 2018, <https://sputniknews.com/docs/about/index.html>.

¹⁵⁷ RT, "RT - Fact vs Fiction," RT.com, accessed February 4, 2018, <https://www.rt.com/facts-vs-fiction/>.

¹⁵⁸ MAVISE, "Company: TV-NOVOSTI," MAVISE, accessed February 4, 2018, <http://mavise.obs.coe.int/company?id=8973>.

¹⁵⁹ Robert Windrem, "Guess Who Came to Dinner With Flynn and Putin," NBCNews.com, 2017, <https://www.nbcnews.com/news/world/guess-who-came-dinner-flynn-putin-n742696>; Michael Crowley, "The Kremlin's Candidate," POLITICO Magazine, 2016, <https://www.politico.com/magazine/story/2016/04/donald-trump-2016-russia-today-rt-kremlin-media-vladimir-putin-213833>.

¹⁶⁰ Lesley Stahl, "RT's Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda."

¹⁶¹ Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections."

Simonyan has not only supported the Russia-as-victim narrative but has also acknowledged that there is a path to Russian resurgence through proliferation of information, and that RT is engaged in something similar to warfare. In an interview with the Russian newspaper *Kommersant* in 2012, she engaged in this exchange with a journalist¹⁶²:

Question: OK, and why does the country need it all? Why should I, as a taxpayer, support you?

Simonyan: Well, for about the same reason as why the country needs a Defense Ministry. Why do you, as a taxpayer, need that?

Question: Really? Are we fighting someone at the moment?

Simonyan: Right now, we're not fighting anyone. But in 2008 we were fighting. The Defense Ministry was fighting with Georgia, but we were conducting the information war, and what's more, against the whole Western world. It's impossible to start making a weapon only when the war already started! That's why the Defense Ministry isn't fighting anyone at the moment, but it's ready for defense. So are we.

This is in line with Simonyan's reason for RT's creation: "We wanted our own CNN".¹⁶³ More importantly, it is also in line with Putin's own strategy. Here, the rhetorical frame is completed by Putin who in an interview with Simonyan broadcast on RT in 2013 said about the station:

¹⁶² Lesley Stahl, "RT's Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda."

¹⁶³ Ben Nimmo, "Question That: RT's Military Mission – DFRLab – Medium," DFRLab / Medium, 2018, <https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88>.

When we designed this project back in 2005 we intended introducing another strong player on the world's scene, a player that wouldn't just provide an unbiased coverage of the events in Russia but also try, let me stress, I mean – try to break the Anglo-Saxon monopoly on the global information streams. And it seems to me that you're succeeding in this job.¹⁶⁴

Putin then emphasized that the state “never expected this to be a news agency or a channel which would defend the position of the Russian political line...we never intended this channel, RT, as any kind of apologetics for the Russian political line, whether domestic or foreign”, but also admits that “Certainly the channel is funded by the government, so it cannot help but reflect the Russian government's official position on the events in our country and in the rest of the world one way or another.”¹⁶⁵

In sum, the narrative constituted by the elements in the rhetorical frame related to Russian national information policy is that Russia is first and foremost about protecting its interests, its people and its values from undesirable, outside influence, and that it also sees itself as under siege by Western information sources, something it must actively counteract. How this aligns with the actual policies implemented out by Russia will be analyzed in the following section. The rhetoric in the Rhetorical Frame clearly outlines a policy in which it would be justified to use

¹⁶⁴ Lesley Stahl, “RT's Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda.”

¹⁶⁵ Margarita Simonyan, “Putin Talks NSA, Syria, Iran, Drones in RT Interview,” RT.com, 2013, <https://www.rt.com/news/putin-rt-interview-full-577/>.

influence tactics on U.S. social media. By now constructing the Action Frame, I will show how these actions speak for themselves as policy implementations.

Action Frame

In this section, I will describe the actions taken by Russia in order to define the Action frame, which together with the Rhetorical frame constitutes the general policy frame under analysis. I will begin by presenting actions from the influence campaign of which there is significant evidence at the time of writing.

Elements of the Russian influence campaign of 2016

Russia has emphatically denied having played an official part in any attempts to influence the election. Nevertheless, both the U.S. and the international intelligence communities now regard it as an established fact. Congressman Adam Schiff of California, the ranking Democrat on the House Permanent Select Committee on Intelligence, replied “Oh, absolutely. There’s no question about it” when I interviewed him for this dissertation and asked him about whether he was as convinced of the Russian involvement as the intelligence community.¹⁶⁶ Schiff thus supports the Intelligence Community Assessment (ICA) published by the Office of the Director of National Intelligence in January 2017, which presents the following conclusions:

¹⁶⁶ Simonyan.

We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency.

We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments. We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him.

Moscow's approach evolved over the course of the campaign based on Russia's understanding of the electoral prospects of the two main candidates.

When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign began to focus more on undermining her future presidency. Further information has come to light since Election Day that, when combined with Russian behavior since early November 2016, increases our confidence in our assessments of Russian motivations and goals.

Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations such as cyber activity with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."¹⁶⁷

¹⁶⁷ Adam Schiff, "Interview, May 11" (Burbank, CA, 2017).

These ICA findings are supported by all four sources interviewed for this section of the dissertation, although Nissen¹⁶⁸ and Slayton¹⁶⁹ both point out that the U.S. has a history of interfering in adversaries' democratic processes too, which makes the consternation over Russia's interventions "ring hollow"¹⁷⁰ and seem slightly hypocritical.

All of those interviews, however, were conducted before representatives from Facebook, Twitter and Google appeared before Congress to present evidence of Russian information campaigns conducted on their platforms, thus providing further evidence of attempts at influencing performed by Russian entities. This happened at a small number of committee hearings between October 30 and November 1, 2017.¹⁷¹ During the hearings, the representatives from the three technology corporations confirmed to members of Congress that their research had come to the same conclusions as some of those presented in the ICA several months prior. The findings corroborated the claims in the ICA that:

- A number of ads were purchased by Russian entities for distribution during the election period on platforms such as Facebook, Instagram, Twitter, Google and YouTube

¹⁶⁸ Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections."

¹⁶⁹ Nissen, "Interview, May 31."

¹⁷⁰ Rebecca Slayton, "Interview, August 24" (Ithaca, NY, 2017).

¹⁷¹ Nissen, "Interview, May 31."

- A number of automated bots adding to the election discussion on the platforms were controlled by Russian entities
- A number of “sock puppet” accounts on the platforms would engage in “trolling” behavior related to the U.S. presidential election.

More specifically, Facebook stated that 29 million Americans directly received material from approximately 80,000 posts from 120 fake Russian-backed pages on the platform.¹⁷² They also stated that due to sharing and liking, up to three times as many people may have been exposed to this material. Towards the end of the hearings, Facebook general counsel Colin Stretch stated that 146 million Americans may have been exposed to the Russia-backed content, including 20 million Instagram users.¹⁷³ On January 31, 2018, Twitter presented the latest findings of their inquiry into the same matter on their blog. The company had found 3,814 Twitter accounts linked to the Russian influence organization known as the Internet Research Agency, which have exposed at least 1,4 million people to influence attempts.¹⁷⁴ At the congressional testimony, Google reported to have identified 1,108 videos on YouTube linked to the same influence organization across 18 YouTube channels, totaling 43 hours of content. Collectively, they had

¹⁷² Jackson Hudgins and Alyssa Newcomb, “Google, Facebook, Twitter and Russia: A Timeline on the ’16 Election,” NBC News, 2017, <https://www.nbcnews.com/news/us-news/google-facebook-twitter-russia-timeline-16-election-n816036>.

¹⁷³ Carol E. Lee and Jo Ling Kent, “Facebook Says Russian-Backed Election Content Reached 126 Million Americans,” NBC News, 2017, <https://www.nbcnews.com/news/us-news/russian-backed-election-content-reached-126-million-americans-facebook-says-n815791>.

¹⁷⁴ Jessica Guynn, “Facebook Says 146 Million Americans Reached by Russia Campaign,” USA Today, 2017, <https://www.usatoday.com/story/tech/2017/11/01/facebook-says-146-million-americans-targeted-russia-campaign/821306001/>.

generated 309,000 views in the U.S.¹⁷⁵ The influence organization known as the Internet Research Agency, has been called a “troll farm” or a “troll factory” and is based in St. Petersburg. It is a private organization who employs operatives who create content and spread it via social media, engage in discussions, post Putin-friendly comments in comment threads on news sites and feed misinformation to forums such as 4Chan and Reddit in hopes that it will be spotted by an American news outlet and given a wider audience.¹⁷⁶ After the attention given to it, first by a 2014 BuzzFeed article¹⁷⁷, then a New York Times investigation that took place in 2014 and 2015¹⁷⁸, and subsequently after the U.S. Presidential election, the company running the operation has changed its name to Glavset, according to some sources.¹⁷⁹ In October 2014 former employees of Glavset/Internet Research Agency were interviewed by Delovoy Petersburg, a daily business newspaper based in Saint Petersburg, where the “troll farm” is also located. According to this article, citing public Russian business records, the company is operated by

¹⁷⁵ Twitter Public Policy, “Update on Twitter’s Review of the 2016 U.S. Election,” Twitter Blog, 2018, https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html.

¹⁷⁶ Hudgins and Newcomb, “Google, Facebook, Twitter and Russia: A Timeline on the ’16 Election”; Chen, “The Agency”; Christopher Paul and Miriam Matthews, “The Russian Firehose of Falsehood Propaganda Model: Why It Might Work and Options to Counter It,” *RAND Corporation*, 2016, 16, <https://doi.org/10.7249/PE198>; Denis Korotkov, “Hundreds of Trolls for Millions - Society - Новости Санкт-Петербурга - Фонтанка.Ру,” Fontank.ru, 2014, <http://www.fontanka.ru/2014/05/29/170/>.

¹⁷⁷ P Bradshaw and P Bradshaw, “Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation” 2017.12 (2017): 1–37, <https://doi.org/http://comprop.oii.ox.ac.uk/>.

¹⁷⁸ Max Seddon, “Documents Show How Russia’s Troll Army Hit America,” BuzzFeed, accessed February 3, 2018, https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.ffyn0XM3B#.wbKbZYMqQ.

¹⁷⁹ Chen, “The Agency.”

Mikhail Bystrov, the former police chief for the Moskovsky district in Saint Petersburg.¹⁸⁰ According to Radio Svoboda¹⁸¹, Bystrov may also have been a retired military colonel, and the same source links the Internet Research Agency to the holding company Concord, which is run by Yevgeny Prigozhin. However, this information may not be reliable, as Radio Svoboda is part of Radio Free Europe/Radio Liberty, a U.S. counter-propaganda organization. Prigozhin has close ties to Vladimir Putin through, among other things, his business as a restaurateur and a caterer. According to some sources, an almost improbably amount of government contracts for e.g. school catering has gone to Concord.¹⁸² Other than the U.S. news sources and intelligence reports claiming that Prigozhin is responsible for the financing (and was a founder) of Glavset/Internet Research Center, several independent, Russian news outlets were making the same claims as far back as 2014.¹⁸³ One of the sources of this information was a Russian hacker group known both as Anonymous International and Shaltai Boltai. From 2013 to 2016, the group were able to illegally obtain e-mail correspondences and other compromising material through hacking, which they would then post on the Boltai.ru website.¹⁸⁴ On May 26, 2014, they posted

¹⁸⁰ Issie Lapowsky, “Facebook May Have More Russian Troll Farms to Worry About,” *Wired*, 2017, <https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/>.

¹⁸¹ Anton Butsenko, “Тролли Из Ольгино Переехали в Новый Четырехэтажный Офис На Савушкина,” *DP.ru*, 2014, https://m.dp.ru/a/2014/10/27/Borotsja_s_omerzeniem_mo.

¹⁸² Viktor Rezunkov, “«Кремлівські Тролі» Розповіли Про Себе: Де Сидять і Чим Займаються,” *Radio Svoboda*, 2015, <https://www.radiosvoboda.org/a/26903778.html>.

¹⁸³ Korotkov, “Hundreds of Trolls for Millions - Society - Новости Санкт-Петербурга - Фонтанка.Ру”; Alexandra Garmazhapova, “Yevgeny Prigozhin: Caterer to the Kremlin,” *OpenDemocracy.net*, 2014, <https://www.opendemocracy.net/od-russia/alexandra-garmazhapova/yevgeny-prigozhin-caterer-to-kremlin>.

¹⁸⁴ Korotkov, “Hundreds of Trolls for Millions - Society - Новости Санкт-Петербурга - Фонтанка.Ру.”

510 megabytes worth of material about Concord, which, among other things, showed evidence of Prigozhin’s involvement with the troll farm through alleged correspondence between Prigozhin and the financial director of Glavset/Internet Research Agency, Olga Dzalba who is also the business partner of Aleksei Soskovets, who allegedly was in charge of recruiting trolls for the “farm”.¹⁸⁵

The leader of the Shaltai Boltai hacker group, Vladimir Anikeev, was arrested by the Russian Federal Security Bureau (FSB) in October 2016. From his testimony, the FSB was also able to arrest two FSB agents, Dmitry Dokuchaev and Sergey Mikhailov on suspicion of cooperating with the hackers to target state officials and collaborating with the CIA – technically an accusation of treason.¹⁸⁶ In June 2017, it was announced that any court proceedings regarding the case would happen behind closed doors.¹⁸⁷ According to some sources, the company known as Glavset/Internet Research Agency is now part of a larger news operation with ties to the federal government in Russia.¹⁸⁸ At a minimum, evidence from Facebook, Twitter and Google shows that there was such a thing as the Internet Research Agency that conducted itself in a manner that aligned with the interests of the Russian government’s national information strategies and used methods historically rooted in Russia. The Russian Federation has not taken

¹⁸⁵ Shaltai Boltai, “Анонимный Интернационал,” Shaltai Boltai, 2014, <https://b0ltai.wordpress.com/2014/05/>.

¹⁸⁶ Korotkov, “Hundreds of Trolls for Millions - Society - Новости Санкт-Петербурга - Фонтанка.Ру.”

¹⁸⁷ Staff, “The FSB Has Caught the Alleged Head of ‘Humpty Dumpty’: What Does This Have to Do with Treason?,” Meduza, 2017, <https://meduza.io/en/feature/2017/01/31/the-fsb-caught-humpty-dumpty>.

¹⁸⁸ Rosbalt Agency, “Russia’s Trial against ‘Anonymous International’ Hacktivist Leader Will Be Closed to the Public,” Meduza, 2017, <https://meduza.io/en/news/2017/06/12/russia-s-trial-against-anonymous-international-hacktivist-leader-will-be-closed-to-the-public>.

any significant action to stop the influence activities from happening. On the contrary, the state has arrested operatives who were allegedly involved in attempts to provide hard evidence of the government's involvement in the influence campaign, as mentioned above. In fact, President Putin, while denying the involvement of the Russian government in both the influence campaign or any hacking attempts related to the 2016 presidential election in the U.S., has praised any perpetrators of such actions as being "patriotic".¹⁸⁹ In other words, even if incontrovertible evidence of official Russian involvement in the influence campaign never emerges, Russia has made it abundantly clear that it supports the campaign.

The social media tools used in the Russian influence campaign

The content with which users of social networks communicate and build relations and social capital has been termed *social currency* by several scholars.¹⁹⁰ The Russian influence campaign in the 2016 election made use of mainly one type of commercial content and four types of social currency proliferated by three types of agents.

Social currency:

1. Advertisements

¹⁸⁹ Alexey Kovalev, "Russia's Infamous 'Troll Factory' Is Now Posing as a Media Empire," The Moscow Times, 2017, <https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534>.

¹⁹⁰ Sabra Ayres, "Putin Denies a Russian State Role in U.S. Election, but Says 'patriotic' Hackers May Have Mounted Attacks," LATimes.com, 2017, <http://www.latimes.com/world/la-fg-putin-russia-hacking-20170601-story.html>; Markus Zinnbauer and Tobias Honer, "How Brands Can Create Social Currency--A Framework for Managing Brands in a Network Era," *Marketing Review St. Gallen* 28, no. 5 (2011): 50–55; Dougless Rushkoff, "Social Currency," *The Digital Divide*, 2011, 127–29; Lynn Magdol and Diane R Bessel, "Social Capital, Social Currency, and Portable Assets: The Impact of Residential Mobility on Exchanges of Social Support," *Personal Relationships* 10, no. 2 (2003): 149–70.

2. Updates/Posts
3. Memes
4. Videos
5. Links to content

1. Advertisements. The outliers in this list are the advertisements bought by Russian operatives in order to influence those exposed to them. Interestingly, these advertisements were often designed to mimic social currency, although they were actually deliberately launched and targeted towards specific audiences. In other words, users were not exposed to the ads because they were shared with them by friends or family, but because the ads were placed right in front of them by e.g. Facebook’s algorithmic ad technology. Facebook’s advertising system is built for as specific targeting as possible¹⁹¹, and so these advertisements would find their intended audiences very accurately¹⁹². As mentioned, several of the ads would appear as social currency, and if designed and targeted properly, would not appear as being out of context, compared to the rest of the user’s news feed. Some ads would look like they were from a Facebook fan page the user had already “Liked”, thereby indicating an interest in seeing posts from that page, or it might be simply soliciting said Likes. An example can be seen in Figure 1.

¹⁹¹ Morten Bay, *Homo Conexus* (Lulu. com, 2013).

¹⁹² Malte Brettel et al., “What Drives Advertising Success on Facebook? An Advertising-Effectiveness Model: Measuring the Effects on Sales of ‘Likes’ and Other Social-Network Stimuli,” *Journal of Advertising Research* 55, no. 2 (2015): 162–75, <https://doi.org/10.2501/JAR-55-2-162-175>.



Figure 1. One of the Facebook ads presented during the October 31 – November 1, 2017 congressional hearings.

It should be mentioned that these Facebook pages were real, but the organizations behind them were not. In this sense, the ads are reminiscent of so-called “Astro-turf” political ads on tv during elections.¹⁹³ Because users would be encouraged to Like pages that fit their political beliefs, and the Facebook advertising algorithm automatically ensures that users mostly saw pages that fit those beliefs, these fake pages were able to assemble hundreds of thousands of Likes, and hence, users whom the Russian influencers now could communicate to directly on a singular channel.

¹⁹³ Caroline W. Lee, “The Roots of Astroturfing,” *Contexts* 9, no. 1 (2010): 73–75, <https://doi.org/10.1525/ctx.2010.9.1.73>.

Other ads came in the form of event invitations that users would normally get from friends. However, these events were almost never real-life events. The realism of the ads and the pages made them highly believable, as witnessed by the fact that some people would actually show up to the fake events mentioned above.¹⁹⁴

In other words, the main purpose of the ads was to turn targeted advertising into direct, social communication. The fake advertisements and pages were not social currency in themselves but would quickly turn into this type of sharable content, because of users pressing the Like button, which in some cases also alerts friends that the users have Liked a page, thereby exposing members of the user's network to the same content. This is a viral form of communication most often used for commercial marketing, but in this case, the same mechanisms were used for information warfare. Nissen argues this is a trend that is increasing its presence on the Internet.¹⁹⁵

2. Updates/Posts. Ads aside, the Russian influence operatives working from e.g. the Internet Research Agency would also to a large extent engage directly with users in social media networks. This happened through fake “sock puppet” accounts controlled by actual human beings, or through automated bots that would post comments or updates. Three examples of these from Twitter can be seen in Figure 2, where the tweets from @Pamela_Moore13 and an

¹⁹⁴ Casey Michel, “How the Russians Pretended to Be Texans — and Texans Believed Them,” The Washington Post, 2017, https://www.washingtonpost.com/news/democracy-post/wp/2017/10/17/how-the-russians-pretended-to-be-texans-and-texans-believed-them/?utm_term=.fedcd9c86b35.

¹⁹⁵ Nissen, “Interview, May 31.”

account that initially pretended to be the official Twitter account for the Tennessee Republicans, @Ten_GOP represent the political right, and the @CrystalJohnson account represents a Black Lives Matter activist on the political left. This is also a clear example of what Thomas Elkjer Nissen referred to above as an influence campaign that is “cleansed” of ideology. The main motive here is to sow division, not propagate a particular ideology as was often the case with KGB influence campaigns during the Cold War. By encouraging users to commit to one of two poles, further polarization can be achieved.



Figure 2. Three tweets from Russian trolls.

3. Memes. A meme (in relation to digital culture) is a piece of social currency that goes viral, often in the shape of an image or a video. By employing meme characteristics that have been established as effective such as humor, engaging/emotional visuality and simplicity¹⁹⁶, the influencers were able to slip into the users' routine behavior and heuristics on social media platforms, such as sharing memes without much consideration.¹⁹⁷

4. Videos. Some videos that did not have meme-like qualities would still be shared profusely by social media users. Examples of these would be videos from RT.com or from the influencer YouTube channels as mentioned above. These would have messages designed to cast doubt on otherwise accepted facts by countering them with disinformation but would often be too long or otherwise demanding to be viewed and shared casually.

5. Links to Content. Links to articles containing different types of (mis-)information would also be shared by Russian influencers in the hopes that they would be further proliferated by users. One of the most discussed types of disinformation content proliferated during the election were the so-called “fake news” stories. These could appear in any of the five types of social currency listed above but always with the purpose of sowing division, spreading doubt and getting users to share what they have just been exposed to. Links to articles were especially in wide use by the

¹⁹⁶ Limor Shifman, *Memes in Digital Culture* (Mit Press, 2014).

¹⁹⁷ Alfred Hermida et al., “SHARE, LIKE, RECOMMEND: Decoding the Social Media News Consumer,” *Journalism Studies* 13, no. 5–6 (2012): 815–24, <https://doi.org/10.1080/1461670X.2012.664430>.

Russian influencers, and as Nyhan et al. have shown¹⁹⁸, thousands of users would be enticed to click on links to news sites with questionable or directly false news stories or information on them. This study shows that particularly Trump-supporting users would be susceptible to this, but the study does not take into account how users who only looked at the headlines for the fake news stories on Facebook would be impacted, or how sharing without clicking on the story helped spread the disinformation further. Howard et al. have concluded that in Michigan, one of the three states (the others being Wisconsin and Pennsylvania) that tipped the election to Trump, approximately two-thirds of total, shared content on Twitter in the days leading up to the election consisted of news stories (meaning that only one-third of content shared in the period was the type of social currency such as pictures of cats and SNL openings that would normally be shared outside the election season) One of the two thirds consisted of fake news and the other third was real news, meaning that fake news was as likely as real news to be shared by Twitter users who indicated they were tweeting from Michigan¹⁹⁹ Out of 4,799,284 voters in Michigan, Trump won the state by 10,704 votes.

Agents

The social currency seeded to the social media platforms by Russian influencers were propagated by three types of accounts:

¹⁹⁸ Guess, Nyhan, and Reifler, “Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 U.S. Presidential Campaign.”

¹⁹⁹ Howard et al., “Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?”

1. **Bots**
2. **Trolls**
3. **Users**

1. Bots Bots are automated “sock puppet” accounts that uses data collection and machine learning to post in forums or on social media platforms. On Twitter, for example, a number of Russian bots replied to tweets during the election, although they were not following the Twitter user they were replying to. Instead, because Twitter is public, the bots would seek out comments made by Twitter users that e.g. might be disparaging to a candidate, and post a reply supporting that candidate in the shape of a meme or a simple hashtag, or some kind of simple, pre-determined message.²⁰⁰

2. Trolls Whereas Bots are software, trolls are actual human beings, often with sock puppet accounts who can engage directly with users on the social media platforms. After the election, several Twitter users began identifying and “doxing” (naming, outing) the troll accounts so that others could dismiss or ignore them.²⁰¹ Twitter also began weeding out the accounts more systematically.²⁰² But during the election, trolls from the Internet Research Agency went about

²⁰⁰ Alessandro Bessi and Emilio Ferrara, “Social Bots Distort the 2016 U.S. Presidential Election Online Discussion,” *First Monday* 21, no. 11 (2016), <https://doi.org/10.5210/fm.v21i11.7090>.

²⁰¹ Sandy Garossino, “Who the Hell Is @RVAwonk and How Is She Cracking the Kremlin’s Code?,” *National Observer*, accessed February 4, 2018, <https://www.nationalobserver.com/2017/12/28/opinion/who-hell-rvawonk-and-how-she-cracking-kremlins-code>.

²⁰² Twitter Public Policy, “Update on Twitter’s Review of the 2016 U.S. Election.”

their business almost without any resistance, mostly due to ignorance on behalf of the users, even though news of Russian trolls campaigns had circulated for two years²⁰³ In KGB terminology, these trolls would have been known as *agents of influence*²⁰⁴, who knowingly and deliberately participate in the *active measures*. The users in Figure 2 are examples of trolls.

3. Users Finally, regular users were essential in the proliferation of the influencer material. As noted above, Facebook reported to Congress that users sharing the content might have grown the reach of the influence campaign severely, possibly reaching three times as many people as the people who were initially exposed to the material²⁰⁵ Which psychological mechanisms in the influence material that persuaded the users to act and share the content still remains to be studied with broadly accepted conclusions. Likewise, a causal relation between the influence campaign and Trump’s election victory may never emerge. But there should not be any controversy in stating that Russian influencers were successful in persuading hundreds of thousands of social media users to share, like, retweet or otherwise engage with the influencer material. In traditional, kinetic warfare, those who participate in acts of war are seen as renegades or enemy combatants²⁰⁶ But even though hundreds of thousands of Americans engaged freely in the Russian influencer campaign “it is stretching the combatant concept too far” to brand these users

²⁰³ Seddon, “Documents Show How Russia’s Troll Army Hit America.”

²⁰⁴ Mitrokhin, *KGB Lexicon: The Soviet Intelligence Officers Handbook*.

²⁰⁵ Lee and Kent, “Facebook Says Russian-Backed Election Content Reached 126 Million Americans.”

²⁰⁶ Kenneth Roth, “The Law of War in the War on Terror: Washington’s Abuse of ‘Enemy Combatants,’” *Foreign Affairs* 83, no. 1 (2004): 2–7, <https://doi.org/10.2307/20033823>.

as enemy combatants, according to Thomas Elkjer Nissen, who instead thinks they belong in the category defined by the KGB during the cold war to include unwilling and unknowing participants in active measures such as influence and disinformation campaigns, “Useful idiots”²⁰⁷

Cultural background

As is required by the frame-critical method, applied to this study, I will now turn to the cultural and historical background that inform the systems of belief in which these policies are made and adopted. Cultural anthropology provides tools for teasing out the components of such systems, but these tools should be employed with caution. Though critics have argued against the phenomenon and continue to do so²⁰⁸, I argue that some amount of cultural harmonization has been the effect of globalization and the emergence of the Internet. Particularly the latter and the decreased emphasis on nationality and geographical boundaries as part of identity-building in post-Internet generations²⁰⁹ makes it more difficult to make sweeping generalization on behalf of

²⁰⁷ Nissen, “Interview, May 31.”

²⁰⁸ Staff, “Engine Failure,” *Logic*, 2017, <https://logicmag.io/03-engine-failure/>; Zygmunt Bauman, “Glocalization and Hybridity,” *Glocalism: Journal of Culture, Politics and Innovation* 1, no. 1 (2013): 1–5, <https://doi.org/10.12893/gjcp.2013.1.9>; Srinivasan, *Whose Global Village?: Rethinking How Technology Shapes Our World*.

²⁰⁹ Robert M Mason, Karine Barzilai-Nahon, and Nancy Lou, “The Organizational Impact of Digital Natives: How Organizations Are Responding to the Next Generation of Knowledge Workers,” *Proceedings of the 17th International Conference on Management of Technology*, 2008, http://faculty.washington.edu/rmmason/Publications/IAMOT_DN_2008.pdf; van Dijck, “‘You Have One Identity’: Performing the Self on Facebook and LinkedIn.”

populations of nation-states. While making judgments across entire populations or ethnic groups may be imprudent and socially undesirable for these reasons, certain elements from Russian sociocultural history still appear to be in correspondence with the policies under examination here. Though these elements and behaviors may not be applicable to all Russians, they have been observed by scholars across several disciplines as components present in Russian culture through several centuries. Furthermore, the post-Internet generations have yet manifest themselves as powerful forces within the political system in Russia. Nadia Diuk, referring to studies made by Russian sociologist Olga Krysthanovskaya, notes that “despite the shakeup in terms of age in the ruling elite, the people rising in the political ranks and also the people getting rich toward the end of the 1990s were precisely those who had been positioned well by the Communist Party in its final days as ruler of the USSR”.²¹⁰ Writing in 2012, Diuk goes on to confirm that the governments led by Vladimir Putin as both president and prime minister since 1999 have not in any meaningful way had their policies influenced by the post-Internet, post-globalization generations. In other words, at the time of writing, it is not unreasonable to seek parameters and components for the institutional action frame of Russian cyber policies in pre-globalization cultural assessments from a time where Russian national identity was both more pervasive and more closely tied to Russian culture and history. The observation by a cadre of scholars of these cultural components - while they are not universal, and their influence may be declining - merits their potential inclusion as part of the institutional action frame analysis I am about to perform.

²¹⁰ Nadia Diuk, *The next Generation in Russia, Ukraine, and Azerbaijan: Youth, Politics, Identity, and Change* (Rowman & Littlefield, 2012), 27–28.

The Russian national character

Kets de Vries states that “The Russian national *character* (a concept here widely construed to include leadership style and choice of organizational practices) is embedded in its *culture*.” (emphases in the original).²¹¹ He further distinguishes *character* from *culture* by defining *character* as “habitual ways in which a person deals with external and internal reality”, while *culture* is “the ideals, values and assumptions about life that are widely shared among a population and that guide specific behavior patterns”.²¹² This distinction is important for the analysis of the institutional action frame, as the latter is an expression of *culture* rather than *character* in this sense. While, as Kets de Vries points out, leadership style may be included in *character*, it doesn’t rise to the level of pervasiveness required to be included in institutional action frames.

Culture, however, does. This is further supported by some of the more widely accepted definitions of culture found in cultural anthropology. Margaret Mead’s definition of culture as “regularities in behavior that are shared”²¹³ or Geert Hofstede’s definition of culture as the “collective programming of the mind that distinguishes one group or category of people from another”²¹⁴ are examples. In the following, I will show how the art of deception and specifically, disinformation tactics, as well as a cultural perception of factuality and truth that is different

²¹¹ Manfred F.R. Kets de Vries, “The Anarchist within: Clinical Refelctions on Russian Character and Leadership Style,” *Human Relations* 54, no. 5 (2001): 589, <http://journals.sagepub.com/doi/pdf/10.1177/0018726701545003>.

²¹² Kets de Vries

²¹³ Martha Wolfenstein and Margaret Mead, *Childhood in Contemporary Cultures*, ed. Martha Wolfenstein and Margaret Mead (Chicago, IL: University of Chicago Press, 1955), 10.

²¹⁴ Geert J. Hofstede, “Cultures and Organizations: Software of the Mind,” *McGaw-Hill, London*, 1991, 5.

from Western notions of the same concepts, have deep roots in Russian culture and therefore must be considered when analyzing the institutional action frames of Russian cyber policies.

A history of deception as strategic virtue

Deception is a task undertaken with great pride in Russian military operations, and a skill associated with admiration among military leaders. This is not so different in other nations and cultures, but it appears to be central to Russian perceptions of power, strength and superiority in a manner unparalleled in most other nations. Major General Alexander Vladimirov is Vice-chairman of the Board of Military Experts of Russia and a member of the Council for National Strategy in Russia. He also teaches military strategy at the Suvorov Military School near Moscow. He is considered an authority on *maskirovka*, the special brand of military deception that Russia considers its own. In an interview with the BBC²¹⁵, Vladimirov espouses an adversarially-conditioned view of humans: "As soon as man was born, he began to fight...When he began hunting, he had to paint himself different colors to avoid being eaten by a tiger. From that point on maskirovka was a part of his life. All human history can be portrayed as the history of deception". Vladimirov also considers Russian mastery of military deception central to its national identity: "Vladimirov quotes liberally from the Roman general Frontinus and the ancient Chinese philosopher Sun Tzu who described war as an eternal path of cunning. But it's Russia,

²¹⁵ Lucy Ash, "How Russia Outfoxes Its Enemies," BBC News Magazine Online, 2015, <http://www.bbc.com/news/magazine-31020283>.

he tells me, with unmistakable pride, that has over the centuries really honed these techniques to perfection”²¹⁶

As mentioned before, deception is regarded as part of the military operational toolbox by most nations. It is important to note, however, that the deception of *maskirovka* does not completely overlap with the concept of disinformation in a Russian context. Rather, as Glantz pointed out in an analysis during the Soviet era, disinformation sets the “atmosphere” for *maskirovka*, and is somewhat of a prerequisite to deceptional ability.²¹⁷ Disinformation, thus, is an instrument of power that is even more fundamental to Russian strategic maneuvering than general methods of deception.

Another source pointing to the fundamentality of disinformation and *maskirovka* in Russian strategic thinking is Ion Mihai Pacepa, a former three-star general in the secret police (Securitate) of Romania during that country’s inclusion in the Warsaw Pact and alliance with the Soviet Union. Pacepa recounts how the KGB training manuals he would read during his ascent within the system would claim that “the “science” of disinformation (and it was specifically and proudly termed a science) was born in Russia, it was deeply rooted in the Russian soil and in that country’s history, and there it would remain forever”²¹⁸ Pacepa describes how the manuals would include the story of the original “Potemkin Village”:

²¹⁶ Ash.

²¹⁷ David M Glantz, “Surprise and Maskirovka in Contemporary War,” *Military Review*, no. December (1988): 6, <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA216491>.

²¹⁸ Ion Pacepa, *Disinformation : Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism* (WND Books, 2013), chap. 5 Kindle Edition.

...born in eighteenth century Russia, disinformation was the fruit of the passionate love affair between Catherine the Great and Prince Grigory Potemkin, her principal political and military adviser. In 1787, Potemkin, by then the governor general of the New Russia (today's Ukraine), took the empress on a tour of the Crimea, which he had been instrumental in annexing from the Turks four years earlier. To impress her, Potemkin had arranged for sham villages to be erected along the route the empress would take. One of those empty-façade villages, erected at the mouth of the small river Bug, went so far as to welcome the empress with a triumphal arch inscribed: "This is the way to Constantinople."

This story has largely been dismissed by historians as an exaggeration of the real inspection tour, during which Potemkin had made certain that the already standing villages on the route had been nicely decorated in preparation for Catherine the Great's visit – and this was never a secret.²¹⁹ However, even if the KGB used this exaggerated version of the story to bolster the notion of disinformation as a Russian-born concept, it is actually just further evidence of how myth, narrative and lack of factuality was a common occurrence at the time, even in contexts from which you would expect otherwise. Pacepa also quotes the Marquis de Custine, who wrote extensively of his travels in Tsarist-era Russia:

In the eighteenth century, the French Marquis de Custine remarked that in fact
"everything is deception in Russia, and the gracious hospitality of the Czar, gathering

²¹⁹ A.M. Panchenko, "'Potemkin Villages' as Cultural Myth," in *Russian History and Culture: Works of Different Years*. (St. Petersburg: Yuna, 1999), 462–75.

together in his palace his serfs and the serfs of his courtiers, is only one more mockery.”

Custine also noted—in language that cannot be improved upon even today—that

“Russian despotism not only counts ideas and sentiments for nothing but remakes facts; it wages war on evidence and triumphs in the battle.”²²⁰

Pacepa, of course, is a defector and cannot be relied upon as an objective source of information with regards to disinformation’s role in Russian culture. However, several other scholars have made similar observations from different perspectives. Still within the military realm, Thomas points to the Russian tactic of *reflexive control*, which is “defined as a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action.”²²¹ Additionally, Thomas makes it clear that this disinformation-related theory is still being refined in the national security agencies of the Russian Federation. Chotikul²²² traces the reflexive control theory to the earliest days of the Soviet Union and its conceptual predecessors and pre-conditions even further back.

“Disinformation” and deception in civilian life

There is evidence to suggest that disinformation plays a cultural role outside the military, intelligence or strategic realms. One example is Svetlana Boym’s exploration of Russian

²²⁰ Pacepa, *Disinformation : Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*.

²²¹ Timothy L Thomas, “Russia’s Reflexive Control Theory and the Military,” *The Journal of Slavic Military Studies* 17, no. 17 (2004): 237, <https://doi.org/10.1080/13518040490450529>.

²²² Ddiane Chotikul, “The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: Preliminary Study,” 1986.

everyday culture in the 19th and 20th centuries, in which she shows how truth is indeed a relative phenomenon for the average Russian: “In Russian there are two words for truth – pravda and istina – and no word for authenticity ... Authenticity is connected to authorship, to a legal authentication. It is irrelevant if not negatively valorized in the Russian intellectual tradition...”²²³ Boym points to the fact that the word “pravda” has been devalued and that “istina” is a more essential, ontological truth, a truth about what is. Yet none of these expressions of truth are absolute. Boym demonstrates how colloquialisms such as “truth is good, but happiness is better”²²⁴ reveal a popular notion that truth can be sacrificed for the greater good, a sort of utilitarian approach to truth-telling. Even more revealing is Boym’s statement that through the decades, and even with the massive upheavals Russia experienced in the early 20th century, “one feature, however, remains the same – truth has to be “Russian” ...” Russian truth” is positively qualified, as opposed to “Gypsy truth” or “Greek truth””. This idea that there is a certain Russian truth that can be different from or the same as any objective or absolute truth is “one of the more important cultural obsessions inherent in the intelligentsia’s discourse on Russian identity since the nineteenth century.” Boym describes the notion of truth as it is presented in Russian oral traditions, from which it made its way into the intelligentsia, as possessing a “common ambiguity”.²²⁵

²²³ Svetlana Boym, *Common Places: Mythologies of Everyday Life in Russia* (Harvard University Press, 2009), 96.

²²⁴ Boym, 96.

²²⁵ Boym, 96.

Some scholars also see this common ambiguity expressed through interpersonal relations and presentations of self. In an analysis of the origins and effectiveness of the reflexive control theory performed towards the end of the cold war, Chotikul explains that Russians have historically been suspicious towards outside influences and actors: "...pre-Bolshevik historical experience has been conducive to the development of a "siege mentality"--the flatness and openness of the Russian landscape has, since the beginning of history, invited invasion and necessitated a state of hypervigilance and suspiciousness of outsiders among the inhabitants"²²⁶ According to Chotikul, this suspiciousness of outsiders made the Soviet Union leadership's use of reflexive control theory on its own population very successful:

There appear to be certain areas of belief, in particular, in which this method of conveying specially prepared information to influence the decision- making process toward predetermined, desired ends has been of exceptional utility to the regime. The first has been in reinforcing the feeling of need for authority and a craving for command by a father or father figure--what has been referred to as the "Little Father System" of government...The second area of belief which seems to carry the mark of reflexive control has to do with the inevitability of Communism... Those citizens who are not won over through the influence of sacrosanct authority and dependency on a "Little Father," are therefore captured on a slightly different, more intellectual level by this dialectical argument in support of the inevitability of Communism. This ideological precept appears

²²⁶ Chotikul, "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: Preliminary Study," 49.

also to have fulfilled the people's "traditionally Russian" desire and quest for simple explanations."²²⁷

From a completely different academic perspective - that of communication psychology – Chotikul’s findings are backed up by Kets de Vries. In his aforementioned study of Russian “character”, he notes that the latter is formed by the trust in authority and distrust of others. This even impacts personal morals:

The KGB did not teach people about the distinction between right and wrong but about the need for sensitive attunement to external, often contradictory, signals of approval and disapproval. Rather than listening to their conscience in deciding the morality of an issue, people listened for the early-morning knock that would send them to a gulag for some fabricated transgression. In the long run, the inconsistency and insincerity of that form of authority eroded individual authenticity and created inner conflict and a feeling of unreality.²²⁸

This uncertainty of moral and factual direction, paired with the Russian distrust of outside knowledge, influence or actors manifests itself as a form of everyday deception pervasive in Russian culture, according to some scholars.

²²⁷ Chotikul, 46–47.

²²⁸ Kets de Vries, “The Anarchist within: Clinical Refelctions on Russian Character and Leadership Style,” 604.

Carbaugh claims that Russians have taken Goffman's concepts of "Front Stage" and "Back Stage" personalities²²⁹ to an extreme, by reserving the true colors of their personality for inner dialogue and communication with those closest to themselves, such as family or very close friends. This private personality is supplemented by a public personality, which is a complete construct formed by the person's external conditions. It can be argued that Goffman showed this as being the case for most people in the modernized world and that both early and late Internet studies work by Turkle²³⁰, Baym²³¹, and others is indicative of a severe split between public and private personas in communicative situations. However, the point made by Kes De Vries and Carbaugh is that this split is integral to Russian culture, and that the split has been developed through several centuries. Carbaugh argues that the Russian persona consists of the body, the physical representation of self, and the "dusa", which roughly translates to "soul": "The "soul" (dusa) of the Russian person, as a passionate, morally committed, distinctly human agent, and as the shared locus of communal symbolic life, is presupposed for each discursive performance, but is more happily and intensely elaborated in private"²³², he writes, and quotes Hedrick Smith²³³ to explain this divide further:

²²⁹ Erving Goffman, *The Presentation of Self in Everyday Life* (New York: Anchor Books, 1959).

²³⁰ Turkle, "Alone Together"; Sherry Turkle, "Life on the Screen: Identity in the Age of the Internet," *NY Etc.: Cop*, 1995.

²³¹ Nancy K Baym, *Tune in, Log on: Soaps, Fandom, and Online Community*, vol. 3 (Sage, 2000).

²³² Donal Carbaugh, "'Soul' and 'Self': Soviet and American Cultures in Conversation," *Quarterly Journal of Speech* 79 (1993): 194, <http://www.tandfonline.com/doi/pdf/10.1080/00335639309384028>.

²³³ Hedrick Smith, "The Russians. New York: Quadrangle," *New York Times Book Co*, 1976.

From childhood onward, Russians acquire an acute sense of place and propriety... They divide their existence into their public lives and their private lives, and distinguish between "official" relationships and personal relationships... They adopt two very different codes of behavior for their two lives—in one, they are taciturn, hypocritical, careful, cagey, passive; in the other, they are voluble, honest, direct, open, passionate. In one, thoughts and feelings are held in check. In the other, emotions flow warmly, without moderation.²³⁴

The almost whimsical and playful relationship Russians have with the truthfulness in which Westerners place such importance and emphasis is perfectly represented in one of the longest-running jokes in the Soviet era. The two main newspapers from which citizens of the Soviet Union would get their information and news, were *Pravda*, which translates as “Truth” in Russian, and *Izvestia*, which translates as “News”. The joke, which in the American societal tradition would be seen as signaling a catastrophic failure of democratic institutions, was that “There’s no *Truth* in *News*, and no *News* in *Truth*”.²³⁵

²³⁴ Carbaugh, “‘Soul’ and ‘Self’: Soviet and American Cultures in Conversation,” 195.

²³⁵ Cameron Hood, “No Truth in News, and No News in Truth,” *Latterly*, 2017, <https://cameronghood.com/2017/04/20/no-truth-in-news-and-no-news-in-truth/>; Svetlana Voreskova, “Yes: ‘There Is No Truth in the News and No News in the Truth’ Was a Very Common Saying,” *Medium*, 2017, <https://medium.com/@svetlanavoreskova/yes-there-is-no-truth-in-the-news-and-no-news-in-the-truth-was-a-very-common-saying-9f44f3d678f7>; Michael Specter, “Russia’s Purveyor of ‘Truth’, *Pravda*, Dies After 84 Years,” *The New York Times*, accessed February 3, 2018, <http://www.nytimes.com/1996/07/31/world/russia-s-purveyor-of-truth-pravda-dies-after-84-years.html>.

Russia's interventionist information security policy and the Rawlsian Frame

Russia as well-ordered / fair and just society

In the following, I will let Russia's Rhetorical and Action frames interact with the Rawlsian frame as described in Chapter 2. As mentioned there, Rawls primarily presents his view of foreign policy ethics in *The Law of Peoples* (LP)²³⁶, where he explores how societies formed as he prescribes would engage with other nations. Since this chapter on Russia's social media policy concentrates on Russia's foreign interactions, rather than its domestic policies, it is appropriate to also focus on Rawls' work in LP.

It is important to note, however, that Russia's external policies are closely tied to their domestic ones. Martin Libicki is Keyser Chair of Cybersecurities at the U.S. Naval Academy, where he teaches and studies cyberwarfare as one of the world's most respected scholars in that field. In an interview for this dissertation, Libicki argues that Putin's strategy of disrupting Western democracies through means of deception does not just make Russian citizens feel proud, the same deception also targets them. He says of the 2016 influence campaign and what followed in its wake:

The Russians have achieved an illusion of success without actually having achieved success. If you are Vladimir Putin, and you want to fool most of the people some of the time, and your perspective takes you out to 2024 and no farther, that's a potentially winning strategy". The Russians believe they were weak in the 90s, as a result of which they were poorer, and therefore, national survival and national prosperity demand that

²³⁶ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*.

they cannot be weak anymore. And the Russians have never been motivated by tender feelings for their neighbors. It is a domestic strategy. And the success is domestic.²³⁷

Libicki's reference to the year 2024 assumes that Vladimir Putin will win the Russian presidential election in 2018 and sit for another term, which will last until 2024. The Russian Federation "attempts to maintain a veneer of democracy" according to Libicki. Its system of government is officially a federal, constitutional republic based on a representative democracy, in which The Federal Assembly is not unlike the United States Congress. The upper house of the Assembly is called the Federation Council and consists of 170 elected members, two from each of Russia's Federal Subjects (federally designated regions). The lower house, the State Duma, consists of 450 elected representatives of Russia's local districts. At the time of writing, 339 of the 450 members of the State Duma belong to the United Russia party, of which Vladimir Putin used to be the leader and prime minister / chairman of the government (and former president) Dmitry Medvedev is now chairman. As the prime minister is appointed by the president and part of the executive branch, Medvedev obtained his position as chairman of the United Russia party separately from his post as prime minister. In the upper house, the Federation Council, party affiliation is banned.²³⁸

²³⁷ Martin C Libicki, "Interview, August 28" (Annapolis, MA, 2017).

²³⁸ Russian Federation, "Government of the Russian Federation | Embassy of the Russian Federation to the United States of America," Embassy of the Russian Federation, accessed February 4, 2018, <http://www.russianembassy.org/page/government-of-the-russian-federation>; Central Intelligence Agency, "Russia," The World Factbook, accessed February 4, 2018, <https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html>.

Add to this the general consensus among organizations such as Amnesty International²³⁹ and the OSCE²⁴⁰ that Russian elections since Putin came to power have been less than fair and just, and an image emerges of a nation where power is centralized in the presidency. For the structure of a society to be fair and just, according to Rawls, it must be “well-ordered” as described in Chapter 2. Is The Russian Federation well-ordered? This is not an easy question to answer. Rawls’ first principle of a well-ordered society entails that “everyone accepts, and knows that everyone else accepts, the very same principles of justice”²⁴¹. Second, a well-ordered society’s “basic structure – that is, its main political and social institutions and how they fit together as one system of cooperation – is publicly known, or with good reason believed to satisfy these principles, and third, its citizens have a normally effective sense of justice and so they generally comply with society’s basic institution, which they regard as just”²⁴². Russia’s “vener of democracy” is certainly organized and its structure publicly known by the people.

However, according to a study by Germany’s Friedrich-Naumann Foundation, Russians do not have a conception of democracy that aligns with Rawls’. For example, 70 percent of the 1,653 respondents did not see a need for freedom of speech or independent media outlets, and a small majority, 53.6 percent, responded that they believed that government security agencies

²³⁹ Amnesty International, “Russian Federation 2016/2017,” accessed February 4, 2018, <https://www.amnesty.org/en/countries/europe-and-central-asia/russian-federation/report-russian-federation/>.

²⁴⁰ OSCE, “Intimidation of Observers at Odds with OSCE Commitments to Ensure Transparent Elections, ODIHR Director Says,” Organization for Security and Co-operation in Europe, accessed February 4, 2018, <http://www.osce.org/odihr/elections/171726>.

²⁴¹ Rawls, *Political Liberalism*, 34.

²⁴² Rawls, 35.

should be able to break the law in order to keep the country safe. 42.2 percent opposed this idea. A large majority, 65.9 percent, supported the idea that the government should collect citizens' data and track their actions. As a response to the survey,

Dmitry Rogozin, the director of research at the Russian Academy of Economics and State Service who oversaw this research, told Deutsche Welle that the divide between support for democracy and the lack of support for certain aspects of it does not in fact reflect ignorance on the part of Russians as to what democracy in fact is. Instead, he said, it reflects something that many will see as even more disturbing: the fact that many Russians do not see democracy as having much to do with their lives and therefore do not place it at the center of their discussions about what the state is doing and what their role in the state actually is.²⁴³

It should be noted that the Friedrich-Naumann Foundation is tied to the German political party FDP which promotes classic liberalism²⁴⁴

Whoever is to blame for the supposed lack of democratic insight in the Russian population does not matter in this regard. It is sufficient to conclude that although the citizens of Russia may in fact believe in the same principles of justice, may be aware of how the system works and may comply with the system and consider it just, Rawls would still not consider Russia a well-ordered

²⁴³ Paul A. Goble, "Survey: Most Russians Say They Want a Democracy but Don't Support Democratic Values," Euromaidan Press, 2016, <http://euromaidanpress.com/2016/10/04/survey-most-russians-say-they-want-a-democracy-but-dont-support-democratic-values/#arvlbdata>.

²⁴⁴ FDP - Die Liberalen, "Free Democratic Party - The German Liberals - English Brochure" (Berlin), accessed February 4, 2018, https://www.fdp.de/files/646/270881_FDP_welcome_berlin.indd.pdf.

society. As he writes: “Any conception of justice that cannot well order a constitutional democracy is inadequate as a democratic conception. This might happen because of the familiar reason that its content renders it self-defeating when publicly recognized”.²⁴⁵ This is exactly the case in Russia, if the Friedrich-Naumann Foundation study is representative of reality. The study concludes that Russians generally are supportive of the idea of democracy, just not its actual implementations, and they aren’t particularly concerned with its impact in their lives. This conception of justice and democracy is hence “self-defeating” as Rawls puts it. Moreover, Rawls also assumes “reasonable pluralism” as a fact of a democratic society. That is, democratic systems must, by definition, be constituted by a reason-based plurality of positions, according to Rawls, as the alternative is oppression:

...a continuing understanding on one comprehensive religious, philosophical, or moral doctrine can be maintained only by the oppressive use of state power. If we think of political society as a community united in affirming one and the same comprehensive doctrine, then the oppressive use of state power is necessary for political community”²⁴⁶

The current state of the elected government in Russia, as described above, has the president’s party in control of more than 75 percent of the seats in the lower house and no party affiliations allowed in the upper house. I argue that this is exactly the type of affirmation of a singular doctrine that Rawls claims can only be achieved through state oppression. This aligns with the

²⁴⁵ Rawls, *Political Liberalism*, 35.

²⁴⁶ Rawls, 36.

fact that the voting process in Russia has been under criticism from international organizations for almost two decades. Summarily, though Russia may live up to the actual words in Rawls' criteria for a well-ordered society, it does not live up to the conditions laid out in his deeper exploration of the concept.

Yet, I shall continue this discursive argumentation as if Russia *is* a well-ordered society in Rawlsian terms. I choose to do this for two reasons. One is the openness and lack of prejudgment required by Rawls' "veil of ignorance", which I have described as part of my method in Chapter 1. The other is the ability to effectively explore the differences between the Russian policy frames and the Rawlsian Frame without simply initially dismissing Russia as a non-well-ordered state.

Idealism and political realism in Russian information policy

As it should be apparent from the frame analysis of its official information policy above, Russia believes that information security is part of a struggle to limit the normative influence from other countries with different value sets. The manner in which this is worded in the doctrine constitutes what Rawls considers to be "political realism":

I reply to the realist theory that international relations have not changed since Thucydides' day and that they continue to be an ongoing struggle for wealth and power by recalling a familiar view of peace or a society of liberal peoples. It leads to a different view of war than the hegemonic theory of the realist.²⁴⁷

²⁴⁷ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 46.

Rawls, citing Saint-Just and Montesquieu, notes that this democratic peace ideal is really a convergence of two ideas:

Putting these two ideas together – that social institutions can be revised to make people more satisfied and happy (through democracy), and that commerce tends to lead to peace – we might surmise that democratic peoples engaged in commerce would tend not to have occasion to go to war with one another. Among other reasons, this is because what they lacked in commodities they could acquire more easily and cheaply by trade, and because, being liberal constitutional democracies, they would not be moved to try to convert other peoples to a state religion or other ruling comprehensive doctrine.²⁴⁸

As mentioned above, Russia's influence campaign in 2016 was free of ideological boundaries, which may be compatible with what Rawls writes towards the end of the quote above, but that is only on the surface and from a foreign policy standpoint. The influence campaign's purpose was to weaken the democracy and social fabric of Russia's greatest adversary, the United States, thereby strengthening Russia's position geopolitically, and in particular, in conflicts such as the ones in Ukraine and Syria. But this strength, as Libicki argues above, translates into domestic policies and a further centralization of power in the executive branch, which is likely the biggest gain and main purpose of the operation. Thus, when Russia in its information security doctrine opens a legislative and moral space up for using act of information warfare to strengthen itself domestically and internationally, it is political realism in Rawls' view, and something that he

²⁴⁸ Rawls, 46.

finds to be detrimental to the hopes of democratic peace. As Leavitt writes in his interpretation of Rawls' Law of Peoples: "From the point of view of political realism, idealism in the international domain undermines the security of a state".

Russia's information security doctrine, with its statement that it is impossible to regulate information operations jointly on the international level, and its emphasis on states trying to corrupt the minds of (especially young) Russians through information operations, is in direct opposition to Rawls' idealism. Rawls, on the other hand, writes that the only way peace can be obtained democratically, is if nations can be satisfied. Citing Aron, Rawls argues for a "peace by satisfaction" (as opposed to "peace by power" or "peace by impotence").²⁴⁹ Here, Rawls argues for one of his principles of international relations laid out in the eight principles of the Law of Peoples, the principle of non-intervention, arguing that nations

...must not seek to extend themselves, either to increase their material or human resources, to disseminate their institutions, or to enjoy the intoxicating pride of ruling... Domination and striving for glory, the excitement of conquest and the pleasure of exercising power over others, do not move them against other peoples...Moreover, liberal peoples are not inflamed by what Rousseau diagnosed as arrogant or wounded pride or by lack of due self-respect. Their self-respect rests on the freedom and integrity of their citizens and the justice and decency of their domestic political and social institutions.²⁵⁰

²⁴⁹ Rawls, 47.

²⁵⁰ Rawls, 47.

This also seems to be in direct opposition to Russia’s information security strategy, as well as Putin’s stated goal of countering “Anglo-Saxon” media narratives and news. Yet, at the same time, Russia’s information strategy is only indirectly expansionist. With the annexation of Crimea, Russia clearly revealed their expansionist intentions²⁵¹, but the information strategy employed speak more of an internal, domestic consolidation of power as mentioned above. If the information strategy contributes to Russian expansionism, it is by weakening Russia’s rivals, not by facilitating any expansionist activities directly. As Martin Libicki points out: “The Russians have used national security as an organizing principle to mobilize the people behind the government”²⁵²

The Reciprocity Principle

The isolationism expressed in the information security doctrine, as well as in the adversarial position Russia has taken against the West as expressed through the policies in the action frame described above, is also at odds with Rawlsian principles of foreign policy. Rawls calls for international, cooperative organizations to be formed by peoples in free and just democracies, arguing that leads to stability. Russia’s introspective and isolationist stance as expressed in its information security policies, works against such cooperation. The notions of cooperation and

²⁵¹ Daniel Treisman, “Why Putin Took Crimea,” *Foreign Affairs*, April 18, 2016, <https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea>.

²⁵² Libicki, “Interview, August 28.”

the satisfaction of peoples are components of the overall principle presented by Rawls as a guiding ethical principle for foreign policy, *reciprocity*:

Thus, the criterion of reciprocity applies to the Law of Peoples in the same way it does to the principles of justice for a constitutional regime. This reasonable sense of due respect, willingly accorded to other reasonable peoples, is an essential element of the idea of peoples who are satisfied with the status quo for the right reasons. It is compatible with ongoing among them over time and the mutual acceptance and adherence to the Law of Peoples. Part of the answer to political realism is that this reasonable sense of proper respect is not unrealistic, but is itself the outcome of democratic, domestic institutions.

Rawlsian reciprocity does not necessarily entail reciprocal or escalational retaliation. Using similar tactics against Russia would be counterproductive according to Martin Libicki: “Russia seems to be engaged in a war on fact and on objective reality. That’s not a fight we want to win. It’s not a fight we want them to win”.²⁵³ Libicki points out that even engaging in such a fight would be acknowledging a form of postmodern hyperrelativism, where “there’s your side and my side, and I’m right, because it’s my side”. Winning such a conflict would only be a victory for a point of view, not for objectivity, and would only further lay the ground for polarization. This is another instance of where the current situation mirrors the situation during the Cold War.

²⁵³ Libicki.

American counter-propaganda policies have been based on countering Russian disinformation with “truth” particularly in *Project Truth* of the Reagan era.²⁵⁴

This, of course, leads into a larger epistemological discussion about truth and fact and whether objectivity is even possible in this era of political communication, something Habermas has cast doubt upon.²⁵⁵ Yet, the pursuit of objectivity and truthfulness is essential for Rawls, when it comes to building the basic structure of society. His argument, inspired by Kant, is that untruthfulness cannot be universalized and thus is not ethical. Rawls presents his theory of justice in two divisions: Ideal theory and Non-ideal theory. The latter applies when conditions are such that the former cannot be used. In Rawls’ Ideal theory, truthfulness is essential because lying is by definition unequal. As Kant also showed²⁵⁶, lying will always favor one actor, object or action over another, for what else would be the reason for intentionally not conveying the perceived truth? Rawls’ veil of ignorance not only demands, but facilitates truthfulness, as lying requires knowledge of others’ interests, something the veil of ignorance filters out.

However, Rawls is, of course, aware that untruthfulness and deceit exists in the world and may even be necessary at times. Through non-ideal theory, he allows for what Korsgaard calls

²⁵⁴ Robert Parry, *Lost History: Contras, Cocaine, the Press & "Project Truth"* (Media Consortium, 1999); Arash Abizadeh, “Historical Truth, National Myths and Liberal Democracy: On the Coherence of Liberal Nationalism,” *Journal of Political Philosophy* 12, no. 3 (2004): 291–313, <https://doi.org/10.1111/j.1467-9760.2004.00201.x>.

²⁵⁵ Jürgen Habermas, “Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research,” *Communication Theory* 16, no. 4 (2006): 411–26, <https://doi.org/10.1111/j.1468-2885.2006.00280.x>.

²⁵⁶ Christine Korsgaard, “The Right to Lie : Kant on Dealing with Evil,” *Philosophy and Public Affairs* 15, no. 4 (1986): 325–49.

“temporary inequality”.²⁵⁷ The problem with “temporary inequality” is that it is seen as an exception, only to be applied under certain conditions, and as such, it cannot be universalized, hence its relegation to non-ideal theory. The Rawlsian Frame, however, is defined through Ideal theory, and thus contingent on truthfulness. Any policies based on the Rawlsian Frame cannot entail lying, if it is to adhere to Rawlsian ethics. Congressman Adam Schiff, who himself has studied Rawls and published papers on his principles²⁵⁸, does not believe that the U.S. can ethically defend using similar tactics as the Russians:

I don't think that we should engage in similar kind of activities that the Russians have done, and I don't think the response to the Russian hacking of our democracy should be American hacking of their democracy, or what little democracy they have left. The Russians are doing a good enough job of destroying their own democracy. But I do think we need a strong response. I think we need to establish deterrent and we need to establish rules of the road.²⁵⁹

The “rules of the road” might come in the form of international treaties and agreements, which the Russian information security doctrine is open to, but, as can be read above, it also expresses a lot of skepticism towards joint regulation of information structures such as the Internet.

Deterrence, as mentioned by Congressman Schiff, is part of Rawls' considerations for

²⁵⁷ Korsgaard.

²⁵⁸ Adam B Schiff, “State Discriminatory Actions against Nonresidents: Using the Original Position Theory as a Framework for Analysis,” *Harvard Journal on Legislation* 22 (1985): 583.

²⁵⁹ Schiff, “Interview, May 11.”

international relations. Rawls did his work prior to the emergence of the Internet as a global phenomenon and before its technology was sufficiently advanced to be used for warfare. But in LP, Rawls discusses nuclear weapon deterrence and just warfare. These considerations, however are all based in Non-ideal theory, which again brings up the question of whether the policies discussed here should be constructed based on Ideal or Non-Ideal theory. As mentioned, this is something I shall return to later.

Forging information access inequality

Another dimension of Russia's influence operations in 2016 was, of course, that they were an attempt to circumvent or disrupt the democratic process which Rawls sees as so essential to the basic structure of fair and just democratic society. Needless to say, this goes against Rawlsian principles. One reason for this is that by flooding the information sphere with disinformation, Russian influencers are "crowding out" factual information. I have shown elsewhere²⁶⁰ that if you accept that economies of attention turn campaigning through information into a zero-sum game, it is not trivial that misinformation and fake news take up a larger share of the information market. As the Computational Propaganda Project at Oxford Internet Institute concluded²⁶¹, there are cases in which fake news was shared as often as real news during the 2016 U.S. Presidential

²⁶⁰ Bay, "The Ethics of Psychometrics in Social Media: A Rawlsian Approach."

²⁶¹ Howard et al., "Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?"

election. Scholars such as Fallis²⁶², Van den Hoven and Rooksby²⁶³ support the notion that Rawls' veil of ignorance entails equal access to information, as it would be impossible for those constructing a fair society to do so without information about the stakes. The whole point of the veil of ignorance, in these authors' view, is to make decisions without any preconceptions or prior knowledge, but with the stakeholders possessing a similar level of information. Van den Hoven and Rooksby argue specifically that access to information is a candidate to be one of Rawls' primary goods, i.e. something that everyone has a right to obtain in a fair and just society, and which is essential to the individual's performance of citizenship.

Rawls himself is in fact even more specific in his assertion that in order to assert their political liberties and make use of their primary goods in the democratic process, there is a need for "assurance of a more even access to public media".²⁶⁴ Rawls sees it as imperative that there is equal access to the educational resources necessary to make informed decisions in the deliberative process among citizens he calls "Public Reason"²⁶⁵, which is essential for democracy. The hypertargeted messaging strategies employed by the Russian influencers I have outlined above essentially creates an unequal access to information (which Luciano Floridi argues is truthful as opposed to misinformation²⁶⁶), at least in the social media sphere, as they

²⁶² Fallis, "Information Ethics for Twenty-First Century Library Professionals."

²⁶³ Van den Hoven and Rooksby, "Distributive Justice and the Value of Information: A (Broadly) Rawlsian Approach."

²⁶⁴ Rawls, *Justice as Fairness: A Restatement*, 149.

²⁶⁵ Rawls, *Political Liberalism*, 216.

²⁶⁶ Luciano Floridi, "Understanding Epistemic Relevance," *Erkenntnis* 69, no. 1 (2008): 69–92.

force misinformation upon targeted users and can crowd out the truthful information that untargeted users are exposed to. This way, forcing misinformation upon social media users may keep them from acquiring the information enabling them to make informed decisions. The “even access to public media” Rawls advocates should be viewed in light of the studies that show that a majority of the U.S. population now use social media as source of news.²⁶⁷ Rawls does not mean “public media” as in “public broadcasting”, but publicly accessible media. It can be argued that since social media were not as widespread when Rawls was alive, they would fall under this category when it comes to news distribution.

Chapter conclusion

Overall, the findings of this chapter show a deep divide between the Russian rhetorical and action frames and the Rawlsian Frame. I have shown here that the divide can be described as a conflict between political realism and idealism as guiding principles for policy construction, and similarly, whether Rawls’ Ideal theory is sufficient for policy construction related to social media, or whether Non-Ideal theory is also appropriate. More importantly, the Russia case shows how preventing access to information can be seen as inhibiting the democratic process, which according to both Rawls and the comments made by congressman Schiff above, are highly unethical. The Russian influence campaign of 2016 succeeded in crowding out the truth on a news platform currently being used by roughly half the American population. This was not done through brute force, which would be a simple flooding of social media with messages that were

²⁶⁷ Elisa Shearer and Jeffrey Gottfried, “News Use Across Social Media Platforms 2017,” Pew Research Center - Journalism & Media, 2017, <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>.

not necessarily very effective. Rather through specialization and hypertargeting, by placing the right message in front of the right people, in perfect continuation of the tactics used by the KGB during the cold war, these Russian operatives were able to sow discontent, distrust and animosity among the American people, a tactic that served at least two purposes: To make Russia stand out as a country with a stronger will and more cohesive communal spirit and to weaken the U.S.' image in the places in the world where Russia has economic or strategic interests, from Syria to the African continent.

No matter the result, it is the interference in democratic elections that causes the most friction with Rawls' principles. The ability to crowd out freely submitted and true information on social media with false propaganda is antithetical to Rawls' principles, and it is not just a tactic used in Russian foreign policy. In China, as I will show in the next chapter, it is a tactic that is used by the government on its own people.

Chapter 4: Policies of Control, Surveillance and Oppression on Social Media

Whereas the Russia chapter looked at an outwardly-facing social media policy, in which social media were used in offensive security measures, this chapter will examine how national social media policies can be used to ensure domestic security and stability through surveillance, censorship, promoting self-censorship, limiting access to information and more forceful means of oppression and human rights violations. As in the previous chapter, I will establish rhetorical and action policy frames and contrast them with the Rawlsian frame, but unlike the Russia chapter, the two Chinese frames require more extensive elaboration of the historical background as well as the current conditions for media, and specifically social media, in China. I will provide this background first and then proceed to establish the frames.

Background

A brief history of information and media in post-revolution China

First, it is important to note – as will become clear further along in this chapter – that information policy in China has always been seen as a national security matter. When the creation of the People’s Republic of China was declared on October 1, 1949²⁶⁸ by Mao Zedong on behalf of the Communist Party of China (CPC), it ushered in a new approach to information policies under the new regime. As I shall relay in more detail later, it seemed at first as if China’s new Communist

²⁶⁸ U.S. Dept. of State - Office of the Historian, “Milestones: 1945–1952,” History.state.gov, accessed February 22, 2018, <https://history.state.gov/milestones/1945-1952/chinese-rev>.

leaders saw an informed populace as the way to keep the government in check. But after only a few years, they opted instead for an approach that restricted information access for the masses. Mao died in 1976 after almost 27 years as China's "paramount leader" (an informal term given to the person who, regardless of their actual position within the top councils and committees of the People's Republic of China, is considered the most powerful individual). Since the person considered Mao's natural successor, Zhou Enlai, had died eight months prior to Mao, a struggle for leadership ensued between Mao's last wife, Jiang Qing and Zhou supporters. Jiang was a founder and leader of "The Gang of Four", a group of top committee officials who were later largely blamed for the excesses, abuses and political failures of China's Cultural Revolution from 1966-1976.²⁶⁹ The Gang of Four took over de facto leadership of China for a few weeks after Mao's death, facilitating the instatement of the relatively unknown Hua Guofeng as chairman of the CPC and thereby China's de facto leader. Sensing the animosity towards Jiang Qing and other Gang of Four-related officials, Hua turned against the group and with military backing, had them removed from their positions and arrested. However, Hua lacked political leadership experience and his only merits were his apparent close relationship to Mao, who on his death bed told Hua that "With you in charge, I am at ease".²⁷⁰ Hua's lack of political experience made it evident that China needed a new paramount leader, and over the course of two years, Zhou Enlai's former deputy, Deng Xiaoping moved into that position. Under Deng's leadership, which lasted from 1978 to his retirement in 1989, China relinquished the hyper-

²⁶⁹ Michael Lynch, *Mao* (Taylor & Francis, 2017).

²⁷⁰ Lynch.

protectionist and isolationist policies of the Cultural Revolution and instead moved towards slowly implementing a more market-oriented economy. Opening up towards the West and market reforms set China on a course of historic economic growth, while still maintaining a totalitarian rule by the CPC.²⁷¹ The opening towards the west also meant opening up Chinese media for Western content and influences, which was regarded with suspicion and detriment in many parts of the party. Deng's famous response to this was "If you open the window for fresh air, you have to expect some flies to blow in."²⁷²

Deng's approach, i.e. letting influences in, but defending against them domestically, was maintained by his successors, Jiang Zemin from 1989-2002 and Hu Jintao from 2002-2013. Under Zemin, the Internet came to China, and as it spread, the "flies" became a swarm so big that the Chinese government felt a need to act in order to maintain control. This, as I describe below, led to what is colloquially known as China's "Great Firewall", and more formally known as "The Golden Shield". Still, the introduction of new media platforms in the 1990s was generally welcomed as a way to encourage more freedom of expression and a press corps that would enjoy more liberty. Chu discovered while studying Chinese media on the brink of the introduction of the Internet in China:

The 1980s may well be remembered as the decade of reform in China, as change in all sectors swept across the country, moving steadfastly away from the near total

²⁷¹ Geert Hofstede and Michael Harris Bond, "The Confucius Connection: From Cultural Roots to Economic Growth," *Organizational Dynamics* 16, no. 4 (1988): 5–21, [https://doi.org/10.1016/0090-2616\(88\)90009-5](https://doi.org/10.1016/0090-2616(88)90009-5).

²⁷² Carl Minzner, "China Is Again Slowly Turning in on Itself," *Los Angeles Times*, 2014, <http://www.latimes.com/opinion/op-ed/la-oe-1019-minzner-end-of-china-reform-20141019-story.html>.

politicization and regimentation that characterized the Cultural Revolution. Although media reform is often regarded as an area where change is slowest and hardest, the Chinese mass media have changed so much during the past 15 years that they are now conspicuously distinguishable from those of the past...

The present reform...has seen the rapid development of not only print but also radio and broadcast and satellite television... audiocassettes, videos, karaoke, and cable television are being adopted, legally or illegally. Spread of these new media is making the Party's control extremely difficult.²⁷³

Even as the Internet was introduced in China and the Chinese government began contemplating how to regulate it, obtaining control of the networks and beginning to build the Golden Shield, there was a general sense of optimism among Western scholars. In 2001, shortly after the Golden Shield project was initiated, Harwit and Clarke wrote:

Chat groups in China (as well as the U.S. and other countries of the world) allow virtually unrestricted opportunity for communication among like-minded individuals. For Chinese, such an outlet for discussion offers a potentially powerful medium for anonymous expression of a wide variety of opinion and thought.²⁷⁴

²⁷³ Leonard L Chu, "Continuity and Change in China's Media Reform," *Journal of Communication* 44, no. 3 (1994): 6-14.

²⁷⁴ Eric Harwit and Duncan Clark, "SHAPING THE INTERNET IN CHINA Evolution of Political Control over Network Infrastructure and Content," 404, accessed February 22, 2018, <http://as.ucpress.edu/content/ucpas/41/3/377.full.pdf>.

The authors do state that expression of political views was limited during their study and pointed to self-censorship as being present. Still, they continue:

In sum, the avenues for greater political dialogue are expanding, and as the number and demographics of users change in the coming years, the kinds of discussion will undoubtedly evolve.... As seen above, foreign web content is already widely available to Chinese audiences, and foreign companies have even been able to take limited financial stakes in Chinese ICPs.²⁷⁵

Much has changed since Harwit and Clarke's article from 2001, but the notion that newly emerged media forms would bestow a more Western-style freedom of thought, expression and the press on the Chinese people was strong in the 1990s and early 2000s. Under Hu Jintao, control of the Internet in China became tighter, but it is under current president Xi Jinping that new Internet and cybersecurity policies have really taken on a completely new form, which I will detail further below.

From industrialization to informatization

The Internet was introduced in China in 1994 and has played an important role in the *informatization* strategies of the nation. The first major attempt to regulate the Chinese part of the Internet date back to 1997, where the Ministry of Public Security issued Internet governance regulations with a focus on usage. According to Chan, these regulations stated that "Individuals

²⁷⁵ Harwit and Clark, 406.

are prohibited from using the internet to harm national security; disclose state secrets; or injure the interests of the state or society.” Also in 1997, the first law defining and regulating cybercrime was passed in China.

The term *informatization*, the process of moving towards an information-based economy, was likely coined by Nora and Minc in 1978²⁷⁶ In official translations of Chinese state documents, this term is used as a translation of the term *Xinxihua*, and I will consider this translation to be proper.

According to Qiang et al., informatization can be traced back to the 1970s in China, but grew significantly in the 1990s, as in many other regions of the world, due to the proliferation and growth of the Internet. In the early 2000s, the Chinese government took informatization on as a national strategy by including it in its five-year economic plan for 2006-2011, but also in the longer-term State Development Informatization Strategy 2006-2020. These state-led initiatives not only have the purpose of extending information technologies and the Internet to rural areas in China, but also to push China forward in the international arena as a dominant producer of technological products.²⁷⁷

The Golden Shield Project AKA The Great Firewall

The phrase “The Great Firewall of China” was likely coined an article in Wired Magazine in 1997, which bore that exact title. Journalists Geremie Barmé and Sang Ye described the early

²⁷⁶ Simon Nora and Alain Minc, *L'informatisation de La Société: Rapport à Monsieur Le Président de La République*, vol. 3 (La Documentation française, 1978).

²⁷⁷ Nagy K. Hanna et al., *Rural Informatization in China*, World Bank Working Papers (The World Bank, 2009), <https://doi.org/10.1596/978-0-8213-8018-5>.

implementations of technical measures and regulations that would monitor and censor the Internet as it was accessed by Chinese citizens.²⁷⁸ The formal name for the “Great Firewall”, as mentioned above, is “The Golden Shield”. This umbrella term covers a large operation of censorship, surveillance and filtering taking place at both the hardware, software and the application/content levels. The Golden Shield project was launched in 2000, when more than 300 companies from 16 different nations attended a conference and trade show organized by, among others, The Chinese Communist Party’s Central Committee Commission for the Comprehensive Management of Social Security. As Walton described it:

A central feature of the show was the Golden Shield Project, launched to promote “the adoption of advanced information and communication technology to strengthen central police control, responsiveness and crime combating capacity, so as to improve the efficiency and effectiveness of police work. At the show, China’s security apparatus announced an ambitious plan: to build a nationwide digital surveillance network, linking national, regional and local security agencies with a panoptic web of surveillance.”²⁷⁹

Since then, the Golden Shield has grown into a massive system that bridges the gaps between technology and institutions in China. The technical side of The Golden Shield is overseen by China’s National Computer Emergency Response Team & Coordination Center (CNCERT/CC).

²⁷⁸ Geremie Barmé and Sang Ye, “The Great Firewall of China,” *Wired*, 1997, <https://www.wired.com/1997/06/china-3/>.

²⁷⁹ Greg Walton, “China’s Golden Shield,” *Human Rights in China 中国人权 | HRIC*, 2002, <https://www.hrichina.org/en/content/4598>.

This agency is placed under the Ministry of Industry and Information Technology (MIIT), which also supervises its work. These two instances are components of a larger hierarchy responsible for policy-making, regulation and enforcement/governance of the Internet in China. As Chan describes it:

...at the top are two major leading groups that monitor the internet, namely the Central Leading Group for Propaganda and Ideological Work (CLGPIW) and Central Leading Group for Internet Security and Informatization (CLGISI). These provide guiding principles and policies to agencies like the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT), the Ministry of Industry and Information Technology (MIIT), the State Internet Information Office (SIIO), and the Cyberspace Administration of China (CAC) that regulate and coordinate the industry.²⁸⁰

The CAC may be placed lower in the hierarchy, but it has immense power and influence. This is affirmed by the fact that Xi Jinping himself is the official leader of the agency, and the CAC was launched upon his initiative in 2014.

As mentioned, the Golden Shield has both a technical dimension and a legislative one. The agencies and institutions mentioned above engage in regulatory action towards Internet Service Providers (ISPs) telecom service providers and network operators in China, which includes

²⁸⁰ Susanne Chan, "Cybersecurity under Xi Jinping: A New Model for Broad Control in China," Center for the Digital Future, 2018, <http://www.digitalcenter.org/columns/cybersecurity-under-xi/>.

forcing them to implement censoring and filtering technology. According to Xu et al.²⁸¹, the filtering mechanisms are placed on the gateways where international Internet traffic physically enters the country via fiberoptic cables (See Fig. 3) as well as on ISP servers connecting users to the Internet.

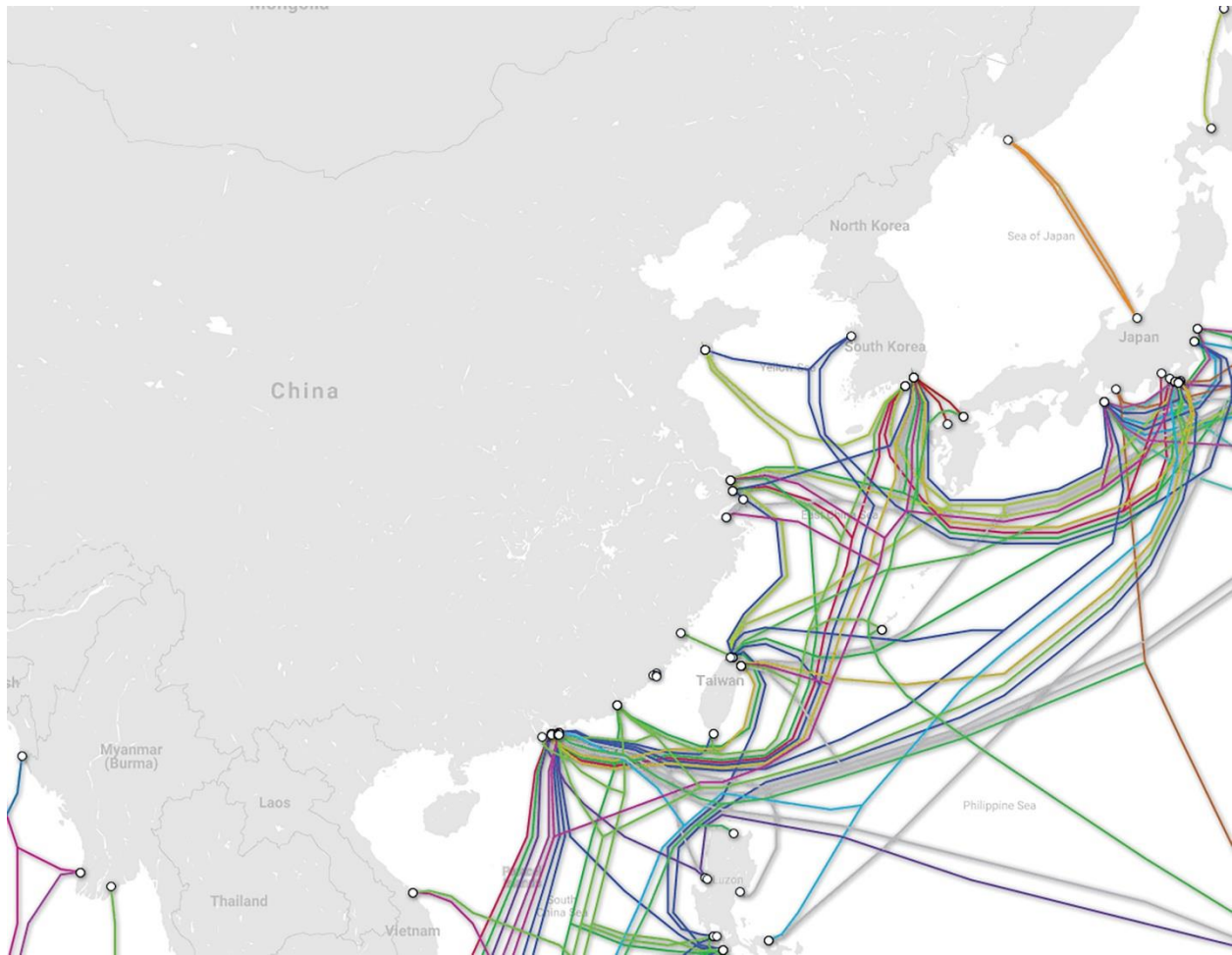


Figure 3. The international, submarine telecommunications cable landings in China in February 2018 (Source: TeleGeography/www.submarinecablemaps.com)

²⁸¹ Xueyang Xu, Z Morley Mao, and J Alex Halderman, “Internet Censorship in China: Where Does the Filtering Occur?,” accessed February 19, 2018, <http://www.cse.umich.edu>.

Contrary to popular belief, it is not the original, incoming Internet traffic that is monitored and filtered. Instead, all Internet packets are copied and sent through a parallel system where it is inspected through Deep Packet Inspection (DPI). If certain undesired keywords or patterns are detected, the system employs one of several options to block the traffic. One method is TCP Reset, where a TCP RST message is sent to both the client trying to access the traffic and the server sending it. This message is injected into the original packet stream. To both client and server, it will look like the connection is lost.²⁸² Other measures simply blocks the user from accessing certain domains. An example of this is DNS poisoning, where the Chinese authorities enter defective IP numbers into the tables on the DNS servers that users access in order to transform a URL to an IP number. Blocking also occurs by routing users to state-controlled DNS servers that simply don't allow users to find a certain domain's IP address and access it.²⁸³ This way, the Chinese authorities are able to tightly control and monitor Chinese users on the Internet who are all subject to technological surveillance of their every action online. King et al. found that some criticism of the government is allowed, but a line is drawn as soon as signs of mobilization appear²⁸⁴: "In both cases, the censorship apparatus allows a great deal of criticism

²⁸² Chao Tang, "In - Depth Analysis of the Great Firewall of China," 2016, <https://www.cs.tufts.edu/comp/116/archive/fall2016/ctang.pdf>.

²⁸³ Chris Hoffman, "How the 'Great Firewall of China' Works to Censor China's Internet," How-to Geek, 2016, <https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/>.

²⁸⁴ Gary King, Jennifer Pan, and Margaret E. Roberts, "Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation," *Science* 345, no. 6199 (2014), <https://gking.harvard.edu/publications/randomized-Experimental-Study-Censorship-China>; Gary King, "How Censorship in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review*, 2013, <https://doi.org/10.1017/S0003055413000014>.

of the regime, its officials, and their policies (which can be useful information for the central government in managing local leaders) but stops discussions that can generate collective action on the ground”²⁸⁵

Means of circumvention are quite popular in China, including web browsers that use dedicated DNS servers to avoid DNS poisoning, and VPNs that will mask the user’s location and IP number. China’s government has cracked down on the latter since 2012, by outlawing the sales or distribution of any type of circumvention software.²⁸⁶ In early 2018, however, the Chinese authorities seem to have shifted their attention to corporations rather than persons, as finding and prosecuting individual VPN users in China has proven difficult and costly.²⁸⁷

Margaret E. Roberts is assistant professor in the Department of Political Science at University of California San Diego, where her research focuses on China and social media censorship. She is a co-author of the King et al. studies mentioned in this chapter, being one of only very few Western researchers who has done both quantitative and qualitative research with regards to social media and freedom of expression in mainland China. Her list of publications on the subject is quite extensive. When I interviewed her for this study, she confirmed that

²⁸⁵ Gary King, Jennifer Pan, and Margaret E Roberts, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,” *American Political Science Review* 111, no. 3 (2017): 484, <https://doi.org/10.1017/S0003055417000144>.

²⁸⁶ Anthony Kuhn, “VPNs In China: Behind Internet Crackdown, ‘Game Of Cat And Mouse’ Continues,” NPR.org, 2017, <https://www.npr.org/sections/alltechconsidered/2017/08/04/541554438/behind-chinas-vpn-crackdown-a-game-of-cat-and-mouse-continues>.

²⁸⁷ Lucy Hornby, “China’s VPN Crackdown Is about Money as Much as Censorship,” *Financial Times*, 2018, <https://www.ft.com/content/35eafc9a-fcf8-11e7-9b32-d7d59aace167>.

It is mostly companies who distribute VPNs that get punished for it, not individuals. It isn't illegal to use VPNs in China, but the government is considering making it illegal. At this point, I think 3-5% of the population use VPNs, which is a lot of people, considering China's size, even if it is a small percentage.²⁸⁸

Roberts generally attributes this use of VPNs to pragmatism, and told me that there is a significantly faster adoption of VPNs and other means of circumventing the Golden Shield when censorship sets in suddenly:

People in China use VPNs when they want to get information they don't feel like they are getting, especially if they've had access to the information before. The Chinese government blocked Instagram use in China very suddenly in September 2014 because images were being posted of the protests that were going on in Hong Kong. The sudden shutdown caused a surge in VPN installations, and people found out that once they had the VPN installed, they could also access other sites. So around that time, Twitter saw a 600% rise in signups from China, and large numbers of Chinese Internet users flocked to the Wikipedia page about the Tianamen Square massacre.²⁸⁹

Roberts is quick to point out that it is the elite who mostly use VPNs:

²⁸⁸ Margaret E. Roberts, "Interview 4/18/2018," 2018.

²⁸⁹ Roberts.

These are tech or finance people in the cities who are better educated, have foreign friends that they keep in touch with on social media and who also read foreign news sources. This is a characteristic of China's digital divide. This way, censorship definitely contributes to the inequality in China.

Social Media in China

As can be seen from Margaret E. Roberts' account of the blocking of Instagram in 2014, Western social media platforms are often able to start up in China before they are shut down by the government. Before access to Instagram was cut off in 2014, Facebook and Twitter had both been blocked in 2009. WhatsApp was blocked in China in 2017. This strategy has pushed Chinese users towards China's own services, a trend that is aided by the absence of a language barrier.

The most popular social media platforms in China are based around instant messaging as the central function, with added social functionalities which makes them closer resemble Western social media services. Two prominent examples of this are WeChat and QQ, both owned by the Chinese investment corporation Tencent Holdings Limited. QQ began as a web portal, a service that is still quite popular. According to Tencent's own financial results report from the third quarter of 2017²⁹⁰, WeChat had a MAU number (Monthly Active Users) of 980 million, while QQ's MAU was 843 million. WeChat was born as a mobile application, while QQ made the transition from the computer to mobile after having existed as a web service for several

²⁹⁰ Tencent, "TENCENT ANNOUNCES 2017 THIRD QUARTER RESULTS 3Q2017 Financial Review" (Hong Kong, 2017), <https://www.tencent.com/en-us/articles/8003451510737482.pdf>.

years. Hence, all of WeChat's users are mobile, while a vast majority of QQ's users, 653 million, access the service from what Tencent calls a "smart device", which in China in 2017 essentially means a mobile device. Whereas Facebook began as a profile- and networking-oriented social media platform and has since branched out into instant messaging through Facebook Messenger and the acquisition of WhatsApp, QQ and WeChat did the opposite. QQ was launched in 1999 as a Chinese version of a then-popular messaging service in the West, ICQ. Named OICQ ("Open ICQ"), it quickly received a complaint over trademark infringement from America On-Line (AOL) who had acquired the Israeli-developed ICQ service the previous year²⁹¹ It then changed its name to QQ and launched as a web portal, maintaining its messaging/chat component. It grew to become China's most popular social media platform, adding personal profiles and rich content to the core messaging function, as social media platforms such as Friendster, MySpace and Facebook became popular in the West in the early 2000s. When Tencent launched the mobile app WeChat in 2011, it quickly became more popular than QQ due to the rising popularity of smartphones in China. In 2017, QQ made a push to transform the platform "from a pure messaging app into one that supports chatting, sharing, interest groups, and digital content like games, anime, literature, music, live streaming, and so on".²⁹² WeChat has already succeeded in providing rich media services, including sharing of images, videos and video conferencing. In providing the latter and not focusing so much on user profiles, WeChat is similar to U.S.-owned

²⁹¹ Zhang Zhao, "Long Conflict over QQ Continues into Court|Business|chinadaily.Com.Cn," China Daily, 2013, http://usa.chinadaily.com.cn/epaper/2013-07/24/content_16824251.htm.

²⁹² Rita Liao, "WeChat's Older Sibling QQ Plans to Stay Forever Young · TechNode," Technode, 2017, <http://technode.com/2017/08/07/wechats-older-sibling-qq-plans-to-stay-forever-young/>.

social media platforms such as Instagram and Snapchat as well as messaging services like WhatsApp.

If WeChat and QQ can be compared to Facebook, Instagram, Snapchat and WhatsApp, the third-largest social media platform in China, Sina Weibo, compares to Twitter. Sina Weibo is one of several services offering “weibo”, or microblogging. Other providers of “weibo” services include the official newspaper of the Chinese Communist Party, *People’s Daily*, and the aforementioned Tencent, who runs a competitor to Sina Weibo. But the Sina Weibo service is by far the most popular, enabling the company behind it, Sina, to spin off the service and rename it, simply, “Weibo” in 2014, in connection with an IPO. In May 2017, Sina Weibo overtook its Western counterpart in popularity. Weibo reported a MAU in excess of 340 million, compared to Twitter’s MAU of 328 million²⁹³

Though Weibo, QQ and WeChat are currently the dominant platforms, changes are underway that mirror the changes happening on social media in the West. A study of the Chinese social media sphere by market intelligence company Kantar showed that the social media user population is stratifying onto more usage-specific or topic-oriented platforms. An increasing number of social media users will spend their time socializing online through social functionality made available on news sites, e-commerce sites or other platforms unrelated to the social media corporations.²⁹⁴

²⁹³ Staff, “Twitter User Numbers Overtaken by China’s Sina Weibo,” BBC News, 2017, <http://www.bbc.com/news/technology-39947442>.

²⁹⁴ Martin Guo, “Kantar China Social Media Impact Report 2017 - Kantar,” Kantar China Insights, 2017, <https://cn-en.kantar.com/media/social/2017/kantar-china-social-media-impact-report-2017/>.

The strength and domination of these Chinese social media platforms is aided by the Chinese government's protectionist policies with regards to social media. The social media platforms dominant in the West, such as Facebook, Twitter, Instagram, Snapchat and Pinterest are either banned in China (i.e., access is prohibited and blocked through the Golden Shield) or have withdrawn from the market due to restrictions put in place by the Chinese government as of February 2018. This is also the case for Google, including their socially-oriented services such as YouTube and Google Plus.²⁹⁵ Russia's largest (and partly government-owned) social network, VKontakte, was banned in China between 2016 and 2018, but the ban has been lifted after pressure from the Russian government as of February 2018.²⁹⁶

China's two-tier media system

There appears to be a consensus among outside observers that news and information conveyed through mass media currently runs on two parallel tracks in China. One attempts to be an independent watchdog on behalf of the population, including against the government. The other is the state-controlled messaging proliferated through state-run media and other means.

However, some scholars now point to a convergence of the two, enforced by the Xi administration.

²⁹⁵ Sherisse Pham and Charles Riley, "Banned! 11 Things You Won't Find in China," Cnn.com, 2017, <http://money.cnn.com/gallery/technology/2016/05/23/banned-china-10/7.html>.

²⁹⁶ Staff, "Russia's Media Watchdog Boasts It 'Convinced' China to Lift Vkontakte Ban," The Moscow Times, 2018, <https://themoscowtimes.com/news/russia-media-watchdog-boasts-it-convinced-china-to-lift-vkontakte-ban-60523>.

In October 1998, then-prime minister Zhu Rongji visited the tv studios of China's national broadcaster CCTV. He was the featured guest of the investigative reporting news program *Jiaodian Fangtan*, a very popular show in China at the time, attracting audiences upwards of 300 million viewers. On air, the prime minister praised the program and emphasized how it helped inform the country's leaders in their decision-making. More importantly, he stressed the program's role in Chinese society as an instrument of "public supervision". He also called it "The people's mouthpiece", the "government's mirror" and the "vanguard of reform".²⁹⁷ But it was the first phrase that stuck. Since then, "public supervision" has been an expression used about media and news outlets in China that strive for independence and are willing to criticize government policies. "Public supervision" should be understood as the public holding the government accountable, not that the public is under supervision. For almost two decades, Rongji's approach to the media as being watchdogs on behalf of the public seemed to slowly spread across a China that was otherwise used to tightly state-controlled media narratives. It seemed like a natural step in the process that had begun with the opening towards the West and gradual marketization of the Chinese economy under Deng Xiaoping in 1978-1979. Four years prior to Rongji's appearance on *Jiaodian Fangtan*, China was connected to the Internet. Only two years later, in 1996, did China first begin regulating the Internet, legislation that would later become the foundation of the "Great Firewall".²⁹⁸ At first, this regulation was mostly in place to

²⁹⁷ Alex Chan, "From Propaganda to Hegemony: Jiaodian Fangtan and China's Media Policy," *Journal of Contemporary China* 11, no. 30 (2002): 38, <https://doi.org/10.1080/10670560120091138>.

²⁹⁸ Jack Linchuan Qiu, "Virtual Censorship in Chin: Keeling the Gate Between the Cyberspaces," *International Journal of Communications Law and Policy Issue* 4 (1999), www.ijclp.org.

establish the organizational/governmental structure in which the Internet, ISPs and other service providers would be regulated in China, but there were provisions against ““harmful information” that is either “subversive” or “obscene””.²⁹⁹ The relaxed (compared to current) legislation can be viewed as a sign of the general atmosphere at the time, which also led to Rongji’s CCTV visit and praise of investigative journalism as a watchdog of the people. The introduction of the Internet did not lead to a sudden liberalization of the media, however, and some scholars argue that the seemingly increasing freedom of the press was mostly for show. As Susanne Chan, a media scholar at Hong Kong University writes of the current media landscape in China:

News reporting, for instance, has morphed into a two-tier system where a market-oriented appropriation of public opinion supervision (*yulun jian du* 舆论监督) exists alongside traditional propagandistic reporting. Investigative journalism and strategic/selective censorship that break the rule of positive reporting have been used increasingly since the 1990s to enhance its appeal to readers while maintaining Party hegemony under the guise of seeming liberalization.³⁰⁰

In an interview conducted as part of the present study, Chan told me that the emergence of a private media market has grown to be a threat to the Chinese state’s ability to control public opinion by diminishing the space for propaganda:

²⁹⁹ Qiu, 11.

³⁰⁰ Chan, “Cybersecurity under Xi Jinping: A New Model for Broad Control in China,” 2.

The introduction of various sorts of responsibility systems dramatically transformed the ways organizations were financed... Propaganda remains important and the party press will never be fully marketized, but there has been rising competition from more consumer-oriented newspapers. The challenge is in part financial but mostly political, and the party press needs to adapt to increase its appeal to readers... So for some party news groups, they may run both parent papers that are primarily responsible for disseminating propaganda, and affiliated ones, like metropolitan dailies that focus more on the commercial market and which would generate more profits.³⁰¹

Some scholars argue that propagandistic reporting has usurped public supervision under Xi Jinping. Bandurski quotes Chinese media scholar Xiao Zhitao, from the Communist party's official *Red Flag* publication in the summer of 2016:

In our country, the media run by the Party and the government have always been the main force in supervision by public opinion. However, in recent years, with the steady emergence and development of new media, and as competition between domestic and international media grows ever more dramatic, certain media have engaged in the one-sided exercise of supervision by public opinion power—and a good number of journalists have fallen into the trap of the West's so-called “freedom of the press,” the “fourth

³⁰¹ Susanne Chan, “Interview, 2/27/2018,” 2018.

estate,” the [idea of the journalist as the] “uncrowned king.” This has been extremely damaging to the Party’s news and public opinion work.³⁰²

Bandurski claims this is a return to a type of media control that China hasn’t seen in a long time:

Supervision under Xi Jinping is to be an internal matter, a backstage ritual. Criticism must be managed, supervision supervised. We might say that the PRC’s second era of critical reporting is at its end, at least as a matter of policy. The gap is closed. Positive propaganda and supervision are unified. Welcome to 1954.

As Bandurski points out, the idea of “public supervision” did not originate with Zhu Rongji’s visit to the CCTV news studios. Neither did it originate when then-prime minister Zhao Ziyang included the concept in a 1987 political report. The concept was part of the early conception of the Chinese republic:

On August 30, 1950, when the People’s Republic of China was still less than a year old, an article on page five of the People’s Daily (“Criticism and Self-Criticism in the Newspaper”), said that newspapers must be used to carry out a “firm struggle” against government officials who tried to suppress criticism of their actions and policies. In such instances, said the paper, “[we] must when necessary organise the collective strength of the readers to carry out mass supervision by public opinion, thereby reaching the goal of criticism.” This article came just four months after the Party’s Politburo passed its

³⁰² David Bandurski, “Supervising Supervision,” China Media Project, 2016, <https://medium.com/china-media-project/supervising-supervision-6812858d5828>.

“Chinese Communist Party Decision On Newspapers and Periodicals Carrying Out Criticism and Self-Criticism,” which underscored the role of the media in carrying out criticism of the Party and government in order to combat such trends as “bureaucratism.”³⁰³

In 1954, however, the party reversed its course. In the document “CPC Central Committee Decision on the Improvement of Newspaper Work”, the Chinese leadership warned journalists against any unwanted criticism of the party and the state. This was almost five years into the rule of Mao Zedong, and the first of many decisions that constituted the totalitarianism of his regime. Thus, Bandurski sees the current media policies of the Xi administration as heralding a return to the same type of oppression, at least when it comes to dissent.

In 2008, one of the first heralds of tighter regulations of the press and the Internet in China came in the form of a speech by then-president Hu Jintao. Ten years then-prime minister Zhu Rongji had visited Chinese state TV with the opposite message (see below), the president at the time, Hu Jintao, paid a visit to the offices of the state-run newspaper People’s Daily on the occasion of its 60th anniversary,

The People’s Daily is the state news outlet and is expected to propagandize, but importantly, Hu Jintao equated “press and propaganda work” throughout the speech, and stressed how essential it is to shaping the public opinion in ways that is desirable for the government:

³⁰³ Bandurski.

In the new situation, press and propaganda work must hold high the banner, serve the overall interests of the people, serve the people, reform and innovation, uphold the correct guidance of public opinions, improve the guidance of public opinion, create a good public opinion environment, give better play to propaganda of the party's advocacy, promote social integrity, and promote social conditions [for] public opinion, guide social hot spots, divert public sentiment, and improve the important role of public opinion supervision.

As I shall show below, “public opinion supervision” is a concept that was touted by Hu’s predecessors – but by 2008, it seems to have a lower priority. About the internet and online media, Hu said:

We must fully understand the social influence of emerging media represented by the Internet, attach great importance to the construction, use and management of the Internet, and strive to make the Internet an advanced culture for the dissemination of socialism.³⁰⁴

On the 27th of November 2012, as he was preparing to step down and hand over leadership to Xi Jinping a few months later, Hu told the 18th CPC Congress:

We should improve the contents of online services and advocate healthy themes on the Internet. We should strengthen social management of the Internet and promote orderly

³⁰⁴ People’s Daily Staff, “在人民日报社考察工作时的讲话--时政--人民网,” People’s Daily, 2008, <https://politics.people.com.cn/GB/1024/7408514.html>.

network operation in accordance with laws and regulations. We should crack down on pornography and illegal publications and resist vulgar trends.

Hu also paved the way for his successor's cybersecurity policies by stating that China should "enhance the capability to accomplish a wide range of military tasks, the most important of which is to win local war in an information age."³⁰⁵ Indeed, this was a policy that Xi Jinping would take to a whole new level. During Xi's tenure so far, he has attempted to reverse the tendencies towards openness that characterized the first decade of the 2000s. He has done so through centralizing the power of the institutions that govern the Internet in China and by presenting a value-based/normative motivation for why the Internet and social media must be censored by the government. This is apparent in the rhetoric surrounding Internet governance coming out of the Xi administration, which I will now proceed to explore.

Rhetorical Frame

In the following, I will construct the rhetorical policy frame for China's information policies, based primarily on public statements by Chinese President Xi Jinping as well as publications of recent legislative agendas and policy documents.

Centralization of media policy and consultation

³⁰⁵ Hu Jintao, "Hu Jintao's Report at 18th Party Congress," China-embassy.org, 2012, http://www.china-embassy.org/eng/zt/18th_CPC_National_Congress_Eng/t992917.htm.

When Xi Jinping assumed power in April 2013, he began working toward reforms that leaned more towards nationalism. This was made apparent by the policy platform document adopted by the 18th CPC Central Committee on November 12, published on November 16, “The Decision on Major Issues Concerning Comprehensively Deepening Reforms in brief”.

The document clearly specifies a continuation of Deng’s “opening-up” policies, as well as deregulation of markets and expansion of property rights, all in order to forward the marketization of the Chinese economy. Two clauses stand out that will be of significance in the application of Rawlsian principles further along in the chapter:

28. Push forward the multi-layer development of the consultative democracy system.

Enhance the construction of new types of think tanks with Chinese characteristics.

Promote a consultative policy system. Strengthen and develop equal, unified and harmonious ethnic relationships. Governments should seek advice from the local Chinese People's Political Consultative Conference before making important decisions.

29. Develop grassroots democracy. Improve the system of grassroots election, discussion, publicity and responsibility. Improve supervision by urban residents and villagers.

Improve the democratic management system, such as the workers' representative conferences, in companies and government institutions.³⁰⁶

³⁰⁶ Communist Party of China, “The Decision on Major Issues Concerning Comprehensively Deepening Reforms in Brief- China.Org.Cn,” China Daily, 2013, http://china.org.cn/china/third_plenary_session/2013-11/16/content_30620736_3.htm.

Of note here is the mention of the “consultative democracy system”. “Consultation” in this regard refers to the extent of which the government consults the people on matters of regulation and governance. In a Rawlsian context, society is constructed by the people from consensual principles of common interests and thus, the ability to extend or change the structures is built into the system through required transparency and just, democratic institutions. I.e., there is no need to “consult” the people in a well-ordered, Rawlsian democracy, as the system requires the people’s participation in order to even exist. It is a socially collaborative effort based on duty, hence the designation of Rawls’ ethics as being deontological. When a system of government is centralized instead, as in China, the disconnect with the public is more substantial. The paternalism inherent in such a system (which I shall return to later) requires consulting the people in order to assess their needs and wants, which should ideally guide the government. In other words, instead of letting the people put together the government through elections or holding referendums on important policy matters, a “consultative democracy system” asks the people about their wants and needs through other means, such as the news media, polls and social media interaction. Rawls operates with a concept known as “decent consultation hierarchy”, and in the discussion part of this chapter, I shall return to whether China’s policies qualifies it for this kind of designation.

A litmus test for journalists

In part XI of the policy declaration, the party lays out a cultural policy, which mostly points towards privatization of cultural institutions, and opening for both foreign, domestic and public investments in cultural products. This is the background for the attempts at converging Chinese

and U.S. cultural production in, among other things, film.³⁰⁷ But article XI also includes this passage:

Transfer the role of the government from being the provider of cultural products to the manager. Improve the mechanism for dealing with emergencies on the Internet.

Institutionalize the government information release system and standardize the vocational qualifications of journalists.

The first line in the passage is a clear indication that the Chinese government might privatize parts of their cultural production, but they will still “manage” it, and this unspecific language gives the government wide authority to set boundaries for expression through cultural products. Similarly, the “mechanism for dealing with emergencies on the Internet” that follows, seems oddly out of place, unless it is to be interpreted as part of a cultural context. What are the “emergencies” that could happen on the Internet in a cultural context? This is also an example of vague language that gives the government wider authority to define the boundaries, even ad hoc. Finally, standardizing “the vocational qualifications of journalists” seems to imply that the government can set rules for who can’t and cannot express themselves in public media – at least in journalistic relations – which would be considered a violation of freedom of speech in the West.

³⁰⁷ Staff, “‘Great Wall’ May Crumble, But More China-U.S. Films Are Coming,” Bloomberg News, 2017, <https://www.bloomberg.com/news/articles/2017-02-17/-great-wall-may-crumble-but-more-china-u-s-films-are-coming>.

Consultational democracy as paternalistic enforcement of societal order

Almost six weeks later, the remarks President Xi Jinping made to accompany the policy document were made public. Here, he offered some elaboration on some of the vague language in the document. After detailing how the policy document came to be through a deliberative process in the Central Committee, Xi explained the main points of each article. Importantly, Xi still defines China as a developing nation, where economic disparities are large and growing, and where rural areas are drastically underserved. He then explains his perspective on the market economy in China: “After 20 years of practice, a socialist market economy has been basically established in China. But there are still many problems. The market lacks *order* and many seek economic benefits through unjustified means.” (Italics mine)³⁰⁸ Xi does not define “unjustified means” and this phrase is left to be understood as either illegal or simply immoral “means”.

Xi explains the aforementioned “consultational democracy” concept thus:

Promoting consultative democracy is conducive to improving the people's *orderly* participation in political affairs, strengthening the ties between the Party and the people. Under the leadership of the Party, China will promote consultation throughout society with regard to major issues of economic and social development and practical issues closely related to the interests of the people and adhere to the principle of consultation before policy-making and during policy implementation. We will build a consultative democracy featuring appropriate procedures and complete segments to expand the

³⁰⁸ Xi Jinping, “Explanatory Notes for the ‘Decision of the Central Committee of the Communist Party of China on Some Major Issues Concerning Comprehensively Deepening the Reform’ (2) - People’s Daily Online,” People.cn, 2014, <http://en.people.cn/102774/8525245.html>.

consultation channels of the organs of state power, committees of the Chinese People's Political Consultative Conference, political parties, and community-level and social organizations; conduct intensive consultations on issues relating to legislation, administration, democracy, political participation and social problems; give full play to the important role of the united front in consultative democracy, make the Chinese People's Political Consultative Conference serve as a major channel for conducting consultative democracy, improve the system of the CPPCC, specifying the contents and procedures for consultation, increase the forms of consultative democracy, and more actively carry out consultations on particular topics, and with specialists and representatives from all sectors of society, and with the relevant government departments on the handling of proposals, to improve the intensity and effectiveness of the consultations. (Italics mine)³⁰⁹

Note that the media are not considered a channel of consultation.

Order as value in Internet and market governance

When it comes to the Internet, Xi dedicates an entire section of the speech to it and lays the groundwork for later policy decisions: “**Eight, accelerating the improvement of the leadership for the management of the Internet.** Internet and information security bear on national security and social stability and pose new challenges for us in many aspects.” (emphasis in original). He goes on to state how the government’s “management” of the Internet is “seriously flawed and

³⁰⁹ Jinping.

cannot function properly”, not least because of a very fragmented system of oversight with multiple agencies looking after specific functions. Xi then continues:

Also, as the Internet grows into a new form of media, the management of this online medium and the industry is lagging far behind the development of the business. With fast growth in the users of micro-blogs, WeChat and other social network services and instant communication tools, which spread information quickly and can mobilize large numbers of users, how to strengthen oversight within a legal framework and guide public opinion, and how to ensure the orderly dissemination of online information, while at the same time safeguarding national security and social stability have become pressing problems for us.

It is clear from this passage that Xi’s approach to the possibilities of expression online is that requires “oversight” and “management” and that the ability to “mobilize large numbers of users” might be a “pressing problem” for “national security and social stability”. Xi explains how the new, adopted policy points towards a solution:

The Decision stipulates that we must adhere to the principles of active usage, scientific development, management in accordance with the law and ensuring safety in strengthening management of the Internet in accordance with the law, and accelerating the improvement of leading institutions for Internet management. The aim of this is to integrate the functions of the related departments and form joint forces in the

management of the Internet covering both technology and contents, and ranging from daily security to combating crimes, to ensure correct and safe Internet usage.³¹⁰

From a Western standpoint “correct” Internet usage may seem like an odd choice of words, but I will explain the moral implications of this later in the chapter. The excerpt above is important for another reason. It lays the foundation for the establishment of the Cyberspace Administration of China (CAC) in 2014, which Xi leads himself. In February of that year, Xi gave a short speech at the first meeting of the committee that oversees the agency, where he said that “Internet security and informatization is a major strategic issue concerning a country’s security and development as well as people’s life and work”³¹¹, During the meeting, Xi elaborated by saying that this meant both in terms of domestic access to the Internet, even in rural areas, but also in terms geopolitical matters and national security writ large.³¹² However, it was what Xi told reporters after the committee meeting that garnered most headlines in the press. Here, he said that he thought “efforts should be made to build our country into a cyber power” and, more importantly, that “No Internet safety means no national security. No informatization means no modernization”.³¹³ This slightly more aggressive stance, in combination with China’s

³¹⁰ Jinping.

³¹¹ Shannon Tiezzi, “Xi Jinping Leads China’s New Internet Security Group,” *The Diplomat*, 2014, <https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/>.

³¹² Ankit Panda, “Xi Jinping: China Should Become a ‘Cyber Power,’” 2014, accessed February 22, 2018, <https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/>.

³¹³ Panda.

investments on the African continent and increased military spending proposals contained in the policy platform document mentioned above, has caused some observers to be concerned that China may be moving away from their position of non-interventionism, which they have assured international community of since 1954.³¹⁴ More importantly, by equating “Internet safety” with national security and informatization with modernization, Xi effectively justified considering any sort of wrongdoing on the Internet as a threat to national security and the progress of the nation.

When I emphasized the references to “order” in the market and on the internet in the Xi quotes above, it has a dual purpose. It is related to the Confucianist notions I shall outline below, but it is also simply part of Xi’s political narrative, his framing of his administration as one that sets about restoring order. Not only does this set the premise that the current state online and in the market is one of *disorder* (an assumption that is never substantiated in Xi’s rhetorical policy framing), but it naturally also puts Xi in a historical cadre of leaders who have used this rhetorical tactic, such as Richard Nixon³¹⁵ (and inspired by him, Donald Trump³¹⁶) to Adolf

³¹⁴ Sherif A. Elgebeily, “How China’s Foreign Policy of Non-Intervention Is All about Selective Action,” South China Morning Post, 2017, <http://www.scmp.com/comment/insight-opinion/article/2091502/how-chinas-foreign-policy-non-intervention-all-about>; Madison Condon, “China in Africa: What the Policy of Nonintervention Adds to the Western Development Dilemma,” *PRAXIS The Fletcher Journal of Human Security* 27 (2012), <http://fletcher.tufts.edu/~media/Fletcher/Microsites/praxis/xxvii/2CondonChinaAfrica.pdf>.

³¹⁵ Julia Azari, “From Wallace To Trump, The Evolution of ‘Law And Order,’” FiveThirtyEight, 2016, <https://fivethirtyeight.com/features/from-wallace-to-trump-the-evolution-of-law-and-order/>.

³¹⁶ Josh Zeitz, “How Trump Is Recycling Nixon’s ‘Law and Order’ Playbook,” Politico Magazine, 2016, <https://www.politico.com/magazine/story/2016/07/donald-trump-law-and-order-richard-nixon-crime-race-214066>.

Hitler and his reliance on Georg Usadel's national socialist ethics based on "Zucht und Ordnung" – discipline and order.³¹⁷

Even before the official events described above, after only five months in office, Xi spoke to a group of propaganda chiefs in Beijing, in which he described how his administration was going to crack down on those who would spread "rumors" online or celebrities whose popularity grew so big online that they would be able to influence or even mobilize their many followers. To this end, Xi ordered the propaganda chiefs to "build a strong army" that could "seize the ground of new media". One source thus claimed that Xi encouraged the party to be "combative" rather than "passive", which again goes against the non-interventionist stance of prior administrations as mentioned above.

With this kind of rhetorical justification and no real political opposition, turning policy into regulation and enforceable law was an easy task for the Xi administration. In the next section, I will describe how it happened and which impact these policies had and continue to have in China.

Action Frame

The action frame constructed below consists of analyses of actions taken by the CPC and the Chinese government as consequences of the policies laid out above, including interpretational, organizational and legislative actions.

³¹⁷ Georg Friedrich Hennig Usadel, *Zucht Und Ordnung: Grundlagen Einer Nationalsozialistischen Ethik* (Hanseatische Verlagsanstalt, 1935).

Order before freedom of speech: Steps taken before the establishment of the CAC

Xi's orders to the propaganda chiefs and the establishment in 2014 of the Leading Group for Internet Security and Informatization, which later led to the establishment of the CAC, are not the only measures the Xi administration has implemented to restrict set boundaries for citizens use of Internet and social media.

In September 2013, the legislative branch of the Chinese government, specifically the Supreme People's Court and Supreme People's Procuratorate declared that they would now interpret Article 293 of the Criminal Law, "creating a serious disturbance", as including the use of information networks "to berate or intimidate others," "to disseminate false information . . . that one has either invented or clearly knows to be fabricated," and "to organize or incite others to disseminate [such information]".³¹⁸ In 2014, the Chinese government passed a new "Counterespionage Law" that replaced some earlier national security legislation, but gave the government much wider authority to define "espionage" and "counterespionage", a strategy which according to some intelligence experts really is intended to justify closely monitoring anyone who exchanges information (of any sort) with foreign actors.³¹⁹ In 2015, a new anti-terrorism law was passed which forces telecommunications and Internet providers to "provide technical support and assistance including decryption" and hold them responsible in the mission to "prevent dissemination of information" of an extremist nature. The latter is not specifically

³¹⁸ Dui Hua Foundation, "Article 293: Deeming Free Speech Disorder in Internet Space," Dui Hua Human Rights Journal, 2015, <https://www.duihuahrjournal.org/2015/03/article-293-deeming-free-speech.html>.

³¹⁹ Didi Kirsten Tatlow, "China Approves Security Law Emphasizing Counterespionage," New York Times, 2014, <https://www.nytimes.com/2014/11/03/world/asia/china-approves-security-law-emphasizing-counterespionage.html>.

defined. It is illegal for citizens to disseminate false stories, but also to spread true information about terrorism.³²⁰ The measure also bans anyone from reporting on a terror incident, unless they belong to a pre-approved news outlet. A new online publishing law was passed in 2016, requiring anyone who operates as a publisher online to be approved and obtain a permit from a government agency. It is unclear from the law text who “publishing” is defined, whether it covers blogs or videos, but most law experts interpret it as online publication that would traditionally publish in print.³²¹

Protectionist Internet governance: People's Republic of China Network Security Law of 2017

Perhaps the biggest tightening of government control over the Internet came into effect in 2017. The deliberative and legislative work done by the CAC and Leading Group for Internet Security and Informatization since their inceptions culminated in a new Cybersecurity law and two new, more specific sets of regulations on user expression online. The “People's Republic of China Network Security Law” was promulgated in November 2016 and took effect June 1st, 2017. The law institutionalizes a protectionist strategy, where China’s government are attempting to keep out or tightly control foreign technology providers by submitting them to rigorous approval and oversight measures. As an example, article 37 states that all information collected in China, must remain on Chinese servers situated in mainland China, where they are subject to government supervision. Western companies have voiced concerns that the law, which might

³²⁰ Stephen Evans, “China Passes Controversial New Anti-Terror Laws,” BBC, 2015, <http://www.bbc.com/news/world-asia-china-35188137>.

³²¹ Dickinson Steve, “China’s New Online Publishing Rules,” China Law Blog, 2016, <https://www.chinalawblog.com/2016/03/chinas-new-online-publishing-rules-another-nail-in-the-vie-coffin.html>.

require them to let the government inspect the source code of their products.³²² This is part of a longer strategy which also coincided with Xi becoming president. In 2014, Gierow described the new, more protectionist stance toward foreign technology companies as both a cybersecurity issue and an attempt to boost the Chinese tech economy:

The Chinese government is increasingly resorting to protectionist measures to improve cybersecurity. The Chinese government perceives software by Western manufacturers as a threat to national security. Therefore, its use in China is strictly regulated.

In 2015, the U.S. and China entered into an agreement on cybercrime and cyberattacks, which also lowered the level of suspicion between the two countries, but the protectionist strategy remains, as witnessed by the cybersecurity law.³²³

The new cybersecurity law continues the strategy of using vague language, as in article 9:

Network operators carrying out business and service activities must follow the laws and administrative regulations, obey social mores and obey commercial ethics, be honest and credible, perform obligations to protect network security, accept supervision from the government and public, and bear social responsibility.

³²² Jack Wagner, “China’s Cybersecurity Law: What You Need to Know | The Diplomat,” The Diplomat, 2017, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>.

³²³ Gary Brown and Christopher D Yung, “Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace | The Diplomat,” The Diplomat, 2017, <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>.

On the user side, article 47 of the law states:

Network operators shall strengthen management of information published by users, and upon discovering information that the law or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting it, to prevent the information from spreading, save relevant records, and report it to the relevant competent departments.³²⁴

In other words, network operators are required to police user-posted information on public networks and are also to evaluate whether something is illegal or not before and take action against it before sending it to the authorities. Thus, the Chinese government is “outsourcing” the legal work to private entities, holding them responsible for the enforcement of the law. This could potentially lead to network operators and ISPs becoming overly cautious and taking action against even slightly provocative user posts which may not be in actual violation of any laws. This strict enforcement-by-proxy is exacerbated by the government’s exertion of pressure on e.g. social media companies.

Two months after the new cybersecurity law went into effect, Chinese authorities charged Tencent and Sina (providers of the three largest social media platforms, WeChat, QQ and Sina Weibo) as well as China’s largest search engine, Baidu, with being in violation of article 47. The charges were made public August 11 and by September 25, the Chinese government had found

³²⁴ Standing Committee of the National People’s Congress, “People’s Republic of China Network Security Law,” China Law Translate, 2016, <http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en>.

the companies guilty and sentenced them to pay the maximum fines possible. As part of the verdict, the government made the following statement: “The internet is not place beyond law. The regulator will scrupulously implement the Cybersecurity Law and other regulations, and increase the supervision of online contents.”³²⁵

“Managing” users and ending anonymity

To further bolster the new cybersecurity law, the State Internet Information Office (SIIO) provided two sets of provisions to be followed by those the law pertains to, i.e., among others, social media platforms and ISPs. “Provisions on the Management of Internet Forum Community Services”, promulgated on August 25, 2017 sets rules on how forums and communities should be managed, which in Chinese law would also extend to social media. It took effect October 1st, 2017. This set of provisions primarily contains common-sense language about how the providers of Internet forums and online communities must have users sign user license agreements that prohibits illegal conduct. As in some examples above, however, the language seems intentionally vague and open to ad hoc interpretation, as when a term such as “serious” is used without further explanation: “where the circumstances are serious, the service providers are to block or shut down the relevant accounts or boards”.³²⁶ Similarly, in Article 7:

³²⁵ Charlotte Gao, “China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law | The Diplomat,” The Diplomat, 2017, <https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/>.

³²⁶ State Internet Information Office, “Provisions on the Management of Internet Forum Community Services,” China Law Translate, 2017, <https://www.chinalawtranslate.com/互联网论坛社区服务管理规定/?lang=en>.

Internet forum community service providers shall strengthen management of their users' publication of information, and where they discover that information prohibited by laws, regulations or relevant national provisions is contained therein, they shall immediately stop the transmission of that information and employ measure as deletion to handle it, storing relevant records and promptly reporting it to the State or local Internet information offices.³²⁷

This passage is merely a reiteration of the ISP/network operator obligations in the overall cybersecurity law, with one subtle difference. The line "relevant national provisions is contained therein" is once again sufficiently vague to be open for interpretation. What is deemed "relevant" is up to the ISPs, network operators and social media supervisors to evaluate, under the risk of letting user content slip through that the government deems as "relevant". The major change brought about by this set of provisions can be found in article 8, however, in which the government now require all the pertinent platforms to verify and register users' identities before letting them onto the platforms, even if they wish to be anonymous when posting:

Internet forum community service providers shall follow the principle of "real names behind the scenes, but using whatever name you please up front", requiring users to go through identity information verification before registering accounts, and carry out identity information recording and periodic verification for the originators and administrators of

³²⁷ State Internet Information Office.

boards. Where users do not provide truthful identification information, internet forum community service providers must not provide them with information publication services. Internet forum community service providers shall strengthen review and management of the registration of fake user identity information, board names, and summaries; and must not allow the appearance of content prohibited by laws, regulations, or relevant State provisions.

Internet forum community service providers shall protect users' identification information, and must not disclose, alter, or destroy it, and must not unlawfully sell it or unlawfully provide it to others.

What constitutes providing the identities “unlawfully to others” is not defined in the provisions. In article 9, the provisions also make it possible for the government to sanction the providers and operators if they can be seen to have benefited from any illegal activity. This may seem inconspicuous, but it could be interpreted as making it punishable to offer advertising space on a forum where someone posts something that crosses the already vague government boundaries:

Internet forum community service providers and their employees may not seek improper benefits through the publication, reprinting or deleting information, or interfering with search results, interfering with presentation sequences on dissemination platforms and other such methods.

Again, the vague language is problematic. Does “benefit” simply mean in an economic sense? Or would obtaining more followers/users be seen as a benefit? How should the term “improper” be

construed? This article is another example of regulatory language that could force e.g. social media platforms to be overly cautious and restrictive to ensure compliance.

“Managing” public opinion

Another set of provisions issued as guidance with regard to the new cybersecurity law is “Provisions on the Management of Internet Post Comments Services”, also promulgated on August 25, 2017 and put into effect on October 1, 2017. From the title, these provisions appear to set rules for commenting, e.g. in comments sections on news websites, but actually apply to any form of expression online, in which a user can make a comment:

Post comment services as referred to in these Provisions, refers to Internet websites, applications, interactive broadcast platforms, and other broadcast platforms of a news and public opinion nature with capacity to mobilize the public, that provide services for users to express text, code, emojis, pictures, audio, video, or other information through methods such as posting messages, responding, leaving messages, live-stream commentary, and so forth,³²⁸

The provisions are very clear about how public comments will be monitored and handled under the new cybersecurity law. The decentralized system of information offices will enforce “daily supervision and inspection” of all venues of public expression online:

The State Internet Information Office is responsible for supervision, management and law enforcement efforts on post comment services nationwide. Local internet information

³²⁸ State Internet Information Office, “Provisions on the Management of Internet Post Comments Services,” China Law Translate, 2017, <https://www.chinalawtranslate.com/互联网跟帖评论服务管理规定/?lang=en>.

offices are responsible for supervision, management and law enforcement efforts for post comment services within that administrative region and on the basis of their duties. All levels' Internet information offices shall establish and complete supervision and management systems that integrate daily supervision and inspection and regular inspections, and lawfully regulate post comment activity on all kinds of broadcast platforms.

The provisions include the same rules regarding liabilities in user terms and conditions agreements and the same requirements regarding registration and verification of the users' identities. The provisions prohibit

...Post comment service providers and their staffs" from interfering "with public opinion by employing methods such as selective deletion or recommendation of post comments so as to obtain improper benefit or on the basis of mistaken value orientations. Post comment service providers and users must not use software, employment agencies, personnel, or other methods to disseminate information, disrupting the normal order of post comments, and misguiding public opinion.

In other words, the "post comment service providers" cannot set their own rules of conduct but are forced to follow those set by the government. These policies seem to have had the desired effect already. In April 2018, Tencent and Weibo announced that they would commence "clean-

up campaigns to sanitise content despite not being singled out by regulators”.³²⁹ Weibo announced the company would “clean up lowbrow content on its live-streaming platforms to “ensure they do not disrupt China’s socialist core values” in a campaign that will last three months”. Note that there is no distinction between user-generated content and commercial/professional content in this regard, and that Tencent and Weibo have not just decided to voluntarily remove any content that might disrupt the public order, harm national security, is criminal in nature or critical of the government. It is also volunteering to remove any content that might be considered “vulgar” by the government, i.e. a decision based on social norms defined by the government.³³⁰ One aspect of the decision by Tencent and Weibo to proactively comply was immediately met with protests and user mobilization, however. This is an example of why Roberts’ does not fully support Kou’s supposition that there is broad tolerance, or even acceptance of censorship in China:

It is not true that censorship in China is merely accepted. Some people may say “Well, they’re just removing pornography and false rumors”, but among other parts of the population, there is a huge backlash against the censorship measures online, often involving mobilization of users. Weibo recently tried to remove all content related to

³²⁹ Celia Chen and Iris Deng, “Weibo, Tencent Volunteer to Clean up Content as China Intensifies Crackdown,” South China Morning Post, 2018, <http://www.scmp.com/tech/china-tech/article/2141375/chinese-social-media-platforms-volunteer-clean-content-crackdown>.

³³⁰ Chen and Deng.

homosexuality as part of a proactive attempt to comply with government regulation, and they had to backtrack and reverse their decision.³³¹

Hence, there appears to be some selectivity in terms of what the Chinese people will stand for in terms of censorship. Weibo's decision to remove anything resembling pornography and references to violent video games (or violent game apps on the Weibo platform) was not met with the same anti-censorship fervor as the banning of content referring to homosexuality. A Weibo hashtag, #IAmGayNotAPervert was seen more than 1.35 million times, and millions of users posted messages reacting against the decision.³³²

There have been other cases where a controversial topic or decision has been, with Roberts' words, "trolled off the Internet", but "...the problem is getting people to care. It's a general problem all over the world when it comes to political participation. People have other stuff to do."³³³

Ensuring trustworthiness through a Social Credit Score

Finally, these provisions order the "post comments service providers" to implement an internal rating system of users that can have far-reaching consequences:

³³¹ Roberts, "Interview 4/18/2018."

³³² Javier C. Hernández and Zoe Mou, "Chinese Social Media Site Reverses Gay Content Ban After Uproar," The New York Times, 2018, <https://www.nytimes.com/2018/04/16/world/asia/china-weibo-gay.html>; Javier C. Hernández and Zoe Mou, "I Am Gay, Not a Pervert': Furor in China as Sina Weibo Bans Gay Content," The New York Times, 2018, <https://www.nytimes.com/2018/04/15/world/asia/china-gay-ban-sina-weibo-.html>.

³³³ Roberts, "Interview 4/18/2018."

Post comment service providers shall establish stratified user management systems, carrying out credit assessments of users' conduct in commenting on posts, and designate the scope of services and functionality on the basis of credit levels; entering the seriously untrustworthy onto a black list, stopping provision of services to those entered onto the black list, and prohibiting them from using methods such as new registration to use post comment services. The State and provincial, autonomous region or directly governed municipality Internet information offices shall establish credit files and a trust-breaking blacklist management system for post comment services, and regularly conduct credit assessments of post comment service providers.³³⁴

This means that users who are somehow seen as violating the government's rules of online conduct may be given a bad "credit score" with regards to trustworthiness, which will also be accessible for government entities. Both online and offline behavior can impact your score: "Actions that can now harm one's personal credit record include not showing up to a restaurant without having cancelled the reservation, cheating in online games, leaving false product reviews, and jaywalking".³³⁵ If you are blacklisted, you will no longer be allowed to use certain services, but some sub-services can also be made inaccessible to those who simply have a bad "credit score" for trustworthiness. These do not just include online services. Many public

³³⁴ State Internet Information Office, "Provisions on the Management of Internet Post Comments Services."

³³⁵ Meg Jing Zeng, "China's Social Credit System Puts Its People under Pressure to Be Model Citizens," The Conversation, 2018, <https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963>.

services, such as public transportation or financial support from the government will be dependent on this “social credit score”:

Being a “good citizen” is well rewarded. In some regions, citizens with high social credit scores can enjoy free gym facilities, cheaper public transport, and shorter wait times in hospitals. Those with low scores, on the other hand, may face restrictions to their travel and public service access.³³⁶

According to Susanne Chan, “These measures effectively kill spontaneity online and further exhibit the Party’s will to monitor the expression of online public opinion.”³³⁷

For Rebecca Slayton, the Chinese government’s trade-off between security and restriction of liberty is tipping in the wrong direction. She is associate professor of Science and Technology Studies at Cornell University, a highly-regarded scholar of international security and cybersecurity and an award-winning author of several books on technology policy. In an interview conducted for this dissertation, she told me that she also believes there is a limit to how far the Chinese government can go with regard to oppressive measures:

...intrusive surveillance could lead to somebody being apprehended. The question is, when you do that systematically or when you single out groups systematically, whether you actually, ultimately erode security? And whether you actually erode the very thing the country exists for? Security is not an end in itself. What are you securing? You are

³³⁶ Zeng.

³³⁷ Chan, “Cybersecurity under Xi Jinping: A New Model for Broad Control in China.”

supposed to be securing a particular kind of society, and when security starts to undermine that, it no longer seems very valid.³³⁸

Dr. Yobu Kou is a Chinese computer scientist at Purdue University who studies the social aspects of Internet and information technology policy in mainland China. In an interview conducted for this study, he expressed his belief that the government uses social media monitoring and data collection to gauge the sentiment of the people, in a way performing the “consultation” that Xi has emphasized (see above), and thus bypassing traditional media as a venue of consultation:

I think there are government projects using big data and social media to do that. I think in the past, when China was purely an agricultural society and taxes got too heavy, people started to starve. Then they naturally know that if they don't rise up, they'll die. In current society, I don't see that possibility, because there is still this thing called the Internet, and people are connected, and I don't think the government would do way too much to suppress people to the point where people are just dying.³³⁹

Margaret E. Roberts agrees that “the Chinese government has to be careful” not to go too far in their oppression. She does not share Kou's view that the Internet provides sufficient mechanisms for proliferating information about mobilization in China:

³³⁸ Slayton, “Interview, August 24.”

³³⁹ Kou, “Interview, February 16,” 2018.

There have definitely been studies showing uncertainty about how long protests organized online last, if it's real collective action or if people just meet up once. There is *some* mobilization over the Internet generally, though, and that's certainly true in China. However, we've seen that there is consistent censorship of information online about protests. There are lots and lots, tens of thousands, if not hundreds of thousands of physical protests every year. The Chinese government stopped releasing the official numbers and information about these protests, but we think they are between tens of thousands to hundreds of thousands. Some of them are organized offline, for example some might be villagers getting together after government grabbed their land some of them are labor protests. But they increasingly being organized online, which has particularly been happening since the first decade of the 2000s. Protests are pretty commonplace, but the danger to the Chinese government is that they spread from one locality to another or become much larger and cannot be contained.

Enforcing propriety: Media oppression under Xi

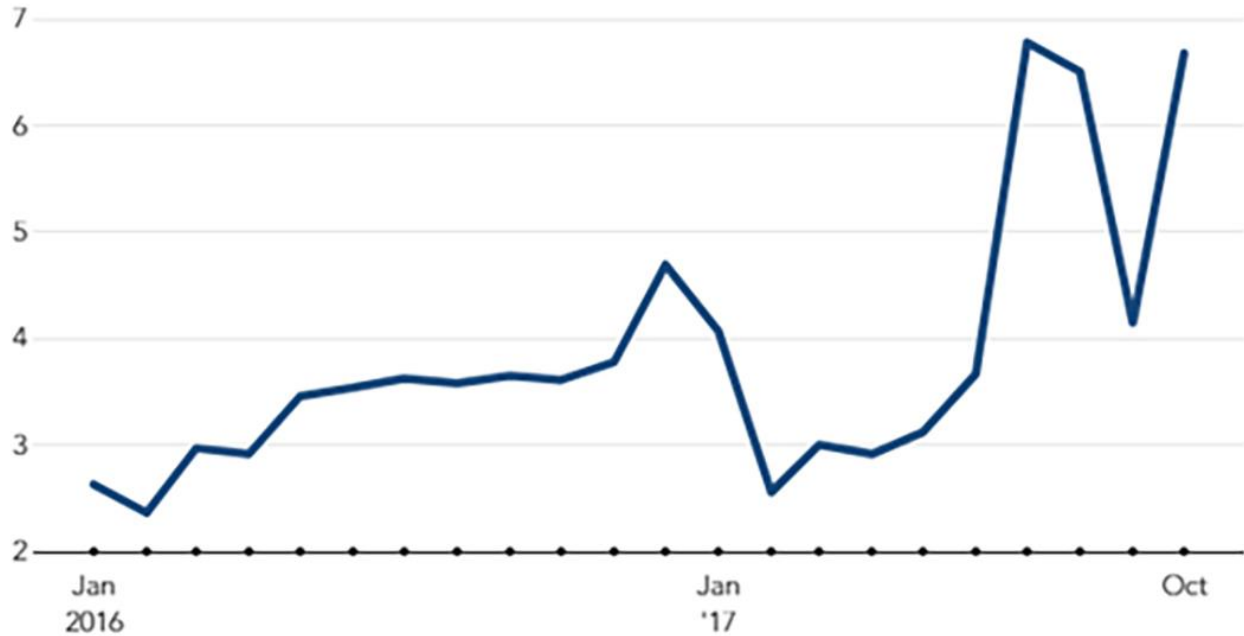
In June 2017, the Xi administration's new cybersecurity legislation became effective. The Beijing Cyber Administration, a local agency under the CAC, did not waste any time enforcing the law, and on June 7, the government met with WeChat officials, resulting in the shutdown of 25 public WeChat accounts mostly belonging to entertainment and fashion magazines and websites, including the U.S.-owned *Harper's Bazaar*. The BCA did not try to hide the fact that the shutdown request was ideological, stating on Weibo that the accounts would not be reopened,

unless the owners “take effective measures to contain the glorification of scandals and the private lives of celebrities, the sensationalization of their conspicuous consumption and low taste.”³⁴⁰

By July, the BCA had shut down more than 60 celebrity-focused accounts on those grounds.³⁴¹

Reports of illegal/inappropriate online information

(Monthly figures, in millions)



Source: China Internet Illegal Information Reporting Center

Figure 4. Registered number of illegal or inappropriate behavior to the CAC (Source: China Internet Illegal Information Reporting Center / Illustration: Nikkei)

³⁴⁰ Yiling Pan, “China Shuts Down Harper’s Bazaar and 24 Others on WeChat,” Jing Daily, 2017, <https://jingdaily.com/china-shut-down-accounts-on-wechat/>.

³⁴¹ Saibal Dasgupta, “China Reducing Massive Influence of Social Media Celebrities,” VOAnews.com, 2017, <https://www.voanews.com/a/china-social-media-celebrities/3942435.html>.

The Japanese news agency *Nikkei* reported in December of 2017 that the China Internet Illegal Information Reporting Center (an agency under the CAC) had given a report on the impact of the new cybersecurity law to the Standing Committee of the National People's Congress.³⁴² The agency's own numbers confirmed a drastic rise in actions taken as part of the crackdown on "illegal information" after the law became effective in June 2017 (See Fig. 4 above)

All in all, in the period between 2015 and late 2017, more than 10 million personal accounts on social platforms of varying sorts were shut down and 13,000 corporate websites had been closed. These shutdowns were not carried out by the authorities directly, but instead through more than 2,200 companies in China who were self-regulating in compliance with the law. According to *Nikkei*, the number of instances in which content had been flagged as inappropriate doubled from 3 million to 6 million after the law took effect. Furthermore, "Officially, these sites and accounts were shuttered for posting pornography, information on terrorism and other inappropriate content. But social and political commentary is believed to have been censored as well out of concern that it might pose a threat to national security."³⁴³

National security was also Xi's official motivation for the new, more authoritative strategy and law, as discussed in the section outlining the Rhetorical Frame. It is difficult to determine the prioritization between national security and moralistic ideology in these actions, however.

³⁴² Shunsuke Tabeta, "Xi's Iron Grip on China's Internet Extends to Social Media- *Nikkei Asian Review*," *Nikkei*, 2017, <https://asia.nikkei.com/Politics-Economy/Policy-Politics/Xi-s-iron-grip-on-China-s-internet-extends-to-social-media>.

³⁴³ Tabeta.

Silencing dissent or expressions of behavior or attitudes deemed inappropriate by the Chinese state is not just contained to account shutdowns. In some cases, criminal charges are brought against users who have voiced dissent on social media.

One example is Zhang Guanghong, who was arrested in October 2017 for posting what was considered disparaging comments about Xi Jinping on WeChat, where Zhang was a moderator for several chat groups. He was held for 24 hours and had four cell phones and a server confiscated by the authorities. Zhang's lawyer stated to Radio Free Asia – a news outlet serving U.S. interests – that he believed Zhang's arrest was linked to the Communist party's 19th Congress and the attempt to keep all dissent far away from this event.³⁴⁴ A month earlier, Beijing police arrested Liu Pengfei, the creator of a WeChat group that had discussed political and social issues.³⁴⁵ Weichu Zhang, unrelated to Guanghong Zhang is a civil rights activist who was also arrested by the authorities with legal basis in the 2017 cybersecurity law. In her case, the charge was the purchase of a router that could act as a VPN, which is illegal (see below). Even so, the router was sold online with the sales pitch: "KFRouter allows to use Google, Facebook, YouTube, Twitter, INS and so on as old days in your country"³⁴⁶. In March of 2017 Deng Jiewei was sentenced to nine months in jail for selling VPNs.³⁴⁷

³⁴⁴ Yang Fan and Qiao Long, "Guangdong Police Swoop on Chat Group Moderator, Activist Who Scaled 'Great Firewall,'" Radio Free Asia, 2017, <https://www.rfa.org/english/news/china/guangdong-police-swoop-on-chat-group-moderator-activist-who-scaled-great-firewall-10052017113158.html>.

³⁴⁵ Human Rights Watch, "World Report 2018: China | Human Rights Watch," World Report 2018, 2018, <https://www.hrw.org/world-report/2018/country-chapters/china-and-tibet>.

³⁴⁶ Fan and Long, "Guangdong Police Swoop on Chat Group Moderator, Activist Who Scaled 'Great Firewall.'"

³⁴⁷ Human Rights Watch, "World Report 2018: China | Human Rights Watch."

Arrests of dissenters and popular Internet figures in China is of course nothing new, but China observers have noted that arrests based on pure ideology appear to be more frequent after Xi Jinping took office. In 2014, the day after Xi gave his above-mentioned speech to the propaganda chiefs in which he encouraged them to build a “strong army”, police arrested people involved with the interactive agency Beijing Erma Interactive Marketing and Planning, including the popular Internet celebrity Qin Huohuo. The charge was rumor-mongering, which exactly what Xi had railed against while talking to the propaganda chiefs. . Three days later, the Sina Weibo star Xue Manzi, who had 12 million followers, was arrested. Behind this pseudonym is Chinese-American businessman Charles Xue Biquan who was charged with soliciting prostitutes.³⁴⁸ In 2015, on July 9, 321 Chinese human rights activists and lawyers were arrested, many of them charged with inciting subversion of state power.³⁴⁹ And in 2016, four Chinese citizens were arrested for spreading “fake information” when bystanders posted pictures and information on Weibo from a violent police crackdown on a demonstration in the fishing village of Wukan.³⁵⁰

³⁴⁸ Cary Huang and Keith Zhai, “Xi Jinping Rallies Party for Propaganda War on Internet,” South China Morning Post, 2013, <http://www.scmp.com/news/china/article/1302857/president-xi-jinping-rallies-party-propaganda-war-internet>.

³⁴⁹ Huang Zheping, “Human Rights Lawyer Wang Yu on Year of Secret Detention in China,” Quartz, 2017, <https://qz.com/1129837/human-rights-lawyer-wang-yu-on-year-of-secret-detention-in-china/>.

³⁵⁰ Zheping Huang, “China Censorship: Chinese Citizens Are Being Arrested for Sharing News about the Wukan Village Rebellion Online,” Quartz, 2016, <https://qz.com/783026/china-censorship-chinese-citizens-are-being-arrested-for-sharing-news-about-the-wukan-village-rebellion-online/>.

Further human rights abuses under Xi

Of the 321 aforementioned human rights activists and lawyers that were arrested in 2015, Human Rights Watch point to 16 whose treatment was particularly harsh:

Over 16 human rights lawyers and activists—detained after a nationwide sweep of rights advocates in July 2015—were the clearest victims of the authorities’ hostility towards independent civil society. Most were held in secret and not allowed to communicate with their families or lawyers of their choosing. Families, lawyers, and supporters who inquired about the cases or sought the detainees’ release also became targets of the authorities’ wrath. The secrecy surrounding these detentions stood in stark contrast to the aggressive state media campaign to smear the detainees, many of them well-known for their years of activism. The publicity, which departed from the quieter treatments of past political trials such as that of Liu Xiaobo’s in 2009, appears designed to punish the activists and advance President Xi’s campaign to depict independent civil society as a national security threat. Chinese authorities’ enforced disappearance of critics from Hong Kong and other countries in 2016 garnered headlines globally. Beijing’s decision to interfere in a politically charged court case in Hong Kong in November undermined judicial independence and the territory’s autonomy. In the ethnic minority regions of Xinjiang and Tibet, Beijing continued its highly repressive rule, curtailing political activity and many peaceful expressions of ethnic and religious identity.³⁵¹

³⁵¹ Human Rights Watch, “World Report 2017: China | Human Rights Watch,” World Report 2017, 2017, <https://www.hrw.org/world-report/2017/country-chapters/china-and-tibet>.

These human rights violations, pertaining to the United Nations Declaration of Human Rights article 19 (on freedom of opinion and expression), article 20 (on freedom of assembly) and several articles on the rights to fair treatment under the law, were from 2016. In 2017, after the new cybersecurity law came into effect, Human Rights Watch reported:

The broad and sustained offensive on human rights that started after President Xi Jinping took power five years ago showed no sign of abating in 2017...The near future for human rights appears grim, especially as Xi is expected to remain in power at least until 2022. Foreign governments did little in 2017 to push back against China's worsening rights record at home and abroad. The Chinese government, which already oversees one of the strictest online censorship regimes in the world, limited the provision of censorship circumvention tools and strengthened ideological control over education and mass media in 2017. Schools and state media incessantly tout the supremacy of the Chinese Communist Party, and, increasingly, of President Xi Jinping as "core" leader. Authorities subjected more human rights defenders—including foreigners—to show trials in 2017, airing excerpted forced confessions and court trials on state television and social media.

Though not specified as a human right in the original declaration, Special Rapporteur to the U.N. on Freedom of Expression, David Kaye, stressed in a 2015 report, that anonymity was essential to the preservation of privacy and information access rights as human rights – as laid out in the declaration's articles 12 and 19. Human Rights Watch believes China violates these rights in their current social media policies: "In September Weibo barred users who had not registered

with their real names from posting messages on their own microblogs or comment on others.”³⁵²

Weibo’s actions were in compliance with new regulations enacted by the CAC that practically made anonymity illegal on social media and put pressure on the social media platforms to enforce the rules.³⁵³ Furthermore, the CAC also put rules in place that would imply guilt by association and establish an internal rating system for users based on their compliance: “In September, the CAC promulgated measures to make creators of online chat groups such as those on QQ and WeChat liable for information other users shared in the groups.”³⁵⁴

These rights violations will have an important role to play later in this chapter, as I begin to discuss China’s social media policies in a Rawlsian sense.

Monitoring and influencing the population via social media

As mentioned above, King et al. found that government officials also use surveillance and monitoring on social media to gauge the sentiment of the people in general. The purpose of this is both a practical and a political one. On the one hand, authorities use the conclusions from the analyses of collected data to know where to apply pressure on individuals or take legislative action to silence dissent or stop mobilization. On the other hand, as Kou stated above, they also use this to ensure that no policies are so unacceptable to the people that it may cause an uprising.

³⁵² Human Rights Watch, “World Report 2018: China | Human Rights Watch.”

³⁵³ Catherine Shu, “China Doubles down on Real-Name Registration Laws, Forbidding Anonymous Online Posts,” TechCrunch, 2017, <https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/>.

³⁵⁴ Human Rights Watch, “World Report 2018: China | Human Rights Watch.”

But King, Pan and Roberts have also found that the Chinese government does not just monitor social media for what they consider subversive posts. There is also a large-scale influence campaign in place that shares a substantial similarity with the one described in the chapter on Russia. The main difference is the target. Whereas Russia uses influence campaigns as an offensive capability as part of a larger, geopolitical strategy, China's influence campaign is only domestic, with the goal of ensuring stability and diminishing unrest among the Chinese people. Journalists and scholars have long suspected the Chinese authorities of hiring the equivalent of the "Russian trolls" described in the Russia chapter, i.e. influence agents whose work merely consists of defending and promoting government positions in online discussions and posting content on social media that describes the government's actions or messages in positive terms. As in the Russian example, this content is posted by the influence agents appearing as ordinary users of the respective platforms. Adopting a term from the popular discourse about these influence agents, King et al. call them "50c party members":

...the Chinese regime also conducts "astroturfing," or what we might call *reverse censorship*, surreptitiously posting large numbers of fabricated social media comments as if they were the genuine opinions of ordinary Chinese people. The people hired for this purpose are known formally as Internet commentators... although more widely as 50c party members... so called because they are rumored to be paid 50 cents (5 Jiao... or about \$0,08) to write and post each comment³⁵⁵ King, Pan and Roberts actually find the payment rumors to be untrue, but they do show evidence of a massive influence campaign is being run in the manner described above,

³⁵⁵ King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," 484.

mostly conducted by government employees working on the campaign part-time. Their analysis is based on a December 2014 leak of an archive containing 2013/2014 e-mail correspondences from the Internet Propaganda Office in Zhanggong District.³⁵⁶ These e-mails included reports on the activities of 50c party members/Internet commentators with claims of completion of influence assignments. From the e-mails, King et al. were able to harvest 43,757 known 50c posts that they then converted to training set for further analysis and to identify other 50c posts. The authors also managed to conduct surveys among 50c party members through an intricate (and IRB-approved) process of anonymization on both sides. The results of the analyses showed that 50c party members engage less in discussions as defenders of the regime, but act more like “cheerleaders”:

More specifically, most journalists, activists, participants in social media, and some scholars have, until now, argued that the massive 50c party is devoted to engaging in argument that defends the regime, its leaders, and their policies. Our evidence indicates the opposite—that the 50c party engages in almost no argument of any kind and is instead devoted primarily to cheerleading for the state, symbols of the regime, or the revolutionary history of the Communist Party. We interpret these activities as the

³⁵⁶ Zhanggong District is a country-level administrative unit in Ganzhou City, located in Jiangxi Province. Its population in 2013 was 468,461.

regime's effort at strategic distraction from collective action, grievances, or general negativity, and so forth.³⁵⁷

The size of the influence campaign, however, is staggering, particularly compared to the Russian influence campaign described in chapter 3. The authors conclude that 50c party members may produce up to 448 million posts on social media per year that can be seen by multitudes of users and therefore have an enormous reach. The posts are further proliferated and their messages (often containing links to government websites) amplified by through strategic timing and placement:

It also appears that the 50c party is mostly composed of government employees contributing part time outside their regular jobs, not, as has been claimed, ordinary citizens paid piecemeal for their work. This, nevertheless, is still an enormous workforce that, we estimate, produces 448 million 50c posts per year. Their effectiveness appears maximized by the effort we found of them concentrating the posts into spikes at appropriate times and by directing about half of the posts to comments on government websites.³⁵⁸

³⁵⁷ King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," 497.

³⁵⁸ King, Pan, and Roberts, 497.

The aforementioned Margaret E. Roberts is one of the authors of the studies above. She told me that this social media influence campaign is one of three censorship methods used by the Chinese government:

In my book I talk about three mechanisms of censorship. The first is Fear, which is the threat of punishment for what you say. Then there's Friction, which is more like actual censorship, that is, removal of what you have said or written. Finally, there's Flooding, where the government distributes information on the Internet and crowds out unwanted content or information. The 50-cent party is an example of the latter.³⁵⁹

To Western minds, it may appear as a mystery why the Xi administration is not overthrown when there are “tens of thousands to hundreds of thousands” of protests every year, according to Roberts. As she and Kou point out, the instruments of mobilization are available, and methods of circumvention can easily be distributed in China. With more than 700 million Internet users, the Chinese population should in theory be able to spread dissenting information and firewall-jumping software to each other at such a rate that it would render the government's propaganda and suppression efforts useless and obsolete. And yet, the many attempts at mobilization never seem to have more than a slightly moderating effect on the government's policies. Could it be that there is something inherent in Chinese culture that prohibits this kind of online mobilization? According to some scholars, as I will show in the next section, this might actually very well be the case. Some argue that the grip that Confucianism has on the Chinese population is strong,

³⁵⁹ Roberts, “Interview 4/18/2018.”

and Confucianism does not allow for the kind of social media behavior that would support an uprising through online mobilization.

Cultural background

The Chinese population is not kept in the dark. Internet users in the country are savvy and well-informed, and, as will be revealed in the following, well-aware of the censorship mechanism and how it works. From a Western standpoint rooted in pluralist, democratic thought, it may seem odd that the Chinese population is so willing to accept this kind of information access suppression, media control and government oppression. As in the case of the Russian tradition of deception as virtue mentioned in the Russia chapter, a possible, unexhaustive explanation might be found in the long cultural history of China, and particularly in Confucianism.

A brief history of Confucianism in China

According to Tu, there is actually no such concept as Confucianism in China. Rather, “Confucianism” is a Western term, coined as recently as the 18th century, describing a way of life and thought deeply ingrained in Chinese culture.

Confucius’ writings are a formulation and crystallization of traditions that go back thousands of years before his own birth in 551 B.C.³⁶⁰ His Chinese name was K’ung Ch’iu but was often referred to as “Master K’ung”, i.e., K’ung-Tzu or K’ung Fu-tzu, which led to the Latinization “Confucius”. He is known in China as being the first private teacher and

³⁶⁰ Wei-Ming Tu, “Confucius and Confucianism,” in *Confucianism and the Family* (New York: SUNY Press, 1998), 3–22.

establishing teaching as an actual vocation. Thus, the idea of “self-cultivation” is central to Confucius’ teachings, which are primarily documented in the *Analects (Lun-yu)*, most likely by the second generation of Confucius’ students and disciples. As he developed these, he rose in the social and official ranks in his home state of Lu, where he obtained the position of minister of justice in his early fifties. At age fifty-six, he realized that his advice and teachings had little impact on the decisions made by the Lu magistrates and leaders, and he decided to resign and leave the state, taking a number of disciples with him.³⁶¹ According to the *Shiji*, the Records of the Grand Historian of China, Confucius was also discouraged by the behavior of the Duke of Lu, who had been easily distracted from his official reform duties in a conflict with the neighboring state Qi. The officials in Qi had sent the Duke 100 good horses and 80 beautiful dancing girls, which kept him from his duty for three days. Together with another collection of historical records, the *Zuo Zhuan*, the *Shiji* chronicles how Confucius traveled to a number of Chinese states between 497 B.C. and 484 B.C., spending more than 12 years spreading his teachings with his disciples.³⁶² He returned to Lu at age 68 upon the request of the chief minister of the state and spent the last five years of his life teaching more than 70 disciples, primarily through what is now known as the *Five Classics*. These are not works of Confucius himself, but rather classic Chinese works of art, tradition and thought. The five classics are the aforementioned *Zuo Zhuan*, the *I Ching*, the *Lijing* (a book of rites describing administration and

³⁶¹ Tu.

³⁶² Qian Sima and Burton Watson, *Records of the Grand Historian of China* (New York: Columbia University Press., 1961); Watson, *The Tso Chuan: Selections from China’s Oldest Narrative History* (New York: Columbia University Press, 1989).

social rites in the Zhou dynasty) and two collections, one of poetry and one of documents, that may have been assembled by Confucius himself.³⁶³

Confucius died in 479 B.C. His disciples created 8 different schools, each based on a particular disciple's interpretation of the master's teachings, at least according another philosopher of the era, Mo Tzu. He advocated a form of collectivist thought now known as Mohism, which was seen as a rival to the self-cultivational aspects of Confucianism, and both of these were contrasted by an extremely individualist philosophy proposed by a third philosopher, Yang Chu.³⁶⁴ A second-generation Confucian disciple, Mencius (371-289 B.C.), would become the most important advocate of the fledgling movement later known as Confucianism. Mencius presented a "third way" between Mohist collectivism and the individualism of Chu by appealing to the virtuous/moral and administrative/pragmatic aspects of Confucius' teachings:

Mencius's strategy for social reform was to change the language of profit, self-interest, wealth and power into a moral discourse with emphasis on rightness, public-spiritedness, welfare and exemplary authority. However, Mencius was not arguing against profit. Rather, he instructed the feudal lords to opt the great benefit that would sustain their own profit, self-interest, wealth and power in a long-term perspective. He urged them to look beyond the horizon of their palaces and to cultivate a common bond with their ministers, officers, clerks and the seemingly undifferentiated masses. Only then, he contended,

³⁶³ Michael Nylan, *The Five "Confucian" Classics* (Yale University Press, 2008).

³⁶⁴ Tu, "Confucius and Confucianism."

would they be able to maintain their own livelihood. He encouraged them to extend their benevolence and warned them that this was crucial for the protection of their own families. Mencius's appeal to that which is common to all people as a mechanism of government was predicated on his strong "populist" sense that the people are more important than the state and the state is more important than the king, and that the ruler who does not act in accordance with the kingly way is unfit.³⁶⁵

After a period of being guided by shifting schools of thought during the first imperial dynasty in China, the Qin dynasty (221-206 B.C.), Confucianism takes hold with the emergence of the Han dynasty in 206 B.C., which is considered a golden age in Chinese history.³⁶⁶ This is witnessed by the fact that China's majority ethnic group refers to itself as "Han people" and that the Chinese script language is known as Han characters.³⁶⁷ The Han dynasty lasted for almost four centuries until 220 A.D, and though it was replaced by several dynasties over almost two millennia, Confucianism was a common thread throughout in terms of governmental thought, administration, ethics and virtue. As Tu writes:

Both in theory and practice, Confucianism has made an indelible mark on the government, society, education and family of East Asia. It is an exaggeration to characterize traditional Chinese life and culture as "Confucian", but Confucian ethical

³⁶⁵ Tu, 15.

³⁶⁶ Jinghao Zhou, *Remaking China's Public Philosophy for the Twenty-First Century* (ABC-CLIO, 2003).

³⁶⁷ Richard T Schaefer, *Encyclopedia of Race, Ethnicity, and Society*, vol. 1 (Sage, 2008).

values have, for well over 2,000 years, served as the source of inspiration as well as the court of appeal for human interaction at all levels – between individuals, communities and nations in the Sinic world.³⁶⁸

This sentiment is echoed by Yubo Kou, who argues that censorship is tolerated in China because of the Confucianist tradition. After the Chinese revolution that brought down imperial rule in China in 1911 and the civil war in 1949 that institutionalized the CPC as China's sole ruling party, it was assumed that Confucianism was a thing of the past. Mao was vehemently opposed to Confucianism. His entire revolutionary mission was to move China away from this school of thought, which, in his view, had led to China to accept submission on several levels, both as an actor on the international scene being taken advantage of by Western powers, and within the power structures of the domestic, feudal system advocated by Confucius. Quoted in Boer, Mao wrote in 1956:

There is no end to learning from experience ... People make mistakes when they are young, but is it true that older people can avoid making mistakes? Confucius said everything he did conformed to objective laws when he was seventy. I just don't believe it, that's bullshit.³⁶⁹

³⁶⁸ Tu, "Confucius and Confucianism," 3.

³⁶⁹ Roland Boer, "Confucius and Chairman Mao: Towards a Study of Religion and Chinese Marxism," 38, accessed February 24, 2018, <http://crisiscritique.org/uploads-new/BOER.pdf>.

Yet, even as China went through Mao’s Great Leap Forward and later, his Cultural Revolution, Confucianism survived. As Kou stated my interview with him: “It has a very long history...Confucianism has been the mainstream idea for thousands of years. Before the 20th century the idea of Confucianism had been so deep in Chinese culture, lives and mentality, so the influence is very big. It’s not something a small, cultural revolution can change”³⁷⁰

How Confucianism impacts online user behavior

In a mixed-methods study, Kou et al. show that Confucian virtues are still very present and can be identified in the usage patterns and attitudes among social media users in China. The authors conclude that “Confucianism continues to have a significant impact over Chinese citizens’ thoughts and actions”³⁷¹, and show how the “Five Constants” set of virtues in Confucianism guide contemporary Internet use in China. Confucius’ “Five Constants” are Benevolence, Righteousness, Propriety, Wisdom and Integrity. As I will show further along in the chapter, the meaning of “Wisdom” is debated, but in the present case it is understood as closer to the Western conception of the word “knowledge”. Kou et al. describe each of the five virtues in terms of Internet use: “The first virtue, Benevolence (仁), describes how people should manifest love and compassion for others. For example, a person might exhibit benevolence by helping disadvantaged individuals or groups.”³⁷² In the interview for this study, Yubo Kou elaborates:

³⁷⁰ Kou, “Interview, February 16.”

³⁷¹ Yubo Kou, Bryan Semaan, and Bonnie Nardi, “Human-Computer Interaction – INTERACT 2017” 10516, no. May (2017): 2, <https://doi.org/10.1007/978-3-319-68059-0>.

³⁷² Kou, Semaan, and Nardi, 2.

It's about how people take care of each other and are nice to each other. This can generally be mapped to the value of harmony in today's context. So, people want to help each other and want to be nice to each other. For example, on social media, when a stranger asks you about some kind of sensitive information, it can be relatively hard to say no, because people want to be nice to each other. There doesn't seem to be any major reason to reject their request, and this is the benevolent part.³⁷³

The second virtue, Righteousness (义), according to Kou, et al.:

...emphasizes how a person's thoughts and actions should conform to his or her own beliefs, and the person should resist temptation. For instance, as our study participants told us, on social media a person should speak about public events through reasoned and factual discourse as opposed to relying solely on personal opinions.³⁷⁴

Kou does qualify this by stating that values of righteousness are not given and may vary: "It operates at a more abstract and normative level in terms of what you think is right or wrong"³⁷⁵

Kou et al. write about the third virtue, Propriety (礼), that it

...refers to how a person should respect behavioral norms that maintain social structures, such as hierarchy. In other words, people should value stability and harmony over radicalism in resolving issues. Confucian teachings encourage people to cope with

³⁷³ Kou, "Interview, February 16."

³⁷⁴ Kou, Semaan, and Nardi, "Human-Computer Interaction – INTERACT 2017," 2.

³⁷⁵ Kou, "Interview, February 16."

problems in a harmonious way consistent with both propriety and benevolence. People should avoid confrontation and seek peaceful alternatives.

Yubo Kou explains how this virtue is not just the one that sets Chinese Internet culture apart from its Western counterpart, but also the one that says the most about why Chinese social media users accept surveillance and censorship:

The next, propriety, I think this is the most important one in current, Chinese society. I think it basically means hierarchical. People know there is a hierarchy in terms of how they are being managed by the government, and there's a hierarchy in terms of social relationships. And people think that this is not just acceptable, but also the common-sense way to behave. So, this is an important part way of why they accept the censorship. In the paper, we also talk about paternalism. It's about how they think that the government should make decisions for major issues for the society and govern the society. So, this is a different view from the liberal perspective.

Kou's introduction of the term "paternalism" to describe Chinese Internet policy is essential, as I will show later. In the paper by Kou et al., it becomes clear that paternalism is an integral part of Confucianism: "With a central focus on individual virtues, Confucianism lends itself to a paternalistic governance model that relies on political leaders to promote and live by example, thus embodying the virtues."³⁷⁶ But the authors also argue that viewing paternalism as preferable

³⁷⁶ Kou, Semaan, and Nardi, "Human-Computer Interaction – INTERACT 2017," 3.

is an effect of the Chinese dedication to Confucianist culture. This attitude “signifies a trust in paternalistic structures that give the government considerable agency in utilizing censorship strategies considered best for the country” and links back to the “participants’ consideration of the Confucian virtue of propriety which explicitly attaches importance to the maintenance of the existing hierarchy and the rule of the government.”³⁷⁷

In a very illustrative example, one of the study participants said of the government’s crackdown on rumor-mongering mentioned above:

I have found that rumors often cause a lot of troubles in China. People are panicked easily. For example, recently there was a rumor on Weibo that a group of human traffickers secretly moved to my hometown. Suddenly all the parents began to pick up their children. They waited outside school gates and blocked the local traffic for hours. Later it turned out that this was a false rumor made up by a random high school student who was bored one day. So yeah, I think the government should take more responsibility in monitoring this kind of online information.³⁷⁸

The fourth virtue, Wisdom (智) manifests itself in how Chinese users express themselves online and prepare themselves before even pressing a key. It is a virtue to “develop knowledge about public events before engaging in public discussion.”³⁷⁹ Yubo Kou says that this is also the key to

³⁷⁷ Kou, “Interview, February 16,” 11.

³⁷⁸ Kou, 11.

³⁷⁹ Kou, Semaan, and Nardi, “Human-Computer Interaction – INTERACT 2017,” 3.

understanding how and when Chinese Internet users decide to circumvent technologies of censorship.

Wisdom is quite apparent. People care a lot about their self-knowledge, so actually this actually links back to my dissertation, where I used Foucault to discuss how people are situated in a very complex media system and all the sort of media powers try to push their own narratives and values onto individual citizens. They then sort of take a different path and step away from the technology and try to cultivate their knowledge about what is really going on in a movement or in political events, before they jump onto the Internet and make rash decisions or do something they haven't thought carefully about.

Another study participant, a 23-year old government employee echoes Kou's words about rash decisions online: "I see a lot of people making immediate, rash comments after reading one single piece of news. They do not even know whether it is true or not. Does this do any good to our online space and our society? Is this really the so-called freedom of speech? I think this is nothing but irresponsible."³⁸⁰ Wisdom also ties Chinese Internet users' relationship with the "Golden Shield", Kou says: "In our paper, Wisdom is about how they want to develop their own views and expertise in terms of knowing better about censorship works and knowing how to bypass censorship if they want to."³⁸¹ It speaks to the flexibility of Chinese Internet users:

³⁸⁰ Kou, Semaan, and Nardi, 11.

³⁸¹ Kou, "Interview, February 16."

People don't see censorship as a totally black or white thing, purely evil or purely good. Imagine that you are walking down the road, and there is a rock in front of you. What do you do? Do you hate it? No, you just bypass it. It's like natural instinct, right? So, if you want to do things, and you know there's a rock in your way, you can just bypass it and do whatever you want. That way, you might acquire knowledge and skills about *how* you bypass the rock.³⁸²

Thus, Kou proposes that Chinese Internet users are not guided by principle or ideology when they circumvent the government's censorship and surveillance technologies. Rather, they will circumvent if it is a necessary step in reaching their intended goal.

The final virtue, Integrity (信), is described thus by Kou et al. : “[Integrity] illustrates how a person's own words and deeds support the collective good. For example, if a person promises to support a collective action in specific ways, he or she should do so.”³⁸³ Like the second virtue, Kou says that this is variable: “Integrity is also more abstract. Like the second value, Righteousness, they are mostly normative“³⁸⁴ Yet, both righteousness and integrity are expressions of accountability in Chinese Internet culture:

The virtues of righteousness and integrity indicate individual responsibility for people's own online behavior. Participants criticized those who made rash comments and

³⁸² Kou.

³⁸³ Kou, Semaan, and Nardi, “Human-Computer Interaction – INTERACT 2017,” 2.

³⁸⁴ Kou, “Interview, February 16.”

emphasized the need for careful thought. Today's social media design often encourages users to take rapid actions such as clicking "likes" or retweeting. The speed encouraged by social media shifts activity away from deliberate, careful reflection.³⁸⁵

The resurgence of Confucianism in contemporary China

Kou et al. are not the only ones to have shown how Confucianism is expressed in contemporary Chinese society. A host of scholars have pointed to a resurgence of Confucianism in different areas of Chinese society in the past two decades. Cui and Wu see the government's use of traditional Chinese values, such as Confucianism as part of a set of tactics that "establish a perceived linkage between Internet governance and moral well-being and are further promoted by the dissemination of moral requirements, including the creation of "healthy and orderly" public spaces on the Internet."³⁸⁶ Confucianist concepts of order fit well with the promise of order made by the Xi government. As can be seen in the Rhetorical Frame described above, order is a recurring and central value extolled by Xi Jinping himself as well as the party behind him. Confucius' concept of order ranges from the ethical to the practical and is divided into three types of order: aesthetic, social and moral. All of these are primarily controlled through a single instrument: The Confucianist virtue of propriety.

³⁸⁵ Kou, Semaan, and Nardi, "Human-Computer Interaction – INTERACT 2017," 18.

³⁸⁶ Di Cui and Fang Wu, "Moral Goodness and Social Orderliness: An Analysis of the Official Media Discourse about Internet Governance in China," *Telecommunications Policy* 40, no. 2–3 (2016): 266, <https://doi.org/10.1016/j.telpol.2015.11.010>.

With regard to aesthetic order, Confucius believes in cultivating what Richey calls “good taste”³⁸⁷ by adhering to a hierarchical structure, i.e. “good taste” is what the elite at the top prefers. The Xi government’s aforementioned rooting out of sensationalism in the news and disempowerment of reality tv stars on social media because of “the glorification of scandals and the private lives of celebrities, the sensationalization of their conspicuous consumption and low taste”³⁸⁸ is in complete alignment with this Confucianist virtue. Socially, hierarchies are even more pervasive. Social order for Confucius is a system of hierarchies within hierarchies: “...rituals properly performed duplicate ideal hierarchies of power, whether between ruler and subject, parent and child, or husband and wife”.³⁸⁹ The CPC has very clearly molded these values into its paternalistic government strategies, thus equating an adherence to hierarchical power structures with stability and order. Finally, the virtue of propriety also informs morality: “good manners demonstrate both concern for others and a sense of one's place”, Richey writes³⁹⁰

Kou says that the Chinese people’s support of the current government’s policies (insofar as they haven’t overthrown it violently) is rooted in their preference for these very values:

It [all] comes from the virtue of propriety. Confucianism was developed 2,500 years ago and then it was enforced and adopted by many leaders of the dynasties. A lot of Confucian scholars dedicated their lives to developing this theory system and built it to

³⁸⁷ Jeff Richey, “Confucius,” The internet encyclopedia of philosophy (Internet Encyclopedia of Philosophy Pub), sec. 4. Harmonious Order, accessed April 16, 2018, <http://www.iep.utm.edu/confuciu/#H4>.

³⁸⁸ Pan, “China Shuts Down Harper’s Bazaar and 24 Others on WeChat.”

³⁸⁹ Richey, “Confucius.”

³⁹⁰ Richey.

support the narrative of the dynasties. So, naturally, propriety and the emphasis on paternalism is an important part of the development of Confucianism. The emperors of the dynasties wanted their people to know that it's natural and just for us to govern you and we will take good care of you. This mentality is different from democracy.³⁹¹

Additionally, in the Confucianism that China has been rooted in for millennia, morality is not just organized around an orderly, hierarchical structure, is also transcendent and metaphysical, beyond the reach of human definitional power. Richey describes how Confucius believes “Tian ("Heaven") is aligned with moral order but dependent upon human agents to actualize its will”, and that the virtue of propriety is “the instrument through which the family, the state, and the world may be aligned with Tian's moral order”.³⁹²

Confucianism, in other words, works in the favor of the Chinese state, and particularly Xi Jinping's value-based style of governance. If Confucianism is believed by the population to be the best path to stability and order, any other belief systems would rationally be seen as leading to higher levels of *disorder* and the spread of undesirable cultural norms. By promising faithfulness to Confucian principles, the Xi administration can position itself as the optimal catalyst for orderliness. Furthermore, a value system in which hierarchies are considered “heavenly” can never encourage uprisings and a flatter, or more network-based organization of

³⁹¹ Kou, “Interview, February 16.”

³⁹² Richey, “Confucius,” sec. Introduction.

the government's institutional structure. It feeds the paternalism and keeps a top-down political structure in place.

Hence, though it may only be a tactic, as Cui and Wu points out above, Chinese leaders have officially acknowledged Confucianism as their preferred guidance for China's future. Xi Jinping extolled the virtues of Confucius when China celebrated the philosopher's 2,565th birthday in 2014.³⁹³ Here, he compared the influence of Confucius on the current Communist party as being as important as that of the 1911 revolutionary hero, Sun Yat-Sen:

Members of the Communist Party of China are Marxists, who uphold the scientific theories of Marxism, and adhere to and develop socialism with Chinese characteristics. But Chinese communists are neither historical nihilists, nor cultural nihilists... Chinese communists have always been faithful inheritors and upholders of the country's fine cultural traditions. We have consciously absorbed nutrition from the teachings of Confucius to those of Sun Yat-Sen.³⁹⁴

An entire book has been dedicated to Xi Jinping's use of Confucius and other classic Chinese thinkers in his speeches and other public utterances.³⁹⁵ It should also be mentioned that the Chinese government since 2004 have sought to expand the knowledge of Chinese language and

³⁹³ Jinping Xi, "Xi Jinping's Speech in Commemoration of the 2,565th Anniversary of Confucius' Birth," Chinausfocus.com, 2014, <http://library.chinausfocus.com/article-1534.html>.

³⁹⁴ Xi.

³⁹⁵ "Xi Jinping: How to Read Confucius and Other Chinese Classical Thinkers," China Daily, 2017, http://www.chinadaily.com.cn/china/xismoments/2017-05/12/content_29324341.htm.

thought through opening branches of the Confucius Institute in countries across the world. These institutes are not, in spite of their name, dedicated solely to the teachings of Confucius, but impart information about China and Chinese culture writ large. They have been seen as an assertion of soft power, however.³⁹⁶

As it turns out, even the new government “social credit score” mentioned earlier can be related to Confucianism. Here, the government has stretched Confucius’ virtues and words into a 21st century context:

The word “credit” in Chinese – xinyong (信用) – is a core tenet of traditional Confucian ethics, which can be traced back to the late 4th century BC. In its original context, xinyong is a moral concept that indicates one’s honesty and trustworthiness. In the past few decades, its meaning has been extended to include financial creditworthiness.³⁹⁷

The return to Confucianism did not begin with Xi, even though he has been very vocal about his Confucianist leanings. Scholars such as Hofstede³⁹⁸ and Dirlik³⁹⁹ have shown how Confucianism seems to have guided the Chinese government through globalization and marketization throughout the last few decades.

³⁹⁶ J.F. Paradise, “CHINA AND INTERNATIONAL The Role of Confucius Institutes” 49, no. 4 (2009): 647–69.

³⁹⁷ Zeng, “China’s Social Credit System Puts Its People under Pressure to Be Model Citizens.”

³⁹⁸ Hofstede and Bond, “The Confucius Connection: From Cultural Roots to Economic Growth.”

³⁹⁹ Arif Dirlik, “Confucius in the Borderlands : Global Capitalism and the Reinvention of Confucianism,” *Boundary* 2 22, no. 3 (1995): 229–73.

Kou also disagrees that the Chinese government's public embracing of Confucianism is meant to signify a new leadership direction. Rather, he believes it is a form of populist appeasement, a way of showing that the government will follow the traditional, Chinese ways – even if it can be argued that their actual policies or agendas do not align with Confucianism. This would put Xi in alignment with other leaders around the world who, at the time of writing, underscore their commitment to the purported traditional values of their own countries as part of a nationalist wave also present in the West.

In February 2018, the CPC moved to further personify the idea of paternalism in Xi Jinping. The party proposed a removal of term limits on Chinese presidents, giving Xi Jinping an opportunity to lead the country indefinitely.⁴⁰⁰ Around the same time, state media began referring to Xi Jinping as *lingxiu*, the “People’s leader”.⁴⁰¹ The only two leaders to have been bestowed that title in China’s history are Mao and his chosen successor, Hua Guofeng. This comes only months after the CPC added Xi’s name to its constitution alongside Mao’s as sources of ideology and thought guiding the party.⁴⁰²

⁴⁰⁰ Chris Buckley and Keith Bradsher, “China Moves to Let President Xi Stay In Power, Ending Term Limit,” The New York Times, 2018.

⁴⁰¹ Staff, “Xi Jinping Is No Longer Any Old Leader - Core Upgrade,” The Economist, 2018, <https://www.economist.com/news/china/21737068-mao-would-be-proud-xi-jinping-no-longer-any-old-leader>.

⁴⁰² Tom Philips and Wang Zhen, “Xi Jinping Becomes Most Powerful Leader since Mao with China’s Change to Constitution,” The Guardian, 2017, <https://www.theguardian.com/world/2017/oct/24/xi-jinping-mao-thought-on-socialism-china-constitution>.

China's policy frames and the Rawlsian Frame

Based on the information laid out above, it would be easy to dismiss China as a state that is not well-ordered and its policies as being in insurmountable conflict with the Rawlsian Frame. But Rawls actually does consider and extend his conceptions of justice to nonliberal societies such as China. In *The Law of Peoples*, he describes how nonliberal societies can be recognized as “equal participating members in good standing with the Society of Peoples”⁴⁰³ – the latter being “all those peoples who follow the ideals and principles of the Law of Peoples in their mutual relations”.⁴⁰⁴ Together with abstaining from sanctions against these nonliberal societies, the recognition of them amounts to what Rawls calls “toleration” of nonliberal peoples. It is Rawls’ own insistence on rationality that forces him to include the toleration of nonliberal peoples in his Law of Peoples. One of the main pillars of Rawls’ well-ordered, liberal society is pluralism, and much of his theory of justice and fairness is dedicated to how a pluralist wealth of ideas and positions can be integrated into the basic structure of society. If he were to exclude nonliberal peoples, he would be in violation of his own pluralist principles. Rawls thus makes space for nonliberal peoples and opens up for their inclusion in societies that can be considered fair and just, though he maintains some principles for justice and fairness that cannot be violated. He uses the term *decent* about peoples who are not liberal, but who still constitute societies characterized by justice and fairness to a degree that liberal peoples should tolerate in the Society of Peoples. A society of decent people is one of five types of domestic societies defined by Rawls, the others

⁴⁰³ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 59.

⁴⁰⁴ Rawls, 3.

being *liberal peoples, outlaw states, societies burdened by unfavorable conditions* and *benevolent absolutisms*⁴⁰⁵ (italics in original).

In the following, I shall move forward by attempting to reconcile the Chinese policy frames relating to social media, as described above, with Rawls' definition of a decent people. The question here is whether the Chinese policies analyzed here qualifies China to be considered a decent society in Rawls' definition and as such deserves to be tolerated (again, in Rawls' definition) by liberal societies as a member of the Society of Peoples. If not, does China then belong to one of the other categories of societies defined by Rawls? If so, which one, and what does that classification say about the ethicality of Chinese social media policies?

Rawls' definition of decent hierarchical peoples

Rawls divides nonliberal, but decent peoples into to two categories, one of which he refuses to describe. He wants to keep leave this category "in reserve, supposing that there may be other decent peoples whose basic structure does not fit my description of a consultation hierarchy, but who are worthy of a membership in a Society of Peoples".⁴⁰⁶ The "consultation hierarchy" mentioned by Rawls here relates to the other category, which he describes in detail. He views the basic structure of this type of decent, nonliberal society as containing a "decent consultation hierarchy", leading him to name such peoples "decent hierarchical peoples". The "consultation" part of this definition may seem self-explanatory, but specifically, it refers to what Rawls calls an

⁴⁰⁵ Rawls, 63.

⁴⁰⁶ Rawls, 63.

associationist approach to a hierarchical, basic structure: “that is, the members of these societies are viewed in public life as members of different groups, and each group is represented in the legal system by a body”.⁴⁰⁷ It is important to note that Rawls does not describe this representation as necessarily being democratic, i.e. the representatives do not have to be elected by the members of society. If they were, the basic structure would be a democracy and subject to Rawls’ principles of a liberal society, rather than the principles of a decent consultation hierarchy.

Two criteria must be met for the latter type of society to be in good standing with the Society of Peoples, according to Rawls. First, it must be non-aggressive and pursue its goals through “diplomacy and trade and other ways of peace”.⁴⁰⁸ This is in line with Rawls’ definition of a well-ordered society as being non-expansionist, and, as I will describe in more detail below, an official policy of the Chinese government. The second criterion consists of three conditions relating to justice: A decent consultation hierarchy must secure human rights for all its members, it must impose moral duties and obligations on its members through law, and those who administer the legal systems (i.e. judges and other officials) must sincerely believe that the law is guided by a common good idea of justice.

The last criterion refers to justice officials’ belief that the law is just and not simply an instrument of force used to maintain a specific power structure. Rawls goes on to explore exactly what such a common good idea of justice entails. It is separate from what Rawls calls the

⁴⁰⁷ Rawls, 64.

⁴⁰⁸ Rawls, 64.

“common aim” of a people, which may be goals that are only indirectly linked to justice, such as prosperity or religious piety. The “common good idea of justice” is instead linked to the basic structure and the consultation hierarchy Rawls insists must be present, even in a nonliberal, undemocratic society:

...The legal system of a decent hierarchical people must contain a decent consultation hierarchy. That is, the basic structure of the society must include a family of representative bodies whose role in the hierarchy is to take part in an established procedure of consultation and to look after what the people’s common good idea of justice regards as the important interests of all members of the people.⁴⁰⁹

This “procedure of consultation” means that the voice of the people must be heard,

...not, to be sure, in a way allowed by democratic institutions, but appropriately in view of the religious and philosophical values of the society as expressed in its idea of the common good. Persons as members of associations, corporations and estates have the right at some point in the procedure of consultation (often at the stage of selecting a group’s representatives) to express dissent seriously and to give a conscientious reply...Judges and other officials must be willing to address objections. They cannot refuse to listen, charging that the dissenters are incompetent and unable to understand, for then we would have not a decent consultation hierarchy but a paternalistic regime.⁴¹⁰

⁴⁰⁹ Rawls, 71.

⁴¹⁰ Rawls, 72.

Here, we are getting close to the characterization of China’s social media policies and the censorship issues as described above. If, as Kou argues, the Chinese government uses the discourse on social media as a gauge for public sentiment, could it also be argued that this is part of a consultation procedure? Indeed, it could be argued that the corporations maintaining both the physical infrastructure of the Internet in China, as well as the communication services (such as social media) that run on the network, are “associations” in this particular sense. The collective of users on the social media platforms and the subgroups they divide into, can also, theoretically, be seen as such associations. The Chinese state’s involvement, both financially⁴¹¹⁴¹² and legislatively, in these associations, and its monitoring of them, could be viewed as the consultation hierarchy that Rawls refers to. If these institutions should not qualify as “associations” in a Rawlsian sense, the pervasive organization through trade unions and the heavily departmentalized bureaucracy of the Chinese state would likely qualify instead.

In addition, the strength of Confucianist culture in China, as described by Kou above, assures the adherence to some of the most foundational, Rawlsian principles, i.e. the duty of the individual to act according to the common conception of good in the particular society, as well as actually comprehending and agreeing to that common conception of good. Because Confucianism is so ingrained in Chinese culture and behavior, it could be argued that the choice off Confucianism as a belief system amounts to a social contract in the Rawlsian sense. The

⁴¹¹ Li Yuan, “Beijing Pushes for a Direct Hand in China’s Big Tech Firms,” The Wall Street Journal, 2017, <https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-1507758314>.

⁴¹² Raymond Zhong and Sui-Lee Wee, “China Seeks Small Stakes in, and More Sway over, Online Firms,” The New York Times, 2017.

virtues contained in the five constants in Confucianism, particularly *Yi* (righteousness/justice) does impose the moral duties and obligations on society's members, and also sets up the hierarchical structure that is the entire basis for Rawls' "decent hierarchical people" societal structure.

Human rights violations as disqualifiers of China as decent hierarchical people

Thus, at least at first glance, China looks like it might meet Rawls' criteria for a "decent hierarchical people". The arguments against this are the Chinese government's crackdown on dissenters, as described in the section on media oppression of this chapter, and China's human rights violations. I have already described the conditions of human rights in China above as they are presented by human rights organizations, and for Rawls, the respect for human rights is an unnegotiable condition of admission into the Society of Peoples, and by extension, the consideration of any related policy as being ethical. Rebecca Slayton illustrates the practical aspects of the same conflict, in that there is an inherent ethical problem in sacrificing human rights for security. She states that it's a false dichotomy to assume that you can't regulate information access without having to go so far as to violate human rights:

I think there is a lot of evidence of human rights abuses in China, and it not being an open and democratic system. To the extent that national security is about enabling that and keeping that injustice in place, I oppose it. I am for an open society where people have access to the information they need to have access to. That doesn't mean that you have to tell everybody how to make bombs.⁴¹³

⁴¹³ Slayton, "Interview, August 24."

The human rights situation in China thus disqualifies it from classification as a decent hierarchical people, but before moving on to how Rawls would evaluate and classify today's China in light of the human rights violation, I want to focus on the conditions for freedom of expression. The ability to voice dissent is closely tied to the social media policies in China, and I will therefore now move forward with the argumentation as if China does not violate human rights. By analyzing the conditions described above for the expression of political views publicly in China, it will be possible to assess how well the specific, related Chinese policies align with Rawlsian principles.

Rawls and Chinese paternalism

As Chan points out above, dissent cannot be voiced openly and publicly in China. In my interview with her, she expanded by saying that China's system of democratic centralism, theoretically, "encourages the freedom of speech internally", i.e. under private circumstances.

Once decisions are arrived at collectively, however, people are expected to comply with the decision top down, hence the word "centralism". Challenging these publicly - that's when the press kicks in - would be seen as "tian luan", "adding to the trouble", instead of contributing to the deliberative process. Both freedoms are conditionally provided to – theoretically – further the interests of the people in China... This is obviously very different from the Western liberal model where the two are seen as countervailing mechanisms against the intrusion of the state. This implied juxtaposition between the state and civil society is non-existent under democratic centralism. Theoretically, the voices of the people and that which the party, and the press (since it's going to be party-regulated

anyway) represent, should be compatible with one another. In practice, however, it may be a different story.⁴¹⁴

Your opinion can, as Kou stated earlier in the chapter, be voiced by circumventing public forums, or by using specific language. As Kou et al. show⁴¹⁵, a vernacular of phrases exists that is a type of satirical code which may cheat automated monitoring systems into not spotting critical language, but the fact that this is even necessary goes against Rawlsian principles, even in a decent consultation hierarchy. Rawls clearly asserts that public officials must be willing to listen to dissenting voices without any prejudice, particularly prejudices based on the dissenters being seen as “incompetent and unable to understand”. Rawls writes that this type of dismissal is an act of a “paternalistic regime”, which corresponds with the term Kou uses to describe Chinese society. Interestingly, Rawls does not explore paternalism further as a regime-describing characteristic in *The Law of the Peoples*, which you would expect after a statement like the one above. He does, however, explore the role of paternalism in the basic structure in *A Theory of Justice*. Here, he describes paternalism as morally permissible, but only if it is chosen freely by the individual. Rawls argues that paternalism can be useful in a basic structure to make decisions on behalf of those who are unable to do so rationally themselves, temporarily or permanently, e.g. because of illness, injury etc. It is essential for Rawls, however, that the paternalist surrender of rights is done under conditions characterized by all the liberal principles he stands for:

⁴¹⁴ Chan, “Interview, 2/27/2018.”

⁴¹⁵ Kou, Semaan, and Nardi, “Human-Computer Interaction – INTERACT 2017.”

Thus, the principles of paternalism are those that the parties would acknowledge in the original position to protect themselves against the weakness and infirmities of their reason and will in society. Others are authorized and sometimes required to act on our behalf and to do what we would do for ourselves if we were rational, this authorization coming into effect only when we cannot look after our own good.⁴¹⁶

The question, then, is whether the Chinese people have made such a decision? If you look at it from a sociocultural point of view, you might be able to stretch the Confucianism-as-collective-culture argument to the point where it can be said that the choice of Confucianism is also a choice of paternalism. But this goes against Kou's description of Confucianism as holding individualist properties through self-cultivation. And it also goes against Rawls' focus on this choice being made from an original position by the individual. This is, of course, in the ideal mode. In reality, it would be difficult to go back to the original position to make this choice, as it is always the case with Rawls. But the whole point of Rawls' idealist principles is to use them to use them as theoretical instruments: How would you do it if you could? In this case, I argue that Rawls' position would be that the individual choice of paternalism can be only be made under conditions where the individual can do so freely and rationally, as this would be the conditions the individual would be under in the original position. The choice of paternalism can only be made by others on your behalf if you are incapable of free and rational thinking. In the case of China, it seems unlikely that the entire population is mentally incapacitated and that the cultural

⁴¹⁶ Rawls, "A Theory of Justice," 269.

background of the people dominates their cognition to a point where they do not have rational instruments at their disposal in the cognitive toolbox. The paternalism in China must therefore, in Rawlsian terms, be forced upon the population either by the dominant culture or the regime in control. In either case, it cannot be ethical in Rawlsian terms, and the fact that Rawls does not explore the “paternalistic regime” further in *The Law of the People* should likely be read as referring back to his prior writing on the subject, i.e., among others, the quoted passage from *A Theory of Justice*.

This argument is further strengthened by the fact that when dissenters attempt to object against the paternalism thrust upon them, they risk being persecuted by the system as noted above. Not only is the choice of paternalism thus not made freely by individuals, it is also difficult, if not impossible, to choose not to adhere to paternalism without risking prosecution, which technically means that paternalism is enforced by the state and individuals are forced to choose it (if we remain within the Rawlsian mode considering paternalism as a choice). This is in violation of almost every principle of liberty in Rawls’ description of how citizens build the basic structure from the original position.

Rawls and information inequity: Slow informatization, “happy news” and the Golden Shield

The paternalism of Chinese society, along with its violation of human rights, thus disqualifies China from being a decent hierarchical people in Rawlsian terms. This is expressed in the policies above not only through the prohibition of free expression of dissent, but also through a limitation on the access to public media and information. First and foremost, the informatization of China that was seen by Deng Xiaoping in the 1970s as a path to development of rural areas cannot be characterized as having been an equitable process. As Ting and Yi has shown, half the

population of China lives in rural areas with limited access to information technology and the Internet, compared to the access available in technology hubs such as Shanghai or Shenzhen. Their study of broadband rollout in the Guangdong province showed that an effort led by a centralized government alone can have its limitations. The process was marred by : “(1) inefficient and wasteful spending resulting from interdepartmental rivalry (2) lack of policy continuity and institutional learning (3) lack of accountability and credible measurements (4) central planning resulting in gap between services and local needs.”⁴¹⁷ Furthermore, Ting and Yi concludes that similar rollouts in other provinces have been “slow, but stable”⁴¹⁸ By the end of 2016, there were 22.9 fixed-cable Internet subscriptions per 100 inhabitants in China.⁴¹⁹ CNNIC released a report in February 2018 stating that China has reached 772 million Internet users, out of which 97.5% are also mobile Internet users.⁴²⁰ A comparison of these two statistics indicate that there is a substantial amount of Chinese Internet users who only go online via smartphones, which has been shown not only to create inequities due to screen size differences, but may also favor more populated areas over rural areas⁴²¹ Overall, 55.8% of the Chinese

⁴¹⁷ Carol Ting and Famin Yi, “ICT Policy for the ‘Socialist New Countryside’—A Case Study of Rural Informatization in Guangdong, China,” *Telecommunications Policy* 37, no. 8 (September 1, 2013): sec. 636, <https://doi.org/10.1016/J.TELPOL.2012.03.007>.

⁴¹⁸ Ting and Yi, sec. 635.

⁴¹⁹ Doreen Bogdan-Martin et al., “The State of Broadband 2017: Broadband Catalyzing Sustainable Development,” 2017, https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf.

⁴²⁰ Nick Beckett and Amanda Ge, “CNNIC Publishes the 41st Statistical Report on China’s Internet Development in China,” Lexology, 2018, <https://www.lexology.com/library/detail.aspx?g=911ae57f-50da-4c53-ab75-2376272b2021>.

⁴²¹ Napoli and Obar, “The Emerging Mobile Internet Underclass: A Critique of Mobile Internet Access.”

population are Internet users, which is 4.1% over the global average at the time of writing. For comparison, the U.S. Internet penetration rate in 2018 is 89% for all adults and 94% for Americans aged 18-64.⁴²² In other words, the slow pace of informatization in China, even though it has been a central strategy for almost 40 years, is contributing to inequities in information access and access to emerging media, mostly along rural/city lines.

As we saw in chapter 3, the Russian influence operation targeting U.S. social media in 2016 had the ability to limit voters' information access by crowding out messages containing genuine news stories through the proliferation of fake news stories. Similar actions are being taken by the Chinese government, as King et al. point out⁴²³ The proliferation of "Happy News" may crowd out news from independent news sources inside China, and government pressure is being put on the latter sources to eschew the "public supervision" role in support of government messaging. As Susanne Chan told me, "Public supervision has become more common and applies to both tiers", i.e. both propaganda-oriented state media and partially state-owned media. However, the effect may be moderated by the "heightening" of "regulation over supervision by public opinion", as Chan described it in my interview with her⁴²⁴

This comes on top of the filtering of international news sources by the Golden Shield / Great Firewall system which means that international news stories are only available to Chinese

⁴²² Pew Research Center, "Demographics of Internet and Home Broadband Usage in the United States," Pew Internet, 2018, <http://www.pewinternet.org/fact-sheet/internet-broadband/>.

⁴²³ King, Pan, and Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument."

⁴²⁴ Chan, "Interview, 2/27/2018."

citizens through the use of VPNs and other means of circumvention. Just as I argued in the Russia chapter, I argue that this is in violation of what Rawls requires in order for a citizen to be able to be both a moral person and a fully capable democratic participant in society. The latter is moderated slightly in the case of China, who does not purport to be a democracy, and thus, the duties of the individual citizens are different. But even if China did qualify as a decent hierarchical people/society, the information required, according to Rawls, to express a person's full, moral capabilities would not be accessible. It can even be argued that Confucianist moral duties are impossible to fulfill because of this, if one accepts rationality as the basis of morality, such as Rawls does. *Zhi* is one of the five constants or virtues in Confucianism, meaning "knowledge".⁴²⁵ As Thompson writes:

Confucius might have accepted this epistemological summary of *zhi* 知 (knowledge, to know), but he made more of the problem of epistemic fallibility in the stream of life. Knowing that, in practice, things are not always what they appear to be, Confucius affirmed that "true knowledge (wisdom) consists in knowing that you do know what you do know and that you do not know what you do not know"⁴²⁶

⁴²⁵ It should be noted that scholars debate Confucius' use of *Zhi*. He uses the graph 智, which can also mean "wisdom", but as Thompson notes, this graph is composed of the graph for knowledge, 知, atop the graph for *Yue*, 曰, which means "to say" or "it has been said". Thus, "wisdom" here can be interpreted as "expressed knowledge", rather than the difference between "wisdom" and "knowledge" in the West, where "wisdom" would likely be construed as having a dimension of experience to it.

⁴²⁶ Kirill O. Thompson, "The Archery of 'Wisdom' in the Stream of Life: 'Wisdom' in the Four Books with Zhu Xi's Reflections," *Philosophy East and West* 57, no. 3 (2007): 331, <https://doi.org/10.1353/pew.2007.0040>.

This almost Socratic approach clearly assumes an epistemology characterized by rationality and critical thinking and encourages inquiry. Restrictions on information access also restricts the ability to inquire, of course, and thus the Chinese government is in violation of the Confucian principles its current and former leader officially have said they wish to promote. As Kou indicated, these statements were likely acts of appeasement rather than expressions of actual strategy.

Classifying China in Rawlsian terms

How, then, would Rawls characterize the current, Chinese society, if not a decent hierarchical society? It is doubtful that he would go so far as to name it an outlaw state. Though China has raised its military spending under Xi (per the policy document analyzed above) and the South China Sea conflict has escalated slightly in the same period, China still maintains a non-expansive, non-aggressive foreign policy, at least officially.⁴²⁷ Both in the Action Frame described above, as well as their overall strategy, there is very little to indicate that China is (currently) on a path that could classify the nation as being an outlaw state in Rawlsian terms. Rawls writes of the outlaw states that "...these regimes think a sufficient reason to engage in war is that war advances, or might advance, the regime's rational (not reasonable) interests"⁴²⁸ It should be noted that some practitioners and scholars view China's cyberattacks on Western

⁴²⁷ Elgebeily, "How China's Foreign Policy of Non-Intervention Is All about Selective Action."

⁴²⁸ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 90.

targets as acts of war⁴²⁹, but in most cases, as shown by Dunlap⁴³⁰ as well as Gombert and Libicki⁴³¹, these cyberattacks can either be construed as industrial espionage for commercial purposes, or as attempts to gather intelligence through the same means as the U.S. and other Western countries use in their intelligence-gathering efforts⁴³². As they, and also Rid⁴³³ argue, these activities are difficult to raise to the level of acts of war. In other words, though China is very active in its intelligence-gathering efforts in the cyber domain, this will not qualify it as an outlaw state in Rawlsian terms.

Rather, Rawls' description of certain nations as "societies burdened by unfavorable conditions (henceforth, *burdened societies*)"⁴³⁴ is a better description of China today. In

⁴²⁹ Siobhan Gorman and Julian E. Barnes, "Pentagon: Online Cyber Attacks Can Count as Acts of War," *The Wall Street Journal*, 2011, <https://www.wsj.com/articles/SB10001424052702304563104576355623135782718>; Bryant Jordan, "US Still Has No Definition for Cyber Act of War | Military.Com," *Military.com*, 2016, <https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html>.

⁴³⁰ Charles J. Dunlap Jr., "'Cybervandalism' or 'Digital Act of War?'" *America's Muddled Approach to Cyber Incidents Will Not Deter More Crises*, *North Carolina Journal of International Law* 42, no. 4 (2017): 989–1012, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=6455&context=faculty_scholarship.

⁴³¹ David C. Gompert and Martin Libicki, "Waging Cyber War the American Way," *Survival* 57, no. 4 (2015): 7–28, <http://www.tandfonline.com/doi/pdf/10.1080/00396338.2015.1068551?needAccess=true>; Martin C Libicki, "Cyberspace Is Not a Warfighting Domain," *Journal of Law and Policy* 8 (2012): 325–36.

⁴³² Libicki, "Interview, August 28."

⁴³³ Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* 92 (2013): 77–87.

⁴³⁴ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 106.

alignment with Kou's description of China as still being "a developing nation" rooted in the conditions and traditions of "an agricultural society"⁴³⁵, Rawls describes burdened societies thus:

Burdened societies, while they are not expansive or aggressive, lack the political and cultural traditions, the human capital and know-how, and, often, the material and technological resources needed to be well-ordered. The long-term goal of (relatively) well-ordered societies should be to bring burdened societies, like outlaw states, into the Society of well-ordered Peoples. Well-ordered peoples have a *duty* to assist burdened societies.⁴³⁶ (italics in original).

Here, Rawls again maintains consistency with his own principles. He actively transcends the duty-bound nature of the deontological ethics found in his social contract theory to the level of international relations. Rawls comes close to privileged post-colonialism here, and unless you read him closely, he could be understood as assuming that a liberal, well-ordered society is the ultimate goal for any nation, thus thrusting a very Western view upon other peoples: "I would further conjecture that there is no society anywhere in the world – except for marginal cases – with resources so scarce that it could not, were it reasonably and rationally organized and governed become well-ordered."⁴³⁷

⁴³⁵ Kou, "Interview, February 16."

⁴³⁶ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 106.

⁴³⁷ Rawls, 108.

It is important to note, however, that Rawls uses the word “could”, not “would”. The context of the quote is important in the case of China. Rawls writes this in relation to wealth and how other nations should help burdened societies financially. His point is that it is not a country’s economic situation that determines whether it is well-ordered or not. It is its political culture, virtues and will. This is one of the few cases in which Rawls addresses China directly:

Some societies – China is a familiar example – have imposed harsh restrictions on the size of families and have adopted other draconian measures. But there is no need to be so harsh. The simplest, most effective, most acceptable policy is to establish the elements of equal justice for women. Instructive here is the Indian state of Kerala, which in the late 1970s empowered women to vote and to participate in politics, to receive and use education, and to own and manage wealth and property. As a result, within several years Kerala’s birth rate fell below China’s without invoking the coercive powers of the state.⁴³⁸

(It should be noted that China abolished the one-child rule in 2015, although according to Human Rights Watch, this did not end the human rights issues related to reproductive rights⁴³⁹) Rawls’ argument here is that the political will of a people will also determine its economic conditions. This, of course, is a very Western notion, in line with Rawls’ liberalism. However, it is important to note that throughout *The Law of Peoples* there is no insistence from Rawls that inclusion in

⁴³⁸ Rawls, 110.

⁴³⁹ Human Rights Watch, “World Report 2016: China | Human Rights Watch,” World Report 2016, 2015, <https://www.hrw.org/world-report/2016/country-chapters/china-and-tibet>.

the Society of Peoples should be contingent on a national strategy leading towards a Western-style democracy. He spends a large part of the text on describing an imaginary Muslim state that could be included in the Society of Peoples, Kazanistan, in which there is a decent consultation hierarchy, and thus the respect for the individual's voice and ability to express moral capabilities and is intact. Though Rawls sees his conception of a well-ordered, liberal society as a preferred system of government, he understands that it isn't necessarily something to be imposed on the rest of the world. As mentioned above, this would be in violation of his own insistence on pluralism as a moral virtue.

In other words, Rawls is willing to accept burdened societies into the Society of Peoples if they meet certain conditions that won't necessarily put these societies on the path to Westernization. A nation or people must first and foremost for human rights and voices of dissent as essential, unassailable virtues to be part of the Society of Peoples. Societies based on different regulatory cultures and traditions than Western democracy can still be ethical this way. To understand how he would include burdened societies in the Society of Peoples, it is helpful to look to another definition of the term offered by Rawls. He expands upon the first part of the definition above by describing burdened societies as societies "whose historical, social and economic circumstances make their achieving a well-ordered regime, whether liberal or decent, difficult if not impossible".⁴⁴⁰ With Rawls' insistence on international pluralism and toleration of nonliberal peoples, could China be seen as meeting these conditions? Considering the analyses and sources in this chapter, it is not unreasonable to view the thousands of years of Confucianist

⁴⁴⁰ Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*, 90.

dominance of Chinese thought as a hindrance to achieving a well-ordered regime in the manner described by Rawls above. Confucianism, with its acceptance of a “natural” hierarchy based on e.g. class, kinship and history, its inherent respect for authority enforced in this hierarchy, its emphasis on individualism with natural limits, its focus on propriety in behavior and attitude and its adherence to a specific epistemology, may in fact be so powerful that a “well-ordered” (in Rawlsian terms) China is “difficult if not impossible”.

Yet this does not make China’s social media policies ethical. Though Chinese citizens may find ways around the censorship, both the strategies of censoring and drowning out dissenting voices goes against Rawls’ principles for a decent society that could be included in the Society of Peoples. Monitoring the discourse of the people to gauge the general attitude of the people and acting accordingly, as is the strategy of the Chinese government, is not a sufficient method of listening to dissent in Rawls’ view. Further, as seen earlier in the chapter, it is also an infringement of the privacy rights of the individual, although privacy is such a Western concept that this type of surveillance would likely not (on its own) keep China from entering into the Society of Peoples if Rawls were to be the judge. As mentioned elsewhere, Rawls’ approach to privacy does not constitute a substantial part of his overall theoretical work.

Chapter Conclusion

China is no longer burdened economically as a nation (although many of its citizens still live in poverty⁴⁴¹⁴⁴²), so it is merely its political traditions, virtues, culture and actions that makes it a burdened society. China's lack of adherence to human rights (which are viewed by Rawls as unconditioned by culture, religion, tradition or politics) and crackdown on dissent keeps it from being admissible into Rawls' Society of Peoples. If China was to reduce its censorship and control of social media and respect human rights, it can be a Communist state with a Confucianist mindset and still be admitted to the Society of Peoples as a mostly ethical society according to Rawls. With Xi's recent consolidation of power, the Chinese state may take an even more aggressive stance towards the media, including social media, in the future. As Chan told me in my interview with her:

The picture is far from rosy. I'd expect more stringent control over the media in the future. Party legitimacy and the maintenance of stability, or "wei wen", are high priorities in China, and the party considers censorship as one key strategy. I doubt this is sustainable in the long run. Anyone who believes in equality and freedom would of course consider policies that suppress them problematic. It is a problem when power is highly concentrated and when there is no effective mechanism to ensure accountability and representation on the national level. At the same time, I don't think it's going to get us too far, if the point of

⁴⁴¹ Shannon Tiezzi, "Is This the Year China Gets Serious About Ending Rural Poverty?," *The Diplomat*, 2018, <https://thediplomat.com/2018/02/is-this-the-year-china-gets-serious-about-ending-rural-poverty/>.

⁴⁴² Human Rights Watch, "World Report 2018: China | Human Rights Watch."

this conversation is to understand the issues better, if we simply stick to a good vs. evil narrative.⁴⁴³

However, it is not just the Chinese government that has realized the duality of the power of the social media infrastructure, being both a tool of suppression and a threat to its authority. The contours of similar policies are beginning to take shape in the United States, albeit at a much smaller scale, at least for the time being. Critics are worried, however, that these tendencies can take hold, even in an open democracy such as the United States. In the next chapter, I will show how the same type of paternalist rhetoric used by the Chinese government is emerging in defense of social media policies being promulgated by the Trump administration, and how these policies can lead directly to the same type of chilling effect that dominates Chinese social media, but this time in the land of the free and the home of brave.

⁴⁴³ Chan, "Interview, 2/27/2018."

Chapter 5: Violations of privacy rights on social media in the name of national security

In the preceding chapters, I have presented analyses of a broad, domestic social media strategy (China) and a narrower, offensive social media strategy aimed at foreign powers (Russia), both contained within the overlapping area between information security and cybersecurity at the national level. In this chapter, I will focus even more narrowly on a specific policy proposed, enacted and implemented by an agency within the federal government of the United States.

Whereas the previous chapters have been concerned with applying security measures within the information sphere, the policy I will analyze in this chapter reaches outside this sphere and into what in military terms is known as kinetic security. To put it differently, in the preceding chapters, I have analyzed information strategies implemented by governments for information security purposes.

The policy analyzed in this chapter prescribes a strategy aimed at using information to target broader, physical challenges to national security. The Chinese and Russian policies are aimed at knowledge, attitudes and beliefs. The U.S. policy I will now analyze is aimed at stopping bombs from going off in major cities. The question, of course, is whether this is effective, and whether that effect is worth the values sacrificed and rights surrendered. The policy I will study in this chapter is a part of the larger information-gathering and surveillance measures put in place by the U.S. government in its efforts to fight terrorism. On its face, it may seem like a small tactic aimed at a very specific group of people that may not seem large enough

to warrant a full, ethical exploration. However, as I will show in the following and the discussion towards the end of the chapter, both the universality requirement of Rawlsian ethics as well as the concrete, real-world consequences of the policy elevates it to a level that concerns the entire population and can be seen as extremely relevant for matters of both privacy, individual freedom and citizens' rights. The two policies studied in this chapter can actually be considered as one - a sort of "dual" policy on social media now implemented by the Department of Homeland Security (DHS). In the following, I will refer to it as one such dual policy.

In the first part of the dual policy, the DHS has now made it possible for law enforcement officers with the Customs and Border Protection agency (CBP) to demand that not only foreign nationals, but also U.S. citizens and permanent residents entering the U.S. unlock personal electronic communication devices, so the officers can study their contents – including social media profiles. Though this policy is not directed exclusively at social media for data collection or monitoring on paper, statements have been made on behalf of the DHS indicating that social media is indeed a vital information source during border searches of electronic devices.

I will analyze this policy in combination with a related social media policy, in which the DHS registers social media information about naturalized U.S. citizens and permanent residents as part of their immigration files. As I will show, these policies challenge U.S. privacy right traditions as well as notions of individual liberty – two concepts that are seen by some as inseparable and fundamental to the United States' national identity. As in the previous chapters, I will begin by presenting the background for the policies, which in this case includes a short history of social media and a historical overview of post-WWW U.S. electronic communication surveillance projects relevant to this study. This will be followed by a description of the policies

under analysis, once again providing the arguments supporting the policies in a Rhetorical Frame first, and an Action Frame containing the real-world policy actions second. I will then provide a cultural context through a discussion of the policies in the light of the American tradition of liberty and the ideal of individualism, and finally, I will use Rawls' foundation in that same tradition as a bridge into the final contrasting and comparison of the dual policy with the Rawlsian Frame.

Background

A short history of social media

Although the term "Social Networking Site" and its acronym "SNS" may be losing both their validity and widespread use, boyd and Ellison's definitional paper from 2007 is still the most authoritative of its kind when it comes to classifying social media. In their definition, social media sites contain at least three characteristics that allow users to : "(1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."⁴⁴⁴ Many other characteristics of social media have emerged since, of course, but these three still constitute the foundation of all both newer and older social media platforms. Of course, it can be argued that these criteria would also apply to earlier, online platforms with social functionality. The SMS text message function in some 1990s mobile phones would almost

⁴⁴⁴ Edward Grabb, Douglas Baer, and James Curtis, "The Origins of American Individualism: Reconsidering the Historical Evidence The Origins of American Individualism: Reconsidering the Historical Evidence," *Source The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie* 24, no. 4 (1999): 524-25, <http://www.jstor.org/stable/3341789>.

qualify as social media according to these characteristics, as would some chat functions on early networks and online services,⁴⁴⁵ were it not for the lack of public disclosure of the "buddy list". Thus, in the case of both this chapter as well as boyd and Ellison's paper, the concern is with "social networking *sites*", referring to (at least at their inception) services that can be found in the form of websites or mobile apps that utilize the HTTP and/or IP protocols. I make this distinction solely to limit the amount of historical material for the study to evidence from older services that resemble the current ones that are relevant to the policies analyzed here.

Sixdegrees.com is, not least due to the work by boyd and Ellison, widely regarded as the first social media platform resembling the platforms we have today. Launched in 1997, it was ahead of its time, but with sharing culture still waiting to emerge along with Millennials becoming old enough to use the Internet, Sixdegrees.com failed to become a viable business and shut down in 2000. In its wake came blogs and a few other platforms that facilitated social interaction and could very easily give web users a presence online. In 2002, Friendster was launched by Jonathan Abrams from his apartment in San Francisco. By 2003, the service had gathered millions of users and raised \$13 million from some of the investors behind the web giants of the time, Amazon, eBay and Yahoo! That same year, MySpace was launched, which

⁴⁴⁵ danah m. boyd and Nicole B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication* 13, no. 1 (October 1, 2007): 210–30, <https://doi.org/10.1111/j.1083-6101.2007.00393.x>; Rich Ling and Naomi S. Baron, "Text Messaging and IM: Linguistic Comparison of American College Data," *Journal of Language and Social Psychology*, 2007, <https://doi.org/10.1177/0261927X06303480>.

rose in popularity at an even faster pace, and by March of 2007 one in five Americans visited the social media platform every month.⁴⁴⁶

In 2004, Facebook launched as a social networking platform for students at Harvard University. By then, a host of services with the sole purpose of facilitating profile presentations and social network communication had launched, such as Hi5, Orkut, Tribe.net and Xing, along with interest-specific sites that included social functionality, such as LinkedIn, Couchsurfing, Last.FM, Dogster and Flickr. When Facebook expanded beyond Harvard to American high schools in 2005, even more services of both the generic and the interest-specific kind had launched, such as YouTube, Ning and Bebo. Two services that had already been launched in 1999 were relaunched, AsianAvenue and BlackPlanet.⁴⁴⁷ At this time, similar platforms fitting the boyd and Ellison definitions were being launched locally countries outside the U.S., such as Cyworld and QQ in China⁴⁴⁸, Skum and Arto in Denmark⁴⁴⁹, Hyves in the Netherlands⁴⁵⁰ and LunarStorm in Sweden.⁴⁵¹

⁴⁴⁶ Diane Kholos Wysocki, “Let Your Fingers Do the Talking: Sex on an Adult Chat-Line,” *Sexualities* 1, no. 4 (1998): 425–52, <https://doi.org/10.1177/136346098001004003>.

⁴⁴⁷ Max Chafkin, “How to Kill a Great Idea,” Inc., 2007, <https://www.inc.com/magazine/20070601/features-how-to-kill-a-great-idea.html>.

⁴⁴⁸ boyd and Ellison, “Social Network Sites: Definition, History, and Scholarship.”

⁴⁴⁹ boyd and Ellison.

⁴⁵⁰ Morten Bay and Julie Ralund, *Generation Netværk* (Copenhagen, Denmark: DR, 2006).

⁴⁵¹ boyd and Ellison, “Social Network Sites: Definition, History, and Scholarship.”

As José van Dijck noted in 2013, it was around 2005 that social media user growth really took off, which meant higher maintenance and development costs for the corporations, and more pressure to find sustainable revenue streams:

As user bases began to explode after 2005, the investment required of users became too big, and the focus of most platforms was diluted. At the same time, many platforms were taken over by big media corporations or were otherwise incorporated; the spirit of "nonmarket peer-production" soon dwindled. During the ensuing years, between 2005 and 2008, corporate owners remained cautious about exposing their profit motives to user communities, and in many instances kept nourishing the image of platforms as peer-production structures that put users before profits.⁴⁵²

In June 2009, Internet traffic and audience metrics company ComScore proclaimed that their traffic analyses showed that the popularity of Facebook had surpassed that of MySpace. From this point in time, the social media realm starts shifting shape into what that realm looks like in 2018: Facebook is by far the most popular social media platform worldwide with more than 2bn monthly users followed by its competitors in the general-interest category in the following order: Instagram (owned by Facebook), Tumblr, QZone/QQ (China), Sina Weibo (China), Twitter and

⁴⁵² Van Dijck, *The Culture of Connectivity: A Critical History of Social Media*, 15.

Snapchat. Messenger services with social functionality are ranked as follows: WhatsApp (owned by Facebook), Facebook Messenger, WeChat (China), QQ and Skype.⁴⁵³

U.S. government surveillance of social media and other electronic communication

U.S. policies towards monitoring social media are conditioned by parameters that can be viewed along three dimensions:

- 1. Domestic or international?** First and foremost, there is the question of locale and nationality: Are the social media platforms being monitored located in the U.S. or abroad? Are the social media users involved U.S. citizens or foreign nationals? These two questions determine which agencies are able to perform the monitoring, and which kind of legal conditions must be met for the monitoring to take place.

- 2. Public or private?** Another dimension to consider is which kind of social media are being monitored. Does the monitoring and subsequent data gathering happen on social media platforms where all, most or some user activity is publicly accessible? Or does it happen on platforms that require some kind of login and interaction with the user before their activity becomes visible to the investigator or investigating system?

- 3. Network, platform or device?** Monitoring, surveillance and investigation can happen at different levels. If all Internet traffic passing through a specific network node is monitored, then so is the social media traffic contained therein. Monitoring can also

⁴⁵³ "Lunarstorm," *Nationalencyklopedin* (National Swedish Encyclopedia), accessed March 11, 2018, <https://www.ne.se/uppslagsverk/encyklopedi/lång/lunarstorm>.

happen at the platform level, where not all Internet traffic is monitored and/or collected, but only the traffic related to a specific social media platform or activity. This kind of monitoring can also happen as simple, regular user interaction within the platform itself. Finally, monitoring happens at the device level, e.g. when investigators focus on a single individual's smartphone or laptop and the social media activities registered on it.

As mentioned above, the policies I analyze in this chapter cover all of the dimensions listed here. However, I will be focusing on the dimensions in 2 and 3 as they pertain to the domestic monitoring as mentioned in 1. To narrow it down further, I will only be looking at a dual social media policy enacted by the Department of Homeland Security.

This dual social media policy is situated in a very specific historical context of social media surveillance in the United States. Excluding, as mentioned earlier, the pre-web social media services, most American social media platforms may very likely have been under surveillance by several governments from their very inception, beginning with SixDegrees.com. The latter, as well as early social media platforms that emerged between 1997 and 2001, such as AsianAvenue and BlackPlanet may have been monitored and been subject to data collection under the ECHELON program.

ECHELON

British investigative journalist Duncan Campbell was the first to disclose the existence of ECHELON, which became a pop cultural phenomenon as a symbol of government surveillance of electronic media for in early web culture, and activists even held “Jam Echelon” days,

beginning in 1999.⁴⁵⁴ However, ECHELON was also a precursor to many of the surveillance initiatives revealed by Edward Snowden in 2013⁴⁵⁵, which was the reason some surveillance and security studies scholars and practitioners were unsurprised⁴⁵⁶ – and some unimpressed⁴⁵⁷ – by Snowden’s revelations. In 1988, in an article in *New Statesman*, Campbell revealed that “American, British and Allied intelligence agencies are soon to embark on a massive, billion-dollar expansion of their global electronic surveillance system”, at the time known as Project P415. According to Campbell’s sources, the new system would put in place satellite listening stations across the globe, which would augment the signal intelligence (SIGINT) efforts already taking place through wiretapping international communication networks, then mostly telephone networks. The new system would build on the common SIGINT operations being performed⁴⁵⁸ jointly under the so-called Five Eyes agreement between the intelligence services of The United

⁴⁵⁴ Statista, “Global Social Media Ranking 2018 | Statistic.”

⁴⁵⁵ Dogcow, laslo, and Robert Kemp, “Jam Echelon Day - 21st Oct 1999,” Thing.net, 1999, <https://www.thing.net/~rdom/ecd/jam.html>; Ewen Macaskill and Gabriel Dance, “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained | US News | Theguardian.Com,” *The Guardian*, 2013, <https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>.

⁴⁵⁶ Lawfare, “Snowden Revelations,” *Lawfare Blog*, 2018, <https://lawfareblog.com/snowden-revelations>.

⁴⁵⁷ Lou Kilzer, “Snowden’s ‘secrets’ Should Not Surprise,” *TribLive*, 2013, <http://triblive.com/news/editorspicks/4408043-74/nsa-snowden-program>; Armerding Taylor, “NSA Surveillance Controversy: Much Ado about Nothing New?,” *CSO*, 2013, <https://www.csoonline.com/article/2133558/strategic-planning-erm/nsa-surveillance-controversy--much-ado-about-nothing-new-.html>.

⁴⁵⁸ Joshua Rovner, “‘Exclusive’ on NSA Surveillance Reveals Almost Nothing New,” *War on the Rocks*, 2014, <https://warontherocks.com/2014/07/exclusive-on-nsa-surveillance-reveals-almost-nothing-new/>.

States, The United Kingdom, Canada, Australia and New Zealand⁴⁵⁹ that came into being after World War II, in 1947.⁴⁶⁰

ECHELON was already in existence as part of the Five Eyes agreement when Campbell wrote his article, having been established in the 60s and enacted with its first eavesdropping network in 1971.⁴⁶¹ But it was not as organized, as technologically advanced or pervasive as it would become within the structure of the new project. The new structure put the U.S. National Security Agency (NSA) and its British counterpart, Government Communication Headquarters (GCHQ) in charge of administration and maintenance of the system, giving them access to the resources of intelligence services in Canada, Australia and New Zealand as part of the project. This arrangement was known as the UKUSA agreement. As the Eastern Bloc and the Warsaw Pact crumbled between 1989 and 1991, the necessity for SIGINT from that part of the world was reduced. A new motivation for maintaining the also came in the same period due to the commercialization of the Internet in the late 1980s, and shortly after, the expanding popularity of the World Wide Web. ECHELON came back into public eye in 1996 in a book by investigative journalist Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network*.⁴⁶² .The renewed, public attention to ECHELON also reached members of the European Parliament

⁴⁵⁹ Armerding Taylor, "NSA Surveillance Controversy: Much Ado about Nothing New?"

⁴⁶⁰ James Cox, "Canada and the Five Eyes Intelligence Community," 2012, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.357.5576&rep=rep1&type=pdf>.

⁴⁶¹ Staff, "What You Need to Know about Echelon," BBC.co.uk, 2001, <http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm>.

⁴⁶² Staff.

who became concerned about the consequences for privacy rights and geopolitical collaboration, if ECHELON really existed. (The system was kept secret even from the NATO partners of the Five Eyes countries). In 1997, a group of parliamentarians ordered an investigation of the matter to be conducted by The Omega Foundation, a research group located in Manchester, England. The lead investigator was Steve Wright, who in January 1998 delivered his first report to the so-called STOA (Science and Technology Office of Assessment) department of the European Parliament. The report detailed the technical workings and some of the defense contractors involved in building the system.⁴⁶³ The STOA report also details how

ECHELON is designed for primarily non-military targets: governments, organisations and businesses in virtually every country. The ECHELON system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like Memex to find key words... Each of the five centres supply "dictionaries" to the other four of keywords, Phrases, people and places to "tag" and the tagged intercept is forwarded straight to the requesting country.⁴⁶⁴

Some European parliamentarians reacted to the STOA report with major concerns. During 1998 and 1999, they submitted questions to the EU government's upper chamber, the European Commission, trying to ascertain what Commission members knew about ECHELON, but: "The

⁴⁶³ Nicky Hager, "Secret Power. New Zealand's Role in the International Spy Network," *Nelson: Neuseeland*, 1996.

⁴⁶⁴ Flaxman, Goel, and Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption."

Commission's replies were evasive and stated that these questions did not fall within its remit, claiming that it could not act on the basis of non-official information."⁴⁶⁵

After several failed attempts, a group of European Parliament members were successful in getting a majority vote in the parliament for the establishment of an investigatory committee on ECHELON in July 2000. 36 members of the European Parliament made up this committee that would call on expert testimony from, among others, Nicky Hager and Duncan Campbell, but also James Bamford, an American investigative journalist who has written several books on the NSA. In addition, a vast analysis of documents provided by member countries' intelligence services as well as reports and testimonies from local member countries' experts and investigative journalists were included in the final report by the committee. In the first half of 2001, the committee traveled to Paris, London and Washington, DC on a fact-finding mission to glean what they could from intelligence operatives in those cities. A number of U.S. intelligence officials refused to meet with the European parliamentarians.⁴⁶⁶

The final report from the committee investigating ECHELON, known as *The Schmid Report* was adopted by the committee on July 3. It unequivocally determined that ECHELON existed, had global reach and had the ability to intercept virtually all forms of telecommunications.⁴⁶⁷

⁴⁶⁵ Steve Wright, "An Appraisal of the Technology of Political Control" (Luxembourg, 1998), 19–20, http://www.europarl.europa.eu/pdf/jadis/2013_12/8.PE4_AP_PV!LIBE.1994_LIBE-199801260050EN.pdf.

⁴⁶⁶ Franco Piodi and Iolanda Mombelli, "The ECHELON Affair - European Parliament History Series," 2014, 11, http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf.

⁴⁶⁷ Piodi and Mombelli, 31.

A resolution was now drafted based on the adoption of the Schmid report. The resolution would force EU member countries to negotiate surveillance agreements with the U.S. that adhered to the European Convention on Human Rights (ECHR) with regards to privacy rights. The resolution also banned using intelligence services such as ECHELON for economic gain, and restricted participation of member countries in ECHELON-related activities. The resolution also condemned any unauthorized eavesdropping that might have occurred. The resolution was adopted on September 6 by the European Parliament, essentially confirming the official European stance that ECHELON was real and had to be restricted by law. Five days later, on September 11, 2001, the Al-Qaeda attacks on New York City and Washington D.C. silenced any debate about ECHELON in the U.S. and Europe.

Several public officials from the Five Eyes nations have since confirmed the existence of ECHELON,⁴⁶⁸ as did revelations from the NSA document leak by Edward Snowden.⁴⁶⁹ It is uncertain whether the ECHELON system intercepted information from social media sources. What we do know is that between SixDegrees.com's launch in 1997 and September 11, 2001, millions of Internet users (in the U.S. and abroad) signed up for both U.S.-based social networks such as SixDegrees, AsianAvenue and BlackPlanet⁴⁷⁰ that social media platforms were

⁴⁶⁸ Piodi and Mombelli, "The ECHELON Affair - European Parliament History Series"; Andrew Bomford, "Echelon Spy Network Revealed," BBC, 1999, <http://news.bbc.co.uk/2/hi/503224.stm>.

⁴⁶⁹ Staff, "What You Need to Know about Echelon."

⁴⁷⁰ Duncan Campbell, "Global Spy System ECHELON Confirmed at Last – by Leaked Snowden Files • The Register," The Register, 2015, http://www.theregister.co.uk/2015/08/03/gchq_duncan_campbell/; Staff, "May 1997: Six Degrees - Then and Now: A History of Social Networking Sites," CBS News, 2011, <https://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites/2/>; Anthony Ramirez, "NEW YORK ON LINE; One Site, 14 Ethnic Groups," The New York Times, 1998,

beginning to emerge in other countries around the globe⁴⁷¹ and that some U.S. citizens and residents would frequent or sign up for these. At the time, it was a more acceptable practice to have notifications of interactions on the social media platforms e-mailed to you, and the massive e-mail collection in the ECHELON systems may have collected social media this way.

The USA PATRIOT Act

In response to the attacks on 9/11, as well as subsequent anthrax mail attacks, the U.S. Congress passed the USA PATRIOT act on October 26, 2001, a mere 45 days after the attacks. It had been proposed within a week of the attacks.⁴⁷² The name of the law was an abbreviation of “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”, which is a fairly accurate name, considering what the law did. It was, in effect, a massive deregulation of surveillance legislation, giving the intelligence community and law enforcement a much wider range of tools for intelligence gathering. The ACLU described the law thus:

The Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit reporting records, and track the

<http://www.nytimes.com/1998/04/12/nyregion/neighborhood-report-new-york-on-line-one-site-14-ethnic-groups.html>.

⁴⁷¹ Dara N Byrne, “Public Discourse, Community Concerns, and Civic Engagement: Exploring Black Social Networking Traditions on BlackPlanet.Com,” accessed March 18, 2018, <https://doi.org/10.1111/j.1083-6101.2007.00398.x>; “Lunarstorm.”

⁴⁷² TimeWarner, “ICQ Celebrates 100 Million Registered Users | Time Warner Inc.,” Press Release, 2001, <http://www.timewarner.com/newsroom/press-releases/2001/05/09/icq-celebrates-100-million-registered-users>.

activity of innocent Americans on the Internet. While most Americans think it was created to catch terrorists, the Patriot Act actually turns regular citizens into suspects.⁴⁷³

Because of the present study's focus on social media, it is the expanded capabilities for surveillance on the Internet that is of interest here. Several methods became available to law enforcement and the intelligence community in this regard with the enactment of The Patriot Act. One such method consisted of the issuance of so-called National Security Letters (NSLs) that gave the FBI the ability to request e.g. personal phone or computer records (as well as financial information) without obtaining a court order or a warrant first. According to the ACLU, out of 143,074 NSLs issued between 2003 and 2006, only 53 led to actual criminal referrals to a prosecutor – none of them were terrorism-related. Out of all the 192,499 NSLs issued in that same period, only one led to a terrorism-related conviction, which could have been obtained even without The Patriot Act being enacted. Any information about a person gathered by use of an NSL could be kept by the FBI indefinitely, and receivers of NSLs were prohibited from telling anyone about the letter. The Patriot Act also enabled the so-called “sneak and peek” searches, wherein federal law enforcement officials could conduct a (court-ordered or warranted) search of an individual's property, home or office without giving notice first. The law enabled the notification to happen after.

Regarding Internet monitoring more specifically, the Patriot act also made ECHELON-like data collection technologies explicitly legal and brought it out in the open. As Whitaker writes:

⁴⁷³ Reg Whitaker, “A Faustian Bargain? America and the Dream of Total Information Awareness,” in *The New Politics of Surveillance and Visibility* (Toronto: University of Toronto Press, 2006), 141–70.

With regard to methods of identifying senders and receivers of telephone communications, section 216 extends court orders to cover e-mail messages and Internet use, and to cover the entire United States as opposed to the former limit to the judicial district in which the court has jurisdiction. Critics point out that, even though the capture of message content is specifically prohibited, e-mail header information, which may include subject headings, or the addresses of specific web sites visited, may be much more revealing than the simple telephone numbers previously captured. This provision may provide sanction to the FBI's CARNIVORE program, even though once installed by an Internet service provider, CARNIVORE may monitor all the communications of all subscribers, not just those targeted by a court order.⁴⁷⁴

Writing in 2006, Whitaker elaborates on what CARNIVORE was, while at the same time acknowledging ECHELON's existence:

A system called ECHELON links all the computers among the UKUSA agencies using a set of keywords in a dictionary contributed by all the agencies; flagged messages are automatically muted to the country or countries that entered the particular keyword flag. In the United States, the FBI had, before 9/11, begun deploying CARNIVORE, a super search engine which, when installed on Internet service providers, is capable of trolling

⁴⁷⁴ ACLU, "Surveillance Under the Patriot Act | American Civil Liberties Union," ACLU.org, accessed March 11, 2018, <https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>.

through e-mail traffic and flagging communications of interest to the agency based on the identities of senders and receivers, keyword recognition, and so forth.⁴⁷⁵

In other words, these collection systems existed prior to 9/11, but the Patriot act expanded what they could legally be used for and, in the case of CARNIVORE, brought their existence into the light. Whitaker also discusses how court orders related to foreign surveillance under the so-called Foreign Intelligence Surveillance Act were now easier to obtain:

. Originally, a FISA surveillance order required certification that 'the purpose for the surveillance is to obtain foreign intelligence information.'...After 9/11, the Justice Department sought to amend FISA to read simply that 'a purpose' was to obtain foreign intelligence. Congress balked at this very low threshold, but instead provided in section 218 that foreign intelligence gathering be a 'significant purpose' to trigger a FISA surveillance or search order...The Patriot Act widens FISA's powers. It permits 'roving surveillance,' that is, orders that are not tied to a particular place or particular means of communication....The Act extends FISA to cover e-mail as well as telephone communication. It extends the duration of surveillance and physical search orders, in some case providing extensions of up to a year.⁴⁷⁶

⁴⁷⁵ Whitaker, "A Faustian Bargain? America and the Dream of Total Information Awareness," 148.

⁴⁷⁶ Whitaker, 143.

Interestingly, between its enactment and the Snowden revelations in 2013, the widened authorities granted under the Patriot act did not seem to have resulted in much activity based on information collected from social media federal law enforcement – at least not within the U.S. In cases where American citizens or permanent residents were targeted by law enforcement under the Patriot act’s widened authority, any electronic information collected came from other sources. In one of the more publicized cases, Brandon Mayfield, an attorney who has represented people of the Muslim faith and is himself a Muslim, was held for two weeks under suspicion of being behind the 2004 bomb attack in Madrid, Spain. This was based on an erroneous exchange of fingerprint information between the FBI and Spanish police.⁴⁷⁷ In a similar situation, writer Lawrence Wright was visited at home by FBI agents asking him about some calls he had made to Egypt. Wright had not been talking to just anyone, his conversations were with a relative of Ayman al-Zawahiri, Osama Bin Laden’s deputy. Wright had written a profile on al-Zawahiri in *The New Yorker*, and it was in this connection he was speaking to the relative. However, this case was not even an example of telephone wiretapping or the like. Wright had spoken to the FBI about al-Zawahiri for the story and had been given a piece of misinformation that he would later unwillingly pass on to the relative, who was already being surveilled. When the misinformation showed up in other communications made by the relative, the FBI knew Wright had been in contact with him. Later calls were then monitored as it was made possible under the Patriot act, and Wright got a visit from the FBI inquiring about those calls.⁴⁷⁸

⁴⁷⁷ Whitaker, 149–50.

⁴⁷⁸ FBI National Press Office, “FBI — Statement on Brandon Mayfield Case,” FBI National Press Releases, 2004, <https://archives.fbi.gov/archives/news/pressrel/press-releases/statement-on-brandon-mayfield-case>.

A 16-year old teenager from North Carolina, Ashton Lundeby, was arrested by local police officers and armed FBI agents. According to the Lundeby's mother, there were 12 agents and officers present to arrest the boy for making bomb threats. His mother initially didn't understand what was going on⁴⁷⁹, but as it turned out, Ashton Lundeby had been building up a secret persona, 'Tyrone', and had engaged with a prank-calling community from the discussion site 4Chan. As Tyrone, he had initiated VoIP conference calls, where up to 300 users would listen to Lundeby make prank calls that have been described as "crude and racist". Listeners would donate to Lundeby through PayPal. After the prank calls began to include bomb threats between mid-2008 and March 2009, law enforcement stepped in. Lundeby pleaded guilty and was sentenced to serve the 22 months he had already been held in custody since his arrest.⁴⁸⁰ The Lundeby case is an example of how the provisions of the Patriot act could be used to gather information on sites that resemble social media, but 4Chan does not conform to Boyd and Ellison's definition, and neither does a VoIP service. Yet, the Lundeby case is likely the closest thing to a case based on social media surveillance made possible by the Patriot act. While these examples all show how the Patriot act facilitated violations of privacy rights, they do not show that this happened as the result of social media monitoring. Until the Snowden revelations of

⁴⁷⁹ David K Shipler, *The Rights of the People: How Our Search for Safety Invades Our Liberties*. (New York: Alfred E. Knopf, n.d.), <http://pearl.stkate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=llf&AN=58150779&site=ehost-live>.

⁴⁸⁰ Staff, "Mom Says Patriot Act Stripped Son of Due Process," WRAL.Com, 2009, <http://www.wral.com/news/local/story/5049867/>; Kevin Poulsen, "Teen Bomb Hoaxer 'Tyrone' Sentenced to 22 Months Time-Served," Wired, 2011, <https://www.wired.com/2011/01/tyrone/>.

2013, monitoring of social media based on provisions in the Patriot act did not seem to have a broad impact on Americans.

Snowden

When the Snowden leaks did emerge, however, it finally came to the attention of the American population that the intelligence community was monitoring electronic communications of American citizens, including on social media.⁴⁸¹ The revelations were seen as “Completely crucial in revealing the sorts of programs that had gone almost without question in the security state, and in causing them to be questioned.” according to Margo Schlanger, whom I interviewed as part of this study. Schlanger is a law professor at University of Michigan, founder and director at the Civil Rights Litigation Clearinghouse and served as Officer for Civil Rights and Civil Liberties at the DHS from 2010-2012, appointed by president Obama.⁴⁸²

More importantly, the Snowden affair revealed that the U.S. intelligence services were able to circumvent some of the strict boundaries that were drawn between them. Henrik Moltke is a New York-based investigative journalist and filmmaker who works for ProPublica but has also co-authored front page articles in The New York Times and has worked for the Intercept. His work with documentary filmmaker Laura Poitras, including on the Academy Award-winning documentary about Edward Snowden, *Citizen Four*, has granted him access to the collection of documents that Snowden illegally acquired from his employer, NSA contractor Booz Allen

⁴⁸¹ Shipler, *The Rights of the People: How Our Search for Safety Invades Our Liberties*.

⁴⁸² Macaskill and Dance, “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained | US News | Theguardian.Com.”

Hamilton. Moltke is one of only a handful of people who has even seen this archive, much less had regular access to it, and has based most of his reporting in recent years on information from and analysis of these documents. He explains that one of the main reasons why the Snowden revelations were important was that they showed how competently, U.S. intelligence agencies were able to adapt to new technical situations:

There was a big change when the social communication platforms, with Yahoo! leading the charge, changed over to using the [more secure] HTTPS protocol around 2007. The sensors that the intelligence community had set up at gateways all over the world couldn't just pick up online conversations anymore. Previously, particularly due to the Reagan-era Executive Order 12333, you could do whatever you want on foreign soil, as long as you were dealing with bad guys. All [U.S. foreign intelligence agencies] had to do to monitor someone in the Middle East was to start "listening" to a sensor close by. There were no legal hassles. After the introduction of HTTPS, these chats were now encrypted, so all that came back from the sensor was gibberish. You would need the encryption keys. This is how the PRISM system, which Snowden revealed, came into being. None of us are still quite sure how it works, but I personally believe the FBI helps the NSA monitor, for example, Facebook traffic that comes in and out of the U.S. by getting warrants for specific, unique Facebook IDs. This ID is then sent to Facebook who redirects that user's traffic through a server that the NSA has access to. What comes out of that is the unencrypted HTML or XML or whatever is being used. The transcriptions with the collected chats have a header that includes the warrant number and when and where the collection happened. And then the chat follows in a readable format. But what we've seen

in the archive are not conversations between you and your hair stylist. They are mostly relevant conversations between people that are relevant to fighting terror. As an example, Al-Qaeda used Yahoo! chat for a while, and in the transcripts of those conversations, you'll see the user names, but if one of the participants in the conversation is a U.S. person, that user name is redacted, and the same goes for references in the conversation to U.S. persons, including corporations. There are analysts and AI systems whose job it is to filter out those instances in the transcripts.⁴⁸³

Moltke is quick to point out that he hasn't seen anything in the Snowden documents that point to a policy of inappropriately crossing the boundaries between foreign and domestic intelligence collection:

The NSA exists to do foreign intelligence and after having studied the Snowden archive for a long time, it is my impression that they place a lot of emphasis on sticking to that interest. The NSA training manuals, the way they train their employees, their internal communication and ethical standards all indicate that they are quite rigorous in that practice. For example, if a U.S. person enters a conversation being monitored by an analyst, the analyst must stop immediately and report what just happened. There are a few exceptions, such as imminent danger or preventing acts of terror. But generally, even if the foreign intelligence collection activities at the e.g. the NSA yield information about a U.S. person, there are now both systems and laws in place that prohibit the NSA from using that

⁴⁸³ Henrik Moltke, "Interview, 3/29/2018," 2018.

information. We've seen some very, almost laughably, detailed examples, such as photos of people having a conversation where one of them is totally blacked out.⁴⁸⁴

After the Snowden affair, the U.S. population now became more aware of what had been happening. A Pew Research study conducted in 2015 showed that 31% of respondents said that they had heard “a lot” about the government surveillance programs, where another 56% said they had heard “a little”. Yet, the awareness of government surveillance brought on by the Snowden affair did not seem to have a substantial impact on the attitudes and behaviors of Americans. Out of those 87%, 17% said they had changed their privacy settings on social media, 15% said they used social media less often. 13% said they have avoided using certain terms in online communications. These users were primarily found in the group that said they had heard “a lot” about the NSA initiatives and skewed younger.⁴⁸⁵ In other words, even after two years of media coverage of the Snowden leaks and an Oscar-winning documentary on the subject, the perception of an infringement of privacy rights on social media by the government was not strong enough to change the behavior of a significant majority of the respondents. After several reauthorizations and extensions, The USA PATRIOT act was retired in 2015 and replaced by the USA FREEDOM act, which I will detail further below.

⁴⁸⁴ Moltke.

⁴⁸⁵ Margo Schlanger, “Interview, March 15 2018,” 2018.

The Homeland Security Act

The USA PATRIOT act was not the only legislative response to the 9/11 attacks. A much larger initiative was the establishment the Homeland Security Act of 2002. Whereas the Patriot act was enacted very briefly after the attacks, this law didn't take effect until more than a year later, on November 25, 2002. This was due to scale of the law and its reorganization of federal departments and agencies, the largest since 1947. The law consolidated a number of functions and institutions under the Department of Homeland Security (DHS), and such a large reorganization takes time. To get some of the capabilities of the future department into effect quickly after the 9/11 attacks, then-President George W. Bush established the Office of Homeland Security as an office in the executive branch, which could be done without Congress' approval.

The first office director, who also transitioned into the position of director of the DHS upon its establishment, Tom Ridge, started the job on October 8, 2001, less than a month after the attacks. In June 2002, a formal bill to establish the DHS was proposed. As mentioned above, the bill was passed into law in November of that year, integrating 22 federal departments and agency into the DHS. These included the Immigration and Naturalization Service, that had otherwise been placed in the Department of Justice but was now split up into three sub-agencies under the DHS with separate functions. The U.S. Customs and Border Patrol (CBP) would be in charge of immigration issues and law enforcement at the nation's borders, the U.S. Immigration and Customs Enforcement (ICE) would perform law enforcement functions within the nation's borders related to foreign nationals and imports from foreign countries, and finally, the U.S.

Citizenship and Immigration Services (USCIS) would be the administrative function of the DHS with regard to visa issuance, immigration and permanent residency as well as naturalization.⁴⁸⁶ The U.S. Secret Service, the U.S. Coast Guard the Transportation Security Authority (TSA) and the Federal Emergency Management Agency (FEMA) were also now organized under the DHS, as was – relevant to this chapter – the former National Communication System office under the Dept. of Defense (DoD) and the Federal Computer Incident Response Center, formerly under the General Services Administration. They became the Office of Cybersecurity and Communications and US-CERT, respectively. Originally, three new directorates were established along with the DHS: The Border and Transportation Security, Emergency Preparedness and Response and Information Analysis and Infrastructure Protection directorates, but a 2005 reorganization of the department abolished all three, with their functions being moved to the institutions mentioned above.⁴⁸⁷

The DHS as national cybersecurity hub

Over the years, post-reorganization, the DHS became a central hub for security operations in the domestic information space. Where cyberattacks by foreign nations were still mainly the responsibility of the DoD and cybercrime was dealt with by the FBI, the DHS became the main home for agencies tasked with national cybersecurity matters.

⁴⁸⁶ Lee Rainie and Mary Madden, “Americans’ Privacy Strategies Post-Snowden,” Pewinternet.org, 2015, <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>.

⁴⁸⁷ Department of Homeland Security, “History | Homeland Security,” DHS.gov, accessed March 12, 2018, <https://www.dhs.gov/history>.

Throughout its history, the DHS has put several initiatives in place to achieve this goal. Many of the initiatives were or are still classified. The first report to Congress from the DHS Privacy Office (that oversees privacy regulation compliance in projects within the DHS' agencies and sub-departments) confirmed the existence of several, domestic data mining initiatives but did not divulge many details about them. In the first 2006 report, the office listed a number of DHS initiatives using data mining, but it is important to note how the DHS defined "data mining" in the report:

Data mining involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. Data mining consists of more than collecting and managing data; it also includes analysis and prediction... Thus, this report would exclude searches using patterns, relationships, and rules focused on a particular individual, such as used in a threat and risk assessment vetting program.⁴⁸⁸

In other words, the list in the 2006 report was by no means exhaustive, with data collection on individuals almost certainly taking place in initiatives not disclosed by the Privacy Office. Some of the listed initiatives used data sources maintained by other DHS agencies or other federal agencies under specific agreements. However, the report does include descriptions of DHS projects that collect data from private information resources and acquire data from commercial vendors.

⁴⁸⁸ DHS.gov, "Who Joined DHS | Homeland Security," DHS.gov, accessed March 12, 2018, <https://www.dhs.gov/who-joined-dhs>.

One project under development in 2006 was Intelligence and Information Fusion (I2F) under the Office of Intelligence and Analysis, which in the report was stated as developing a system that was anticipated to “incorporate data from both government and commercial sources.”⁴⁸⁹ I shall return to the I2F project later. Another initiative, Fraud Detection and National Security Data System (FDNS-DS) under USCIS, was described as primarily using CLAIMS (the central database for visa, permanent residency and naturalization applications) as its data source, but it was “...expected that case specific data from commercial data aggregators will be stored in future releases of FDNS-DS.”⁴⁹⁰ The report listed a similar description of the data practices at the National Immigration Information Sharing Office (NIISO). Furthermore, at least one project was described as monitoring and scraping data from the web:

The NETLEADS project is a tool suite designed to provide a means of performing more efficient searches on a combination of structured data, such as Oracle, Microsoft and mainframe databases, and unstructured data, such as textual reports, open source documentation, Web pages, Reports of Investigation narratives from ICE databases, and images such as PDF files.⁴⁹¹

⁴⁸⁹ Maureen Cooney, “Data Mining Report DHS Privacy Office Response to House Report 108-774 Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties Respectfully Submitted,” 2006, 8, https://www.dhs.gov/sites/default/files/publications/privacy_data_mining_report_0.pdf.

⁴⁹⁰ Cooney, 26.

⁴⁹¹ Cooney, 27.

It is clear then, that the DHS had the capability to scrape web content for analysis in 2006 and had implemented it as a practice. It is impossible to know (at least without a high-level security clearance) to which extent this would include monitoring of publicly-accessible social media activities (which would not require a warrant under the Patriot act), but since MySpace, which used publicly-accessible personal profiles at the time, had reached more than 100mn users in 2006, it is at least likely that some DHS scraping would have occurred there.⁴⁹² Also, the reliance on private data vendors would also makes it likely that social media data would find their way into these government databases, as data brokers and other third-party vendors were already purchasing and generating data from social media platforms at the time⁴⁹³

From mapping social networks to targeting users

By 2007, social media platforms were definitely recognized by federal agencies as resources for collecting data about individuals. For example, some agencies began training investigators in data and information collection through social media, as in the case of SEARCH Training Services under the Department of Justice. This service center issued at least two manuals in 2007 on how to gather information about individuals and map their connection on MySpace.⁴⁹⁴ As a leading social media platform at the time, MySpace, along with several other

⁴⁹² Cooney, 25.

⁴⁹³ Pete Cashmore, "MySpace Hits 100 Million Accounts," Mashable, 2006, <https://mashable.com/2006/08/09/myspace-hits-100-million-accounts/#vRglqLpSS5qj>; Katherine Q. Seelye, "Microsoft to Provide and Sell Ads on Facebook, the Web Site," The New York Times, 2006, <http://www.nytimes.com/2006/08/23/technology/23soft.html>.

⁴⁹⁴ Harvey Jones and Hiram Soltren, "Facebook: Threats to Privacy," 2005, <https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>; Lauren Wagner,

platforms, had already established relationships with law enforcement, issuing guidance documents on how to proceed with requests for information about users as early as 2005.⁴⁹⁵

It was also in 2007 that advocacy groups such as the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF) increased their focus on DHS activities with regards to social media. EPIC criticized the DHS' plans to create a federal network of state and local "fusion centers" that were a result of the above-mentioned I2F initiative and expand their range of data sources into the private sector. Fusion centers, according to EPIC, are mechanisms "to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources"⁴⁹⁶

Over the next few years, the DHS increased their activities within monitoring and gathering information from social media. A 2011 media monitoring manual for DHS analysts states that "Leveraging news stories, media reports and postings on social media sites concerning Homeland Security, Emergency Management, and National Health for operationally relevant data, information, analysis, and imagery is the first mission component", because "Social Media outlets provide instant feedback and alert capabilities to rapidly changing or newly occurring

"MySpace Friend Mapper Article," *SEARCH Training Services*, 2007, <https://www.eff.org/document/doj-social-network-foia-myspace-friend-mapper-article>.

⁴⁹⁵ Lauren Wagner, "How to Search MySpace," *SEARCH Training Services*, 2007, <https://www.eff.org/document/2007-article-how-search-myspace>.

⁴⁹⁶ MySpace.com, "MySpace 2005 Law Enforcement Guide" (EFF.org, 2005), <https://www.eff.org/document/myspace-2005-guide>; EPIC, "'National Network' of Fusion Centers Raises Specter of COINTELPRO," *Spotlight on Surveillance*, 2007, <https://epic.org/privacy/surveillance/spotlight/0607/>.

situations. ⁴⁹⁷ Initially, the media monitoring analysts at the DHS were prohibited from collecting or distributing/forwarding personal identifiable information (PII), with the only exception being extreme situations where e.g. loss of life was imminent. However, in January 2011, the DHS was granted further permissions with regard to PII. According to the manual, DHS analysts could now collect and disseminate PII for “certain narrowly tailored categories” which the manual does not specify. In addition, PII could be collected “when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners” about any public figures among U.S. and foreign officials in both the government and private sectors, reporters who use “traditional and/or social media in real time”, public officials who are victims of Homeland Security-related incidents, and finally, anyone who “may be involved in major crimes of Homeland Security interest...who are killed or found dead”⁴⁹⁸

In other words, with these deregulations, the DHS now gained the ability to register public social media statements by journalists and dead criminals. As we shall see later in this chapter, the former may impede freedom of speech. The latter may implicate third parties unreasonably. These deregulations led to further changes over the next year, which would become the basis of the policy analyzed here. These changes were described by the EFF thus:

At least as early as 2012, DHS began monitoring social media for more targeted “operational uses” that involve specific individuals... For example, DHS scrutinizes

⁴⁹⁷ EPIC, “‘National Network’ of Fusion Centers Raises Specter of COINTELPRO.”

⁴⁹⁸ Department of Homeland Security, “DHS Media Monitoring Desktop Reference Manual | Public Intelligence,” Public Intelligence, 2012, 4, <https://publicintelligence.net/dhs-media-monitoring-desktop-reference-manual/>.

public posts when “investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, [or] making a personnel determination about a Department employee.” This 2012 policy permits DHS to collect social media information about those seeking U.S. immigration status,⁴⁹⁹

The next big steps in this evolution after the 2012 policy enactment was Obama’s increase of the spending on cybersecurity. The increase in social media monitoring at the DHS came as a consequence of the Comprehensive National Cybersecurity Initiative (CNCI), established by George W. Bush in the last year of his presidency. President Obama expanded the initiative and strengthened the partnerships between the private and public sectors. Obama would further increase spending on cybersecurity measures (which, in this case, includes intelligence gathering via social media) during his presidency, including in 2016, when The White House presented the National Cybersecurity Action Plan, which further strengthened DHS’ role in cyber activities⁵⁰⁰

The National Cybersecurity Action Plan was a reaction to several events. As mentioned in the chapter on Russia, in 2015 American media began reporting on Russian troll activity on social media more than occasionally, and researchers and analysts had already actively pointed to

⁴⁹⁹ Department of Homeland Security, 25.

⁵⁰⁰ The White House, “FACT SHEET: Cybersecurity National Action Plan | Whitehouse.Gov,” obamawhitehouse.archives.org, 2016, <https://obamawhitehouse.archives.org/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

insufficiencies in the social media strategies of both the DoD and the DHS.⁵⁰¹ Perhaps more importantly, the San Bernardino terrorist attack in December 2015 created an attitudinal shift with regard to social media monitoring. The attack resulted in bipartisan demands from Congress to loosen the restrictions on social media monitoring and intelligence-gathering.

This was a general change of direction from only few years earlier, when the Snowden revelations caused a national debate and a series of public investigations, which led to a tightening of many of the regulations and oversight structures that had been relaxed under the Patriot and Homeland Security acts following the 9/11 attacks. For a few years, lawmakers worked to restrict government surveillance, and sunset provisions in the Patriot act meant that the law was not renewed as planned in 2015, but rather replaced with the USA FREEDOM act, which to some seemed like a restoration of privacy rights for Americans⁵⁰², and to others, the changes seemed small and ineffective.⁵⁰³

The San Bernardino attacks seemed to swing the pendulum back towards the post-9/11 atmosphere. As an example, Senator Jeanne Shaheen (D – NH) lead a group of a total of 25 Democratic senators who signed a letter to Secretary of Homeland Security Jeh Johnson voicing their concern about the DHS’ apparently insufficient social media surveillance. In a press

⁵⁰¹ Sophia Cope and Adam Schwartz, “DHS Should Stop the Social Media Surveillance of Immigrants | Electronic Frontier Foundation,” EFF.org, 2017, <https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants>; Nissen, *The Weaponization of Social Media: Characteristics of Contemporary Conflicts*.

⁵⁰² Morten Bay and Isaac R. Porsche III, “West Can’t Ignore Islamic State Social Media War | World Report | US News,” U.S. News and World Report, 2015, <https://www.usnews.com/opinion/blogs/world-report/2015/07/23/west-cant-ignore-islamic-state-social-media-war>.

⁵⁰³ Bart Forsyth, “Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection,” *Washington and Lee Law Review* 72 (2015), <http://heinonline.org/HOL/Page?handle=hein.journals/waslee72&id=1349&div=31&collection=journals>.

release, Shaheen said: “ISIS and other radical terrorist organizations are using social media as one of their primary channels for inspiring hate and coordinating attacks...the recent attack in San Bernardino underscores the vigilance that’s needed when determining whether to approve visa applications. A review of applicants’ social media activity should be at the very top of the checklist for DHS personnel.” Shaheen’s letter is indicative of a bipartisan concern on the issue. From the other side of the aisle, Senator Ted Cruz (R – TX) also wrote to Secretary Johnson only a few weeks later voicing similar concerns: “Given the rise and proliferation of social media, and younger generations’ increasing reliance on these media, DHS cannot afford to have policies that are blind to information made available on social media and the Internet.”⁵⁰⁴

Social media monitoring without electronic surveillance

The development of the U.S. government’s monitoring of electronic communications from ECHELON to the current policies is characterized by increased monitoring and data collection by more agencies across more sources and interfaces. Collection and privacy breaches can now happen in a multitude of places compared to ECHELON, where mostly e-mail, fax and telephone communication was monitored. Now, breaching electronic privacy rights doesn’t have to happen electronically, as the dual policy of border searches and social media profile registration of naturalized citizens shows. As the number of places this type of monitoring and collection has grown, so has the need for explaining the policy, and as I will now show, the arguments have shifted towards paternalism of the sort described in the previous chapter on China. The

⁵⁰⁴ Sergio Suarez, “Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and NSA Have, Can, and Should Be Doing,” 2017, http://scholarship.shu.edu/student_scholarship.

construction of a Rhetorical Frame for the dual policy under analysis will be followed by a construction of an Action Frame and an exploration of the cultural background upon which these policies appear, i.e. how they fit into the American ideal of individualism, and by extension, the right to privacy.

Rhetorical Frame

The rhetoric surrounding the dual policy analyzed here constitutes a Rhetorical Frame that shows a growing tendency towards paternalism in the arguments supporting privacy breaches as policy. As examples of the arguments for such policies, I will now review a statement specific to the policy of border searches of electronic devices from the acting general counsel of the DHS, followed by a review of the Trump administration's national security strategy, which sets out to provide the strategic justification for the dual policy.

Border searches as paternalism: DHS defense of border searches of electronic devices

After the first news reports emerged in March 2017 indicating a rise in the number of searches of electronic devices at the border (more on this below), acting general counsel for the Department of Homeland Security, Joseph B. Maher wrote an op-ed in USA Today defending the policy. Maher equated the search of electronic devices with other searches that seemingly have been less prone to controversy:

Just as Customs is charged with inspecting luggage, vehicles and cargo containers upon arrival to the USA, there are circumstances in this digital age when we must inspect an electronic device for violations of the law. These electronic media searches have produced information used to combat terrorism, violations of export controls, and

convictions for child pornography, intellectual property rights violations and visa fraud. This authority is critical to our mission, and Customs exercises it judiciously. Electronic searches affect less than one-hundredth of 1% of all arriving travelers.

Maher points to the Supreme Court’s determination that the government’s interest is at its “zenith” at the border, when it comes to blocking unwanted persons or effects from entering the country. He also claims that the CBP “exercises this authority judiciously”, and that

Customs has proactively developed a disciplined policy with proper oversight for searches of electronic devices. We made this policy available to the public in 2009. Courts have reviewed it. A federal court in Brooklyn, for example, concluded that Customs is “sensitive to the privacy and confidentiality issues posed by border searches of electronic devices.” No court has concluded that such searches require a warrant, and our use of this authority has been repeatedly upheld. This includes a review by the 4th and 9th Circuit Courts of Appeals, which approved the search of laptops at the border. Our policy has been subject to ongoing review by our offices of Privacy and Civil Rights and Civil Liberties, and it reaffirms our commitment to protecting individuals’ rights while ensuring that officers can lawfully take the necessary actions to secure our borders and protect the American people.⁵⁰⁵

⁵⁰⁵ Ted Cruz, “Letter to Secretary Johnson” (U.S. Senate, 2016), https://www.cruz.senate.gov/files/documents/Letters/20160122_TerrorismLetterUSCISFDNSSocialMediaUsage.pdf

It should be noted that a shorter, yet somewhat similar statement was made to at least one journalist with regard to the registration of social media information of naturalized U.S. citizens and lawful, permanent residents, a description of which is provided in Action Frame section rather than in this section, since it helps shed light on the concrete policy steps taken.

The National Security Strategy: Paternalism through purposefully vague language

On December 18, 2017, President Trump presented his administration's new national security strategy document at the Ronald Reagan Building and International Trade Center in Washington D.C. As part of his remarks given at this occasion, the president presented the motivation behind the strategy and outlined its contents, including the following lines about matters relevant to this chapter:

In addition, our strategy calls for us to confront, discredit, and defeat radical Islamic terrorism and ideology and to prevent it from spreading into the United States. And we will develop new ways to counter those who use new domains, such as cyber and social media, to attack our nation or threaten our society...This strategy includes plans to counter modern threats, such as cyber and electromagnetic attacks. It recognizes space as a competitive domain and calls for multi-layered missile defense. (Applause.) This strategy outlines important steps to address new forms of conflict such as economic and political aggression.⁵⁰⁶

⁵⁰⁶ Joseph B Maher, "DHS: Device Searches Improve Safety," USA Today, 2017, <https://www.usatoday.com/story/opinion/2017/03/27/dhs-device-searches-improve-safety-editorials-debates/99697022/>.

The strategy document itself reveals a national security strategy resting on four pillars:

- I. Protect the American People, the Homeland and the American Way of Life
- II. Promote American Prosperity
- III. Preserve Peace through Strength
- IV. Advance American Influence⁵⁰⁷

The relevant topics for this chapter are covered in a few places in the strategy, which I will examine below. Under Pillar I, the national security strategy introduces the broad need to “Secure U.S. Borders and Territory” overall with this passage:

State and non-state actors place the safety of the American people and the Nation’s economic vitality at risk by exploiting vulnerabilities across the land, air, maritime, space, and cyberspace domains. Adversaries constantly evolve their methods to threaten the United States and our citizens. We must be agile and adaptable.⁵⁰⁸

Cyberspace is thus considered a central to future conflict from the very beginning, as are “vulnerabilities” exploited by both “State and non-state actors”. This is a continuation of the doctrines put in place by the Obama and Bush administrations, in which a significant shift

⁵⁰⁷ Matthew Kahn, “Document: December 2017 National Security Strategy and Transcript of Remarks - Lawfare,” Lawfare, 2017, <https://www.lawfareblog.com/document-december-2017-national-security-strategy-and-transcript-remarks>.

⁵⁰⁸ The White House, “National Security Strategy of the United States of America,” 2017, V–VI, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

occurred from what could be called traditional warfare to a concept of warfare that includes non-state actors and less kinetic means.⁵⁰⁹

In the strategy, it is also considered a national security priority to “Strengthen Border Control and Immigration Policy”. Here, the administration’s concept of “enhanced vetting” comes into play:

The United States will continue to welcome lawful immigrants who do not pose a security threat and whose entry is consistent with the national interest, while at the same time enhancing the screening and vetting of travelers, closing dangerous loopholes, revising outdated laws, and eliminating easily exploited vulnerabilities. We will also reform our current immigration system, which, contrary to our national interest and national security, allows for randomized entry and extended-family chain migration.

This passage, as well as preceding parts of the text, seems to make the assumption that there are persons wishing to enter the U.S. with the purpose of staying permanently who simultaneously have the intention of disrupting national security. The strategy does not, however, propose any concrete actions to alleviate the assumed threat, other than what president Trump had already promised on the campaign trail, i.e. building a wall along the southern border of the U.S. and implementing the above-mentioned enhanced vetting procedures. In the section where such proposals would be expected to appear, a very general, unspecific approach is taken. Besides

⁵⁰⁹ The White House, 8.

measures that are already in place such as the actual enforcement of immigration laws, the “Priority Actions” section proposes:

We will secure our borders through the construction of a border wall, the use of multilayered defenses and advanced technology, the employment of additional personnel, and other measures...The U.S. Government will enhance vetting of prospective immigrants, refugees, and other foreign visitors to identify individuals who might pose a risk to national security or public safety. We will set higher security standards to ensure that we keep dangerous people out of the United States and enhance our information collection and analysis to identify those who may already be within our borders...We will improve information sharing across our government and with foreign partners to enhance the security of the pathways through which people and goods enter the country. We will invest in technology to counter emerging threats to our aviation, surface, and maritime transportation sectors.⁵¹⁰

These proposals are most likely intentionally vague, so that departments and agencies further down in the administration hierarchy have more room to create fitting policies. The dual policy analyzed in this chapter, in which private social media information is examined by immigration officials, can be viewed as fitting within the priority action passage above. This is a good example of why Schön and Rein’s method requires viewing Rhetorical Frames as different from Action Frames.

⁵¹⁰ Reese Nguyen, “Navigating Jus Ad Bellum in the Age of Cyber Warfare,” *California Law Review*, 2013.

Even though it was the conclusion of multiple law enforcement and intelligence entities that the San Bernardino attackers were mostly radicalized through contacts made on social media and their related messaging services⁵¹¹, the national security strategy does not address the cyber domain directly as a space where de-radicalization actions need to be taken. Rather it states about “jihadist terrorists” that they “rely on encrypted communication and the dark web to evade detection as they plot, recruit, finance, and execute their operations” and “use virtual and physical networks” in their radicalization efforts. Under “Priority Actions”, the strategy states that the U.S. will “go after their digital networks and work with private industry to confront the challenge of terrorists and criminals “going dark and using secure platforms to evade detection”, and “degrade their ability to message and attract potential recruits”⁵¹² which seems to hint at some kind of monitoring of messaging systems online, including those associated with social media. But in the de-radicalization section, it merely states that

We will deny violent ideologies the space to take root by improving trust among law enforcement, the private sector, and American citizens. U.S. intelligence and homeland security experts will work with law enforcement and civic leaders on terrorism

⁵¹¹ The White House, “National Security Strategy of the United States of America”; Mario Anzuoni, “Report: San Bernardino Shooter Made Social Media Contact with Extremists,” Newsweek, 2015, <http://www.newsweek.com/report-san-bernardino-shooter-made-social-media-contact-extremists-400708>.

⁵¹² Matt Hamilton, “Families of San Bernardino Attack Victims Accuse Facebook, Google and Twitter of Aiding Terrorism in Lawsuit,” Los Angeles Times, 2017, <http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-tech-lawsuit-20170503-story.html>.

prevention and provide accurate and actionable information about radicalization in their communities.⁵¹³

The national security strategy contains a specific section on cyberspace, “Keep America Safe in the Cyber Era”, in which the administration defines cyberspace in very broad strokes:

...cyberspace offers state and non-state actors the ability to wage campaigns against American political, economic, and security interests without ever physically crossing our borders. Cyberattacks offer adversaries low-cost and deniable opportunities to seriously damage or disrupt critical infrastructure, cripple American businesses, weaken our Federal networks, and attack the tools and devices that Americans use every day to communicate and conduct business.⁵¹⁴

The administration’s view on how to counteract undesirable cyberactivities is equally broad, but carries a very clear ideological stance, continuing the Obama administration’s policy of public-private cooperation, but also stating emphatically that government role in enforcing the rule of law must be “limited”:

The government and private sector must design systems that incorporate prevention, protection, and resiliency from the start, not as an afterthought. We must do so in a way

⁵¹³ The White House, “National Security Strategy of the United States of America,” 11.

⁵¹⁴ The White House, 11.

that respects free markets, private competition, and the limited but important role of government in enforcing the rule of law.⁵¹⁵

The “Priority Actions” in this section also mainly state objectives that are already in place and have been for a number of years. Among the more specific actions it proposes is defining six key areas where risk must be assessed: “national security, energy and power, banking and finance, health and safety, communications, and transportation”⁵¹⁶, all of which are part of what is normally considered critical infrastructure in the cyber domain, but it is notable that the administration defines the scope of their actions so concretely within these six areas.

Also notable is the administration’s decision to adopt a strategy of deterrence in the cyber domain:

The United States will impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyber activities. We will work with allies and friends to expand our awareness of malicious activities. A stronger and more resilient critical infrastructure will strengthen deterrence by creating doubt in our adversaries that they can achieve their objectives.

It should be mentioned that in spite of this stated strategy, the administration has been criticized for its reluctance towards imposing further sanctions on Russia, even though the intelligence

⁵¹⁵ The White House, 12.

⁵¹⁶ The White House, 13.

community's assessment is that Russia has carried out several cyberattacks on the U.S., including the ones described in chapter 3, and although several Russians have been indicted by the FBI for the same reason. Sanctions that were criticized for being "largely symbolic" were finally imposed in March 2018.⁵¹⁷ Additionally, although several cyberattacks on the U.S. have been attributed to North Korea, a deterrence strategy has not been implemented against that nation either⁵¹⁸, and instead, a strategy that has been criticized for being too forthcoming is in place..^{519##}

The strategy is also vague when it comes to data collection and respecting citizens' rights. In the paragraph "Improve Information Sharing and Sensing", the administration aims to expand the collaboration on information sharing with the public sector without compromising the privacy of individuals:

We will also invest in capabilities that improve the ability of the United States to attribute cyberattacks. In accordance with the protection of civil liberties and privacy, the U.S. Government will expand collaboration with the private sector so that we can better detect and attribute attacks.⁵²⁰

⁵¹⁷ The White House, 13.

⁵¹⁸ Gregory Korte, "U.S. Sanctions on Russia Remain Largely Symbolic," USA Today, 2018, <https://www.usatoday.com/story/news/politics/2018/03/15/trump-sanctions-russia-following-poisoning-british-spy/427464002/>.

⁵¹⁹ Alex Hern, "North Korea Is a Bigger Cyber-Attack Threat than Russia, Says Expert," The Guardian, 2018, <https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia>.

⁵²⁰ Kara Scannell, David Shortell, and Veronica Stracqualursi, "Mueller Indicts 13 Russian Nationals over 2016 Election Interference," CNN, 2018, <https://www.cnn.com/2018/02/16/politics/mueller-russia-indictments-election-interference/index.html>; Steve Chapman, "Trump, the Wimp - Chicago Tribune," Chicago Tribune, 2018,

In Pillar III, “Preserve Peace Through Strength”, another strategy related to cyberspace can be found, this time more focused on national defense. A section named “Renew Capabilities” contains a list of defense areas, such as “Military”, “Defense Industrial Base”, “Nuclear Forces”, “Space”, “Intelligence” and “Cyberspace”. The latter mostly repeats the threat assessment mentioned above, but it does have some small, significant differences. For one, it addresses the problem of attribution by stating that cyberattacks have “a troubling degree of deniability” and that cyberattacks can be used for “extortion, information warfare, disinformation, and more” which can “undermine faith and confidence in democratic institutions and the global economic system”. It is indeed interesting to note that in a section focused on defense capabilities in cyberspace, there is almost no mention of the type of critical infrastructure attacks addressed in the broader section from Pillar I described above – or what the strategy proposes to do about them.

Although it is primarily the Department of Defense and USCYBERCOM⁵²¹ who are tasked with taking actions to protect the nation against, e.g. cyberattacks on critical infrastructure, the section covering, among other things, the DoD’s role in cyberspace, is mainly focused on information warfare. Under Priority Actions however, the strategic considerations turn towards critical infrastructure and more technologically-driven cyberattacks, and these considerations, similarly to those mentioned above, pave the way for the policies analyzed here:

<http://www.chicagotribune.com/news/opinion/chapman/ct-perspec-chapman-trump-weak-russia-north-korea-201803186-story.html>.

⁵²¹ The White House, “National Security Strategy of the United States of America,” 13.

We will improve our cyber tools across the spectrum of conflict to protect U.S. Government assets and U.S. critical infrastructure, and to protect the integrity of data and information. U.S. departments and agencies will recruit, train, and retain a workforce capable of operating across this spectrum of activity... We will improve the integration of authorities and procedures across the U.S. Government so that cyber operations against adversaries can be conducted as required. We will work with the Congress to address the challenges that continue to hinder timely intelligence and information sharing, planning and operations, and the development of necessary cyber tools.⁵²²

Finally, under the “Intelligence” section of the national security strategy, further creates a foundation for the type of policies under analysis in this chapter. The administration acknowledges that we live in an “information-dominant era” which puts the intelligence community in a constant state of change and adaption. The administration wishes to give the intelligence community the ability to “Harness all information at our disposal”, but continues to be vague beyond that: “The United States will, in concert with allies and partners, use the information-rich open-source environment to deny the ability of state and non-state actors to attack our citizens, conduct offensive intelligence activities, and degrade America’s democratic institutions.”⁵²³

⁵²² U.S. Strategic Command, “U.S. Cyber Command (USCYBERCOM) Factsheet,” Stratcom.mil, 2016, <http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscycbercom/>.

⁵²³ The White House, “National Security Strategy of the United States of America,” 32.

The vague phrasing of the National Security Strategy is reminiscent of the vague language used in China's new cybersecurity laws and by the public his explanation of it by Xi Jinping (See Chapter 4). It also echoes the Chinese government's paternalism in that it implies that citizens do not need to know how the government protects them, but only need to trust that it will – without asking questions. While unspecific language can ensure operational security and give less information away to adversaries, it can also conflict with the requirements for transparency inherent in any democracy. In the previous chapter, I showed how transparency (or lack thereof) comes into play for Rawls as part of a democratic process, but also how the type of paternalism on display in the rhetoric above goes against Rawlsian principles on a societal level. However, in a Western-style democracy that does not have a Confucian heritage like China's, this type of rhetorical paternalism contradicts the ability of the individual to express itself, which is broadly seen as being at the core of the American liberty ideal, which I will discuss in the Cultural Background section of this chapter. As I will now continue to show, policy actions performed by the Trump administration also come into conflict with this ideal, including the dual policy under analysis in this chapter.

Action Frame

In terms of national security in the cyber domain, the Trump administration have primarily taken action at the macro level, and the actions have been criticized as being somewhat insufficient. In May 2017, President Trump signed a much-delayed executive order (EO) on Cybersecurity, which primarily allocated resources for a modernization of federal IT systems and networks,

including an assessing and resolving security vulnerabilities in it. Specifically, according to the President's homeland security adviser, Tom Bossert, the EO mandates the adoption of the cybersecurity framework developed by NIST for protection of all federal networks, it centralizes federal IT as one enterprise network and reorganizes federal IT to be more reliant on cloud-based services.⁵²⁴ The EO contains requests for a number of reviews to be completed within a few months of its signing. Among them are a cyber vulnerability review by the DoD, a list of cybersecurity adversaries from the DNI, both to be handed to the president within 90 days. The EO also requests a capability review from the NSA, DoD and DHS, with an added review of cybersecurity education by the latter two departments. The DHS and Department of Commerce are requested to deliver a report on how the private sector can be incentivized to adopt better cybersecurity practices within 120 days, and the American Technology Council, together with the OMB and the GSA are to produce a plan containing concrete steps to modernize the federal IT infrastructure as mentioned above.⁵²⁵

However, after some of these deadlines had passed, The White House was not willing to disclose whether the deadlines had been met, but merely said that "Departments and agencies continue implementing Cybersecurity Executive Order 13800 and have made significant progress"..⁵²⁶ The modernization plan, however, was delivered by the ATC, OMB and GSA on time in September. This report helped inform the Modernizing Government Technology (MGT)

⁵²⁴ The White House, 32.

⁵²⁵ Conner Forrest, "Trump's Cybersecurity Executive Order: 4 Things You Need to Know," TechRepublic, 2017, <https://www.techrepublic.com/article/trumps-cybersecurity-executive-order-4-things-you-need-to-know/>.

⁵²⁶ Forrest.

act, which was then appended to the 2018 National Defense Authorization Act (NDAA), which passed Congress in November and was signed into law on December 13, 2017 by the president. Thus, a modernization effort got underway, but the results of the other reviews requested in the EO have not been made public. In late August, after the deadlines of some of the reviews had passed, the general impression of insufficiency of actions in the cyber domain caused several members of the National Infrastructure Advisory Council, which advises the DHS, resigned. The resignation letter contained this passage: "You have given insufficient attention to the growing threats to the cybersecurity of the critical systems upon which all Americans depend".⁵²⁷

Except for the passage of the MGT act and the rhetorical contributions to the public discourse described above, most of the recent policy action in terms of heightening cybersecurity under the Trump administration has happened at the department or agency level. These actions range from recommendations on cybersecurity policy like those given to private companies by the SEC in February 2018, to full-on implementations of new policies, such as the dual policy on social media information collection analyzed here. To begin the journey towards the analysis of said policies and the actions taken in their implementation, I will first provide the context in which they should be understood.

Modification of the 1974 Privacy Act System of Records

I can now proceed with describing the first of the two related policies I wish to discuss in this chapter. In September 2017, the DHS proposed a modification to the so-called "Department of

⁵²⁷ Lily Hay Newman, "Trump's Cybersecurity Executive Order Gets Off To a Slow Start," Wired, 2017, <https://www.wired.com/story/trump-cybersecurity-executive-order/>.

Homeland Security/U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection—001 Alien File, Index, and National File Tracking System of Records.“ This is the internal record-keeping system the DHS and its immigration-focused agencies USCIS, ICE and CBP use for keeping track of foreign nationals located in the U.S. longer than the three months a regular, tourist-based visa-waiver program allows. These foreign nationals include not just temporary visa holders, but also permanent residents, colloquially known as Green Card holders. In USCIS terms, the latter are “immigrant aliens” as opposed to “non-immigrant aliens”, the latter being those who only have temporary visas and therefore haven’t emigrated to the U.S. permanently. Each immigrant alien is assigned an “A-number” which signifies the number of the “Alien File” in the title of the above-mentioned records system. The file has traditionally contained background information on the individual such as country of origin, citizenship information and any other information that came to light during that person’s application for permanent residency. The changes proposed by the DHS would

...expand the categories of records to include the following: country of nationality; country of residence; the USCIS Online Account Number; social media handles, aliases, associated identifiable information, and search results; and the Department of Justice (DOJ), Executive Office for Immigration Review and Board of Immigration Appeals proceedings information;⁵²⁸

⁵²⁸ Newman.

Notably, “search results” and “associated identifiable information” are not defined further, and it is difficult to know, for example, whether the term “search results” means results obtained by investigators as they conduct a background check as part of the immigration application process, or whether it is search results yielded by a search performed by the applicant that the DHS has obtained somehow. Furthermore, in line with similar integrations of commercial/private datasets in DHS data processes described above, the agency’s proposals would “update record source categories to include publicly available information obtained from the internet, public records, public institutions, interviewees, commercial data providers, and information obtained and disclosed pursuant to information sharing agreements”.⁵²⁹ Again, this allows personal information and data obtained through social media to find its way to government databases by way of a third party.

The proposal was posted in the Federal Register on September 18, 2017, requesting that comments be submitted by October 18. The changes received some press coverage, but this was not particularly agenda-setting.⁵³⁰ In an e-mail to journalist Matt Novak, Joanne F. Talbot from the DHS Office of Public Affairs claimed that this was not a new policy:

This amendment does not represent a new policy. DHS, in its law-enforcement and immigration-process capacity, has and continues to monitor publicly-available social media to protect the homeland. In an effort to be transparent, to comply with existing

⁵²⁹ Department of Homeland Security, “Privacy Act of 1974; System of Records,” Federal Register, 2017, <https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records>.

⁵³⁰ Department of Homeland Security; Adolfo Flores, “People Are Worried About DHS Plans To Gather Social Media Info,” BuzzFeed, 2017, https://www.buzzfeed.com/adolfoflores/people-are-worried-about-dhs-plans-to-gather-social-media?utm_term=.gq0Xgr8Jm#.kxeLdzR2a.

regulations, and due to updates in the electronic immigration system, DHS decided to update its corresponding Privacy Act system of records, DHS published this notice in the Federal Register on Sept. 18 to comply with the administrative requirements of the Privacy Act to help address these requirements, not launch a new policy initiative.⁵³¹

However, it is clear from the amendment text that the A-files have not included this information before. A policy like this one could be considered part of a defensive strategy against foreign attackers at both the individual and group level. But it is clear from the text that visitors to the U.S. are not the primary targets of the changes. The first two “categories of individuals covered by the system” are lawful permanent residents and naturalized U.S. citizen., followed by anyone seeking to benefit from the INA (Immigration and Naturalization Act). Only then does the list mention individuals currently or formerly under investigation by the DHS or those connected to such investigations.⁵³² Notably, spouses, relatives and attorneys for individuals seeking to benefit from INA are *also* covered by the changes, regardless if they have U.S. citizenship by birthright. The amendment went into effect without any major alterations on October 18.⁵³³

Margo Schlanger does not believe that the registration of this information amounts to monitoring and thus, it cannot necessarily be regarded as surveillance:

⁵³¹ Matt Novak, “US Homeland Security Will Start Collecting Social Media Info on All Immigrants October 18th [Updated],” Gizmodo, 2017, <https://gizmodo.com/us-homeland-security-will-start-collecting-social-media-1818777094>.

⁵³² Novak.

⁵³³ Department of Homeland Security, “Privacy Act of 1974; System of Records”; Cope and Schwartz, “DHS Should Stop the Social Media Surveillance of Immigrants | Electronic Frontier Foundation.”

I don't have the impression at all that USCIS is working to monitor naturalized at all. My understanding is that as part of the immigration process they want to do some social media vetting, and then after the vetting process is done and you are naturalized, they don't want to have to go back and purge it. Which is very different thing from saying that they are monitoring naturalized citizens. I don't have any reason at all to think that they are monitoring naturalized citizens. They don't generally purge the A-files of naturalized citizens. If you're a naturalized citizen, your A-file stays around, and it's got a lot of information in there that the government doesn't collect for folks who haven't been through an immigration adjustment.⁵³⁴

CBP Directive Governing Border Searches of Electronic Devices

The second policy to be analyzed in this chapter regards the relatively recent CBP officer practice of searches of electronic devices belonging to individuals entering the United States. The policy has recently been the subject of public controversy and a joint lawsuit filed by the EFF and the ACLU, which has led to a more concrete formalization of the policy, without much change in its effect, as can be seen below.

This policy is closely related to the USCIS policy described above through several links. First, the motivation is the same. The policy can be seen as being part of President Trump's broader strategy of tightening control at the border, which also includes the aforementioned "enhanced vetting", the so-called "travel ban" and the initiative to build a border wall along the

⁵³⁴ Joan Friedland, "DHS Is Collecting Information on Immigrants' and Citizens' Social Media Use and Making It Part of Their Permanent Records," National Immigration Law Center, 2017, <https://www.nilc.org/news/torch/11-30-17/>.

U.S.-Mexico border.⁵³⁵ Trump's travel ban aside, this policy is motivated by the mission to prevent potential terrorists or individuals affiliated with terror organizations from entering the country, which is also part of the motivation for the above-mentioned registration of immigrants' social media information. Second, and notably, the targets are the same. Both the USCIS and the CBP policies target those who plan to stay in the U.S. permanently, are lawful, permanent residents or naturalized citizens. The CBP policy can also be applied against visitors, but since this analysis discusses the rights of those living in the U.S., the most important aspect is that the policy is being used towards citizens and permanent residents too. Third, the two policies are both parts of a larger DHS effort to glean information about individuals from social media and fourth, for that same reason they have emerged roughly at the same time. For these reasons, I analyze them as part of the same policy frame.

In January 2018, the CBP revised its policy on border searches of electronic devices, after several media outlets and advocacy organizations had made it clear to the public that devices such as smartphones were being searched at the nation's borders. Organizations such as the ACLU have pointed to the fact that the number of monthly electronic device searches at the border more than tripled between October 2016 (857 searches) and September 2017 (2,580 searches).⁵³⁶ Esha Bhandari is a staff attorney on the ACLU's Speech, Privacy, and Technology Project and heavily involved in the court cases the ACLU has filed with regard to border

⁵³⁵ Schlanger, "Interview, March 15 2018"; Jeremy Diamond, "Donald Trump: Ban All Muslim Travel to U.S.," CNN.com, 2015, <https://www.cnn.com/2015/12/07/politics/donald-trump-muslim-ban-immigration/index.html>.

⁵³⁶ Scott Bixby and David Agren, "Trump Reveals Plan to Finance Mexico Border Wall with Threat to Cut off Funds," The Guardian, 2016, <https://www.theguardian.com/us-news/2016/apr/05/donald-trump-mexico-border-wall-plan-remittances>.

searches of electronic devices. In an interview conducted for this dissertation she explains that these numbers

...may not include all searches conducted by other agencies, such as ICE, of devices seized at the border. The latest figures are not broken down by citizenship status, but an earlier ACLU FOIA request had yielded information that of the over 6500 border device searches that happened between October 2008 and June 2010, nearly half were U.S. citizens.⁵³⁷

Bhandari explains the new revision to the 2009 directive thus:

CBP recently revised its policy on electronic device searches at the border in January 2018. The new policy requires reasonable suspicion to conduct some subset of searches, but not all, whereas the previous CBP policy required no suspicion for any search. CBP's previous policy from 2009, and ICE's 2009 policy continues to remain in effect.⁵³⁸

Bhandari also explains that the "reasonable suspicion" must refer to "unlawful activity" or a "national security concern", if an "advanced" search is to be conducted: "An advanced search — sometimes called a forensic search — is any search involving external equipment connected to

⁵³⁷ U.S. Customs and Border Protection, "CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics | U.S. Customs and Border Protection," CBP.gov, 2017, <https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and>.

⁵³⁸ Esha Bhandari, "Interview March 8, 2018," 2018.

an electronic device to scan, analyze, or download the data on the device.”⁵³⁹ The new CBP directive reaffirms that officers cannot search information located remotely and requires officers to place devices in airplane mode to avoid seeing material that e.g. is stored in the cloud. However, this doesn’t mean that they won’t be able to see information in social media apps, as these apps can be set to cache information such as photos or messenger conversations locally. If a social media app was open when the phone was put into airplane mode, the chances of information in it still being visible when the phone is unlocked are very high. Furthermore, as Bhandari states, “basic searches conducted on the spot can continue without individualized suspicion, even under the new directive. This can expose travelers’ photographs, contact lists, text messages, emails, documents etc.”⁵⁴⁰

Neither the 2009 CBP directive nor the 2018 revision of it mentions social media specifically. But that part of the CBP’s mission is to look at social media as part of the “information” gleaned from border searches of electronic devices is quite evident. In April 2017, then-Secretary of Homeland Security John Kelly confirmed to the Senate Homeland Security and Governmental Affairs Committee that social media accounts were being searched via electronic devices at the border and that this also applied to U.S. citizens and lawful, permanent

⁵³⁹ Bhandari.

⁵⁴⁰ Bhandari.

residents.⁵⁴¹ News outlets such as NBC News⁵⁴², The Nation⁵⁴³ and The New York Times⁵⁴⁴ have all reported on U.S. citizens that have had their electronic devices searched with the partial or specific purpose of monitoring social media.

The ACLU and EFF are suing the Department of Homeland Security on behalf of 11 U.S. citizens who have had their devices searched. Bhandari explains:

We are litigating a case, *Alasaad v. Nielsen*, on behalf of 11 Americans who had their electronic devices searched at the border. The searches of their devices were unconstitutional, because the Fourth Amendment does not permit warrantless, suspicionless searches of electronic devices at the border given the serious privacy interests at stake.

It should be noted here that "The Fourth Amendment, even for U.S. citizens, doesn't apply at the border. That's under case law that goes back 150 years.", according to Mary Ellen Callahan, a former chief privacy officer for the Department of Homeland Security until 2009. However, according to Hugh Handeyside of the ACLU, the Fourth Amendment is only inapplicable at the

⁵⁴¹ Bhandari.

⁵⁴² Senate Homeland Security and Governmental Affairs, "Committee Hearing on Border Security and Public Safety" (U.S. Senate, 2017), https://www.thisweekinimmigration.com/uploads/6/9/2/2/69228175/hearingtranscript_senatehomelandsecurityandgovernmentalaffairshearingwithsecretarykelly_2017-04-05.pdf.

⁵⁴³ Cynthia McFadden et al., "American Citizens: U.S. Border Agents Can Search Your Cellphone," NBC News, 2017, <https://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746>.

⁵⁴⁴ Aaron Cantú and George Joseph, "Trump's Border Security May Search Your Social Media by 'Tone,'" The Nation, 2017, <https://www.thenation.com/article/trumps-border-security-may-search-your-social-media-by-tone/>.

border when it comes to the requirement of a warrant or court order for searches. The requirement that the search must be “reasonable” still applies.⁵⁴⁵

This is exactly the case the ACLU is making. The organization is trying to get the court to determine that a search at the border must either be reasonable in accordance with the Fourth Amendment or must be contingent on the issuance of a Warrant. According to Bhandari,

We are seeking relief from the court that would require the government to get a warrant before it can conduct such device searches. The case was filed in September 2017 and is pending in federal district court in Massachusetts...Additionally, we have filed amicus briefs and presented oral argument in pending criminal cases in the U.S. Courts of Appeals for the Fourth and Fifth Circuits, where the question of the proper standard for border device searches has been raised. We have also filed Freedom of Information Act requests to get more information on the government’s practices in this regard, and we support proposed legislation in Congress requiring border agents to get a warrant before they search electronic devices.⁵⁴⁶

As the CBP points out, the roughly 49,000 travelers (out of which only some are U.S. citizens or lawful, permanent residents) whose devices were searched during the CBP fiscal years of 2016 and 2017 is a very small fraction of the close to 800 million travelers processed by the CBP in

⁵⁴⁵ Daniel Victor, “What Are Your Rights If Border Agents Want to Search Your Phone?,” *The New York Times*, 2017, <https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html>.

⁵⁴⁶ McFadden et al., “American Citizens: U.S. Border Agents Can Search Your Cellphone.”

the same period.⁵⁴⁷ Taken out of this context, however, 49,000 people constitute a very large group to have experienced unconstitutional searches, if the ACLU and EFF are able to convince the court that this is the case. As I shall discuss later, the argument made by the DHS that only a tiny fraction of those entering the country have their electronic devices searched, is a utilitarian one which may not hold up to closer scrutiny.

Margo Schlanger is not so certain that it is a better solution to require a warrant for electronic device searches, because it might simply lead situation so inconvenient for the individual that they may feel pressured into consenting to a search anyway:

Be careful what you wish for. For most people, requiring a warrant would be much less convenient than the current situation. In the current situation, in most cases, when they search your device, you get it back pretty much right away. In the other situation, an officer might ask: “It’s up to you, do you want to wait for a few hours while we try to get the warrant, or do you want to consent?” This happens all the time. You get stopped by the cops, and they ask if they can do a search of your car. If you say no, you have to wait until they get a K9 unit out. And if the K9 unit alerts and they want to get a warrant, you have to wait another while. But if you say yes and you’ve got nothing in there, then you’re on your way. The balance of privacy versus convenience is just endemic to the project of conducting searches.⁵⁴⁸

⁵⁴⁷ Bhandari, “Interview March 8, 2018.”

⁵⁴⁸ U.S. Customs and Border Protection, “CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics | U.S. Customs and Border Protection.”

In the latter case, the potential of a search clearly acts as a deterrent aimed at preventing people from carrying illegal items in their car. But it obviously becomes problematic if the same principle of deterrence is applied to information. Bhandari argues that the policy may set a dangerous precedent, both in the U.S. and abroad, that might lead to self-censorship of the type seen in China:

If governments around the world adopt the U.S. policy of suspicionless searches of electronic devices, and this becomes a widespread condition of travel, it will affect freedom of expression and association worldwide, as people will self-censor for fear of hostile governments reading their private information.⁵⁴⁹

Bhandari points out that it is not only the Fourth Amendment rights that might have been violated for the 11 plaintiffs in the ACLU/EFF lawsuit, but also the First Amendment: “If people crossing back into the country know government agents can search through their phone on a whim, they will think twice about what they say and write. Strong protections are crucial to avoid chilling the exercise of First Amendment rights.”⁵⁵⁰

A 2017 EFF report also points to potential unconstitutionality of these border searches:

...The border is not a Constitution-free zone. The powers of border agents are tempered by the First Amendment (freedom of speech, association, press, and religion), the Fourth Amendment (freedom from unreasonable searches and seizures), the Fifth Amendment

⁵⁴⁹ Schlanger, “Interview, March 15 2018.”

⁵⁵⁰ Bhandari, “Interview March 8, 2018.”

(freedom from compelled self-incrimination), and the Fourteenth Amendment (freedom from discrimination).⁵⁵¹

It can also be argued that being forced to surrender a password or other login information (as some of the plaintiffs in the ACLU/EFF case have experienced) constitutes compelled speech, which is unconstitutional in most interpretations of the First Amendment⁵⁵², as freedom of expression also means freedom not to express anything.

Cross-pollination between agencies

A general problem with all information collection performed by the federal government is that though regulations are in place to prevent it when inappropriate, some people still suspect that some inter-agency exchange of information happens. A naturalized citizen whose social media handles are in the USCIS' archives simply can't know whether that information is being made available to other agencies, and so the citizen is not in control of their information – something that also applies to any information collected by border patrol agents performing a search.

Moltke believes there are many ways this can happen:

The DHS and the other agencies are all NSA “customers”. They are all part of the U.S. government, and if they for example need to perform a keyword, and the NSA is the best place to do it, they will oblige. If there's domestic suspicion of a human trafficking ring, and

⁵⁵¹ Bhandari.

⁵⁵² Sophia Cope et al., “Digital Privacy at the U.S. Border: Protecting the Data On Your Devices | Electronic Frontier Foundation,” *Eff.Org*, 2017, <https://www.eff.org/wp/digital-privacy-us-border-2017>.

word comes around about a big exchange going down, a domestic agency can ask the NSA to look for keywords related to that exchange, as long as it happens abroad. And there are very strict rules surrounding these services. The DHS can't ask the NSA to help them figure out who is in the country illegally, for example.

Moltke reiterates that there are no signs in the Snowden documents that the NSA is using their tools to conduct domestic intelligence gathering and surveillance, but:

...Then there's what happens in practice. For that, we only have eyewitness accounts from people like Snowden, who said that he could sit and read everyone's conversations. The individual analyst may stumble onto something that in theory should make them stop but they might ignore the rules or try to find a foreign intelligence angle on the activity so that they can use the information anyway. If you want to cast doubt on the efficacy of the checks and balances, there's also the risk of what is known as "parallel construction" where the ability to listen to one side of a conversation for foreign intelligence purposes ends up also gathering enough domestic intelligence from the other side of the conversation to build a case that can then be handed over to a domestic agency like the FBI or the DHS. Those agencies can then request a domestic surveillance warrant that is particular to that case, but they will already have collected some intelligence, or they can set up new surveillance measures to gather evidence. I think that is a fairly common practice in investigations of drug-related, organized or financial crime, particularly cross-border crimes. It's a civil rights issue, because the original intelligence is gathered by a foreign intelligence agency in the context of fighting terror, but the intelligence is then

laundered and handed over to, say, the FBI or the DHS. It's illegal, but it's my impression that it's a fairly common practice...Another loophole is this: If I work for a foreign intelligence service and I want to start surveilling a U.S. person's e-mail, I can simply wait until that person is abroad before I get a warrant and start the surveillance. That will give me legal access to that person's e-mail both before and after that person has traveled abroad.

In other words, the "suspicion" needed to perform a border search can be established while a person is traveling abroad, so that a border search is certain upon the person's return. Any agency can ask the NSA to use their tools to pick information about those who travel abroad, according to Moltke:

The DHS and the other agencies are all NSA "customers". They are all part of the U.S. government, and if they for example need to perform a keyword, and the NSA is the best place to do it, they will oblige. If there's domestic suspicion of a human trafficking ring, and word comes around about a big exchange going down, a domestic agency can ask the NSA to look for keywords related to that exchange, as long as it happens abroad. And there are very strict rules surrounding these services. The DHS can't ask the NSA to help them figure out who is in the country illegally, for example.

It should be emphasized here that the FISA's Section 702 does not allow for the intentional collection of intelligence about Americans, even if they travel abroad. But as critics have

noted⁵⁵³, and Moltke also states above, unintentionally collected information about Americans can be collected through these measures and make its way to other agencies, such as the DHS who can use border searches as “parallel construction”.

Privacy, liberty and the chilling effect

At the heart of the matter, however, is what Bhandari refers to as the “chilling” of the exercise of First Amendment rights. Moltke also stresses his concern about the chilling effect:

If you know you have to report your Facebook user id or your Twitter handle or your Instagram name when you enter the United States, people will stop using those platforms for communication and will be pushed towards using Telegram or other encrypted tools. If you know you have to account for every critical comment you’ve made about Donald Trump on Facebook at the border, you’ll stop making them or make them in secret. This means that people will stop expressing themselves publicly and participate in debates, thereby no longer impacting or inspiring others.⁵⁵⁴

In the two previous chapters, I showed how this kind of self-censorship can be viewed as just as antithetical to a truly open, democratic discourse as using disinformation to drown out the information needed to make an informed decision. This is why, as I have discussed in depth

⁵⁵³ Alex Ward, “House Approves FISA and Allows Spying on Americans to Continue,” Vox, 2018, <https://www.vox.com/2018/1/11/16878220/house-vote-surveillance-spying-fisa>.

⁵⁵⁴ Moltke, “Interview, 3/29/2018.”

elsewhere⁵⁵⁵ and will also argue below, privacy rights are inseparable from the right to freedom of expression – simply because it *must* be possible to develop opinions and attitudes as expression/speech without being held accountable for the same expression/speech taken out of context or used without your acknowledgement. Put another way, an individual must be able to express themselves freely in private in order to develop the expression/speech the individual wishes to make public using First Amendment rights. Also, if the First Amendment indeed does protect an individual against being compelled to express themselves or speak, it follows that there is no true freedom of expression without the ability to express thoughts privately.

It is imperative for the free exchange of ideas through freedom of speech that ideas can be developed without influence, intrusion or untimely interpretation from and by outside forces. As the British Lord Steyn put it “Freedom of speech is the lifeblood of democracy. The free flow of information and ideas informs political debate. It is a safety valve: people are readier to accept decisions that go against them if they can in principle seek to influence them.”⁵⁵⁶

Referencing literary classics by Kafka and Orwell, Daniel Solove⁵⁵⁷ points to how surveillance and the fear of decontextualized interpretation can have an inhibiting effect on the free flow of information. Being able to develop even the most subversive ideas through discussions with others without the risk of it taken out of context and used against you, is at the core of freedom

⁵⁵⁵ “Compelled Speech - Dictionary Definition of Compelled Speech,” *Encyclopedia of the American Constitution* (The Gale Group, 2000), <https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/compelled-speech>.

⁵⁵⁶ Bay, “The Ethics of Unbreakable Encryption: Rawlsian Privacy and the San Bernardino iPhone.”

⁵⁵⁷ Australian Law Reform Commission, “A Common Law Right,” ALRC.gov.au, 2018, <https://www.alrc.gov.au/publications/common-law-right>.

of speech and thus, the right to freedom of speech by definition must also have a privacy dimension. If a right to freedom of speech exists, so must the right to freedom of speech in private. Of course, no development and discussion of ideas can happen without access to the information from which those ideas grow. Intellectual freedom and the ability to access information freely, without having to provide justification, is as closely tied to privacy as the ability to express what results from contemplation of that information. In its Code of Ethics, the American Library Association emphasize the connection between intellectual freedom and privacy in principles II and III, with the first being a vow to resist censorship and the second being a vehement defense of the right to privately and confidentially seek, receive information and consult, borrow, acquire or transmit resources within the library setting.⁵⁵⁸ This is further expanded upon in the ALA's *Intellectual Freedom Manual*.⁵⁵⁹ But, as, Neil M. Richards makes abundantly clear in the definition of his concept of *Intellectual Privacy*, intellectual freedom extends far beyond the library walls. For Richards, privacy is crucial to our development of a perception of self as well as pluralist, democratic ideals:

Intellectual-privacy theory suggests that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy —

⁵⁵⁸ ALA, "Code of Ethics of the American Library Association," *ALA Code of Ethics*, 2008, 1, <http://www.ala.org/advocacy/proethics/codeofethics/codeethics>.

⁵⁵⁹ American Library Association Office for Intellectual Freedom, *Intellectual Freedom Manual Ninth Edition, Intellectual Freedom Manual (9th Edition)*, 2015, https://carleton-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=01BRC_CCO_ALMA51385855100002971&vid=01BRC_CCO&search_scope=Everything&tab=default_tab&lang=en_US.

protection from surveillance or interference — is necessary to promote this kind of intellectual freedom... This claim requires at a minimum protecting individuals' rights to think and read, as well as the social practice of private consultation with confidantes. Surveillance inclines us to the mainstream and the boring...when we are watched while engaging in intellectual activities, broadly defined — thinking, reading, web surfing, or private communication — we are deterred from engaging in thoughts or deeds that others might find deviant. Protection of these individual rights and social practices allows individuals to develop both intellectual diversity and eccentric individuality. They reflect the conviction that big ideas like truth, value, and culture should be generated from the bottom up rather than from the top down.⁵⁶⁰

All of this, however, may very well simply be a Western paradigm. Until recently, there was no word in any of the Chinese languages for “privacy”, only recently has the word “Yin-si” been put into a context of information security and given a meaning that approximates the Western understanding of “privacy”. Before then, its meaning approximated “sinful secret”.⁵⁶¹⁵⁶² The Confucianist culture in China, even with its rather individualist notion of self-cultivation,

⁵⁶⁰ Neil M. Richards, “The Dangers of Surveillance,” *Harvard Law Review* 126, no. 7 (2013): 1946–48, <https://doi.org/10.1093/wbro/10.2.201>.

⁵⁶¹ Daniel J. Solove, “Nothing to Hide. The False Tradeoff between Privacy and Security,” *Yale* 8, no. 6 (2011): 1–255, <https://doi.org/10.1038/ncb0606-541b>.

⁵⁶² Hao Wang, *Protecting Privacy in China: A Research on China's Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China* (Springer Science & Business Media, 2011).

seemed to have less of a need for privacy as a concept. Since freedom of speech and privacy are intrinsically tied to individual rights, are they also tied to the preference for individualist culture in the U.S. and the rest of the Western world? Is it only because our culture is individualist that we even care about a border agent or a DHS analyst looking at our social media information? To create an understanding of this, and to provide the cultural dimension that will lead us into the discussion of the policies through a Rawlsian lens, I will now explore privacy in light of the hypothesis that the United States has an individualist culture because of its history.

Cultural background

What is privacy?

There is an abundance of scholarship surrounding privacy, although much of it takes privacy for granted without actually defining the term. Some high-profile attempts have been made, of which some are essential to any review of privacy literature. As noted by Acquisti, Friedman and Telang⁵⁶³, attempts at defining privacy often produces mixed results – the concept and its definition often remain ambiguous, changing with the perspective of the observer. Perhaps the most classic definition of privacy comes from Warren and Brandeis’ classic 1890 formulation of privacy being “the right to be let alone”⁵⁶⁴ This line has been repeated often and has become

⁵⁶³ Staff, “The Long March to Privacy | The Economist,” The Economist, 2006, <https://www.economist.com/node/5389362>.

⁵⁶⁴ Alessandro Acquisti, Allan Friedman, and Rahul Telang, “Is There a Cost to Privacy Breaches? An Events Study,” *Fifth Workshop on the Economics of Information Security*, 2006, 2, <https://doi.org/10.1.1.73.2942>.

such a standard in privacy discussions that Diffie and Landau⁵⁶⁵ uses it without even referencing Warren and Brandeis:

The right to privacy is the right to autonomy and it includes the right to be let alone.

Privacy encompasses the right to control information about ourselves, including the right to limit access to that information. The right to privacy embraces the right to keep confidences confidential and to share them in private conversation. Most important, the right to privacy means the right to enjoy solitude, intimacy and anonymity.

Diffie and Landau begins and ends this quote with Warren and Brandeis' idea that privacy is intertwined with solitude. The authors also point to ancient Jewish law as including a right to privacy, and they cite article 12 in the UN's 1948 Universal Declaration of Human Rights as an argument for privacy rights. Although article 12 is very explicit that "No one shall be subjected to arbitrary interference with his privacy..."⁵⁶⁶, it lacks a definition of what privacy actually is. Context is important here. Warren and Brandeis wrote about the right to be let alone in relation to the increasing emergence of news media, and they are mainly concerned with the private lives of citizens being made public through newspapers, as mass media began to mature. This contextual discussion highlights the need to define privacy as something that is related to something else. From what are things being kept private? Privacy is the right to be let alone by

⁵⁶⁵ Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 1, <https://doi.org/10.2307/1321160>.

⁵⁶⁶ Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT press, 2010), 142.

whom? Whose access to one's information is it that one has the right to limit according to Diffie and Landau? The easy answer is: Everyone. But as we've seen above, it matters who and in which situations we choose to divulge or withhold private information or imagery.

Helen Nissenbaum has unpacked contextuality in the privacy discussion very thoroughly. She suggests a normative approach to privacy by presenting the concept of contextual integrity. According to this concept, two norms must be upheld in order for invasions of or limitation of privacy to be allowable. One is appropriateness, about which Nissenbaum writes:

As the label suggests, norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.⁵⁶⁷

What is not appropriate to Nissenbaum is to cross those lines, i.e. to reveal religious affiliations or financial status with one's employer or share romantic information with the bank. Or, more

⁵⁶⁷ United Nations, "Universal Declaration of Human Rights | United Nations," UN.org, 1948, <http://www.un.org/en/universal-declaration-human-rights/>.

importantly, that these lines are crossed without the individual's permission or voluntary participation. The other norm, or set of norms, regards distribution and flow of information. Nissenbaum finds that in some contexts, distribution and flow of private information can be allowable, such as within medical or financial systems, but in most cases, it requires the voluntary participation of the individual to whom the information relates. According to Nissenbaum, to overstep the boundaries of (informational) privacy, the privacy breach must be both appropriate and the flow of information must be acceptable to the person it concerns. If one of these norms are not upheld, the breach of privacy can be viewed as unethical.

Richard A. Posner shows the importance of context in privacy by first defining privacy through economic analysis. He shows that the ability to keep information private is something of economic value which is why, in many cases, disclosure is resisted. In cases of misrepresentation in, e.g. the marketplace, private information is of key value to the misrepresenter, otherwise he would not necessarily be compelled to keep the information private. On the other side, the person trading with the misrepresenter would view less limited access to this private information as valuable because it gives him a bargaining advantage. Trade secrets and yet-unpublished sales numbers are parts of such a private/public system. In this economic analysis, Posner suggests that the ability to keep information private is related to the right to own and control property. I shall return to this notion later, when discussing Rawls' view of privacy. While Posner suggests that privacy can be seen as part of an economic transaction and as part of a larger property right paradigm, he also indicates that there are boundaries. The law, as well as ethics, set boundaries for another right which works contrary to the right to privacy, namely the right to transparency:

But everyone should be allowed to protect himself from disadvantageous transactions by ferreting out concealed facts about individuals which are material to the representations (implicit or explicit) that those individuals make concerning their moral qualities.⁵⁶⁸

In fact, Posner finds that simply returning to Warren and Brandeis' right to be let alone as an argument for privacy more generally, is insufficient:

It is no answer that such individuals have "the right to be let alone." Very few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves. Why should others be asked to take their self-serving claims at face value and be prevented from obtaining the information necessary to verify or disprove these claims?⁵⁶⁹

He does, however, agree that as humans, most of us have a need for some level of personal privacy, just as Diffie and Landau state that "Privacy is at the very soul of being human"⁵⁷⁰ But, he writes, this can also be seen as a part of a type of Homo Economicus privacy:

Some private information that people desire to conceal is not discreditable. In our culture, for example, most people do not like to be seen naked, quite apart from any discreditable fact that such observation might reveal. Since this reticence, unlike concealment of discreditable information, is not a source of social costs, and since transaction costs are

⁵⁶⁸ H. Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review*, n.d., 120.

⁵⁶⁹ Richard A Posner, "The Right of Privacy," *L. Rev* 2, no. 393 (n.d.): 400, <https://www.copyright.com/cc/basicSearch.do?>

⁵⁷⁰ Posner, 400.

low, there is an economic case for assigning the property right in this area of private information to the individual; and this, as we shall see, is what the law does.⁵⁷¹

In other words, Posner believes that since our bodies are our property, we control what should happen to them in terms of being on display or being depicted in, say, photographs. And this makes privacy a property discussion. Posner objects against any a priori, unsubstantiated and/or metaphysical needs for privacy. He dismisses Edward Bloustein's argument that privacy is related to individuality, and that without privacy, everyone would tend towards being more conformist, simply because one would be constantly under public scrutiny. Posner writes: "...history does not teach that privacy is a precondition to creativity or individuality. These qualities have flourished in societies, including ancient Greece, Renaissance Italy, and Elizabethan England, that had much less privacy than we in the United States have today."⁵⁷² In summary, even though Posner argues from an economic angle, his notion of privacy seems to be reduceable to the right to keep secrets. In this he joins Diffie and Landau and their advocating for the right to "keep confidences confidential" as mentioned above, even though the latter authors argue from a more basic, almost a priori privacy stance.

Alan Westin, one of the most notable and respected privacy scholars has also made a similar reduction, defining privacy as "the claim of an individual to determine what information

⁵⁷¹ Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 142.

⁵⁷² Posner, "The Right of Privacy," 400.

about himself or herself should be known to others”.⁵⁷³ James Moor⁵⁷⁴ presents a similar idea, that privacy is the ability to control the flow of information about oneself. But as Solove⁵⁷⁵ shows, defining a right to privacy as merely a right to keep secrets is flawed and over-reductive. From such a definition follows that you don’t need protection of your privacy if you have no secrets to hide, which is an invalid argument according to Solove, as it rests on the “underlying assumption that privacy is about hiding bad things. Agreeing with this assumption concedes far too much ground and leads to an unproductive discussion of information people would likely want or not want to hide”.⁵⁷⁶

Running with Solove’s argument, secrets are usually some form of information and hence reducing privacy to mere secret-keeping also reduces the whole notion of privacy to the sub-category of information privacy. More importantly, inserting a normative evaluation into what should or shouldn’t be private based on what is “bad” or “wrong”, turns the right to privacy into a question of moral judgment. It would validate the restriction of human rights seen in many theocracies, which is in direct contradiction to the pluralistic ideal that, among others, Rawls presents us with. Thus, the conception of privacy as the right to keep secrets is by no means the only such conception. I have already discussed Warren and Brandeis’ “right to be let alone”, and

⁵⁷³ Posner, 407.

⁵⁷⁴ Alan F. Westin, “Social and Political Dimensions of Privacy,” *Journal of Social Issues* 59, no. 2 (2003): 3, <https://doi.org/10.1111/1540-4560.00072>.

⁵⁷⁵ James Moor, “Towards a Theory of Privacy in the Information Age,” *Computers and Society* 27 (1997): 27–32.

⁵⁷⁶ Daniel J. Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” *San Diego Law Review* 44, no. May (2007): 1–23, <https://doi.org/10.2139/ssrn.998565>.

Introna and Poloudi defines it as “freedom from the judgment of others”⁵⁷⁷ All of these definitions however, define privacy as an individual right an infringement of which is also an impediment to personal freedom. This turns out to be essential in exploring an American or even a Western view of privacy as a concept.

Privacy as expression of individualism

Privacy values are intrinsically linked to values of liberty, freedom from oppression and freedom of speech. These are also values that are usually emphasized when attempts are made at defining a national identity for the United States. As a nation that broadly embraces multiculturalism, it is, of course, difficult to even speak of a national, cultural identity in the U.S. However, those freedom values are often touted as what binds the many cultures in the U.S. together. The common, Jeffersonian pursuit of happiness through liberty in life is what drew the original colonists to the continent, it was the cause of the American revolution and the founding of the nation, and arguably, it was the pursuit of freedom ideals (albeit with extremely different and uneven allocations of liberty) that caused the Civil War.

The dual policy analyzed in this chapter, however, is seen by some as being a massive infringement upon the privacy – and thereby the freedom – of individuals. Arguably, it is in direct contradiction of that sole tenet of individual freedom that constitutes the cultural identity of the United States, and it seems paradoxical that such a policy (and others like it) can even be found in the U.S. In the following, I will explore this paradox and thereby provide the cultural information necessary to contextualize the policy frames that are to be held up against the

⁵⁷⁷ Solove, 764.

Rawlsian frame at the end of the chapter. Untangling the paradox begins with understanding why the United States' sociocultural identity is so intrinsically tied to freedom. To explore this, I will begin by presenting Seymour Martin Lipset's hypothesis and argument for why the U.S. has a closer relationship with liberty than other nations, part of the concept of *American exceptionalism*.

The concept of American exceptionalism can be traced all the way back to the founding of the nation.⁵⁷⁸ The United States is widely viewed as the first democratic nation to be constructed from the ground up using principles borne out of the Enlightenment, rather than being a result of past tribal wars or monarchic/imperial wielding of power, and this has caused some to posit the view that the U.S. is different than all other democracies.⁵⁷⁹ The writings of some of the “founding fathers” of the U.S. have been interpreted as presenting an exceptionalism that is more theoretical in nature, i.e. it is the unique conditions under which the nation was founded that sets it apart from other democracies. In this view, there is not necessarily an American identity that is substantially different from many other national identities, although smaller, cultural differences do of course, exist. For others, however, the exceptionalism is an integral part of what it means to be American. The prioritization of individual liberty over communitarianism is what makes the U.S. exceptional in this view, which has proponents across political, ideological, sociological and philosophical fields of thought. In particular, the sociologist Seymour Martin Lipset is

⁵⁷⁸ Lucas Inrona and Athanasia Pouloudi, “Privacy in the Information Age: Stakeholders, Interests and Values,” *Journal of Business Ethics* 22, no. 1 (1999): 1, <https://doi.org/10.1023/A:1006151900807>.

⁵⁷⁹ Bernard Bailyn, *The Ideological Origins of the American Revolution* (Harvard University Press, 2017); Louis Hartz, *The Liberal Tradition in America* (Houghton Mifflin Harcourt, 1991).

credited with arguing for this view. In his 1963 book, *The First New Nation: The United States in Historical and Comparative Perspective*⁵⁸⁰, Lipset argues that distinctly American values were developed in the post-revolutionary period of American history, which underpins the identities, mentalities and politics of Americans even in contemporary society. He uses historical events as data to substantiate his argument, and compares the United States to other modern democracies, attributing most of the differences he finds to these values. Two of the central values in this value set are equality and achievement, which Lipset says are in constant conflict with each other:

America's key values equality and achievement stem from our revolutionary origins... we believe all persons must be given respect simply because they are human beings; we believe that the differences between high- and low-status people reflect accidental, and perhaps temporary, variations in social relationships....The value we have attributed to achievement is a corollary to our belief in equality. For people to be equal, they need a chance to become equal. Success, therefore, should be attainable by all, no matter what the accidents of birth, class, or race. Achievement is a function of equality of opportunity. That this emphasis on achievement must lead to new inequalities of status and to the use of corrupt means to secure and maintain high position is the ever recreated and renewed American dilemma.⁵⁸¹

⁵⁸⁰ Alexis De Tocqueville, *Democracy in America (1835)*, vol. 10 (Regnery Publishing, 2003).

⁵⁸¹ Seymour Martin Lipset, *The First New Nation: The United States in Historical and Comparative Perspective* (Heinemann, 1963).

This view is somewhat aligned with Rawls' original position and the disregard for pre-established status, which gets filtered out by the veil of ignorance. For Rawls, however, the principles of Justice as Fairness and particularly the difference principle, are ways to reduce inequalities of status if these impede on equality of opportunity and achievement. For Lipset, the latter does not initially appear as necessary. In 1963, Lipset argued that the "American Creed"⁵⁸² of equality and achievement had done away with deference to hierarchies based on anything other than achievement and merit for two centuries, with some major exceptions coming along slower than the rest of society, such as slavery and equality of ethnicity, gender and sexuality. Lipset writes that the reason why these values straggle behind in the U.S. is in part because the American South is more like Europe: "The American South, in other words, places more emphasis on elitism, on ascription, on particularism, and on diffuseness, than does the North, and this makes the South more like Europe than are other parts of the United States."⁵⁸³

Lipset's book first came out before the assassination of president John F. Kennedy on November 22, 1963. For Lipset, that tragedy initiated a "series of political disasters and protest reactions", and he added a new foreword to *The First New Nation* in which he called the late 60s and the 70s a

...dismal story of the subsequent decade-and-a-half of Vietnam, a country divided by mass protest, the growth of left- and right-wing extremism, Watergate, exposés of corruption and malfeasance in business and the intelligence agencies, the overthrow of

⁵⁸² Lipset, 2.

⁵⁸³ Lipset, 319.

two incumbent presidents, Johnson and Nixon, followed in office by two men perceived by much of the public as weak and inept and finally during the seventies, serious recession succeeded by a runaway inflation.

This caused Lipset to refocus his view of American exceptionalism towards and move towards individualism. In 1986, well into the Reagan presidency, he wrote a paper in which he described the two main values “embodied in the Declaration of Independence” and serving as a “orientations throughout subsequent American history” as *individualism* and achievement, rather than *equality* and achievement, adding “Thus, the United States remained through the nineteenth and early twentieth centuries the extreme example of classically liberal or Lockean society which rejected the assumptions of the alliance of throne and altar, of ascriptive elitism, of mercantilism, of *noblesse oblige*, of communitarianism.”⁵⁸⁴

In his 1963 work, Lipset discussed and problematized the conflict between equality and achievement as being a constant struggle, with the latter often yielding both cultural and economic inequalities that contradicts the former. In 1986, he argued that it was not so much the *opportunity* or *result* dimensions of equality that drove those who built the nation (and thereby made America exceptional) over the past centuries, but rather the individualism and rejection of communitarianism associated with *pursuing* opportunity.

⁵⁸⁴ Lipset, 320.

When he died towards the end of 2006, Lipset was described as one of the first neoconservatives⁵⁸⁵, albeit in the historical definition rather than the meaning of the term co-opted in popular discourse. In 1988, Lipset explained that the term “neoconservative” was originally coined as a way to describe people holding right-leaning positions on the American left, rather than to describe someone being wholly right-of-center politically:

Many in the United States and elsewhere assumed that neoconservatives were hardline right-wingers on domestic as well as foreign issues, whereas in fact almost all of them remained supportive of welfare planning state and New Deal policies... But this background was forgotten or ignored as the old-line conservative intellectuals, Republican politicians, and many in the business community reacted positively to being told that a number of prestigious intellectuals, who had once been on the Left, were now conservatives. Neoconservatives thus found themselves rejected by their old friends and hailed by their opponents.⁵⁸⁶

As a result, Lipset argued that neoconservatism:

...has ceased to exist. The term lost its meaning as commentators applied it, beyond its original application to strongly anticommunist leftists, to a wide range of traditional

⁵⁸⁵ Seymour Martin Lipset, “Historical Traditions and National Characteristics: A Comparative Analysis of Canada and the United States Historical Traditions and National Characteristics: A Comparative Analysis of Canada and the United States,” *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie* 11, no. 2 (1986): 114, <http://www.jstor.org/stable/3340795>.

⁵⁸⁶ Douglas Martin, “Seymour Martin Lipset, Sociologist, Dies at 84,” *The New York Times*, 2007, <http://www.nytimes.com/2007/01/04/obituaries/04lipset.html>.

conservatives in the United States and abroad who are classically liberal antistatists on domestic issues and hard-liners on foreign policy.⁵⁸⁷

Lipset's description of the labels and positions in American politics in the 20th century and particularly around the election of Ronald Reagan in 1980, is emphasized here because it introduces an important distinction that must be understood as part of the cultural background from which the policies analyzed here emerge – and how Rawls fits into the picture. Lipset's use of the term “antistatist liberalism” is related to his notions of individualism/equality and achievement as intrinsic parts of the “American Creed” and national identity ever since the nation's inception.

Regardless of how the term is used colloquially today, “liberalism”, in its original Lockean sense, emphasizes the rights of the individual vis-à-vis the state. Adding Hobbes⁵⁸⁸ and Rousseau⁵⁸⁹ (and later, Rawls) to the picture produces a conception of the state as a malleable, but firmly defined instance of representation of the will of voluntarily congregating, free individuals. Yet, Lipset wrote that after the election of Ronald Reagan (and Margaret Thatcher in the United Kingdom) no-one in American politics could say that they were *not* liberal:

⁵⁸⁷ Seymour Martin Lipset, “Neoconservatism: Myth and Reality,” *Society*, no. July/August (1988): 34, <https://link.springer.com/content/pdf/10.1007/BF02695739.pdf>.

⁵⁸⁸ Lipset, 36.

⁵⁸⁹ Garrath Williams, “Thomas Hobbes: Moral and Political Philosophy,” Internet Encyclopedia of Philosophy (Internet Encyclopedia of Philosophy Pub), accessed March 10, 2018, <https://www.iep.utm.edu/hobmoral/#SH4d>.

Liberalism remains the source of contemporary political values of the American Right and Left. The American Revolution gave rise to an ideology that is antistatist, antimonarchical, antichurch establishment, promeritocratic competition, and ultimately populist. Basically, the American creed has been suspicious of the state...The Bill of Rights was designed to inhibit state power.⁵⁹⁰

It can be argued that what Lipset really described here is what would be understood as neo-liberalism today, at least according to the definition of the term in the Oxford English Dictionary (which also illustrates that like “Neo-conservative”, the term was originally meant to describe positions that were left-of-center rather than right-of-center)⁵⁹¹

To sum up, according to Lipset, the predominant culture in which the policies analyzed here emerge should be rooted in a strongly individualist, anti-statist, meritocratic, anti-communitarian culture which grew out of the revolutionary era and which has survived ever since. This seems to be at odds with this chapter’s analysis of a policy that has been criticized for allegedly allowing the state to overreach, violate privacy rights, and infringe on individuals’ liberties. An explanation to this paradox may be found in the work of those who have critiqued Lipset.

⁵⁹⁰ James Delaney, “Jean-Jacques Rousseau (1712—1778),” The Internet Encyclopedia of Philosophy (Internet Encyclopedia of Philosophy Pub), accessed March 10, 2018, <https://www.iep.utm.edu/rousseau/>.

⁵⁹¹ Lipset, “Neoconservatism: Myth and Reality,” 29.

Local communitarianism and privacy

A prime example is a paper by Grabb, et al. from 1998 written seemingly in response to Lipset's paper from 12 years prior about the differences between Canadian and American national identities. Though Grabb et al. do not dispute most of Lipset's description of the national American identity (itself a fractured image, as can be seen by Lipset's 1963 separation of the American South from the rest of the nation when it comes to adherence to the American Creed), they call into question the individualistic emphasis that Lipset developed on the verge of the Reagan era. They argue that the historical evidence from which Lipset builds his understanding of equality, and later, individualism, may be at best incomplete, at worst misguided. The authors argue "that the major defining element in Lipset's version of the American Creed is the belief in what we refer to as "liberal individualism", or the idea that each person should have the right to think and act in a way that is largely free from communitarian or collectivist restrictions."⁵⁹² Grabb et al. posit that though individualism is described as part of the historical, sociocultural fabric of the United States by scholars other than Lipset, those researchers are actually describing a type of individualism that is different from Lipset's:

These researchers suggest that the American value system, at least during the period of the nation's founding, was not anchored in or defined by such extreme self-interest. On the contrary, most of these authors identify a far more group-oriented and socially responsible set of cherished ideals at the core of Revolutionary American society. In this portrayal of the early American value system, personal liberty is highly prized and

⁵⁹² Oxford English Dictionary, "Neo-Liberal, Adj. and N.," *Oxford English Dictionary*, accessed March 10, 2018, <http://www.oed.com/view/Entry/245592?redirectedFrom=neo-liberal#eid>.

encouraged, but, at the same time, is consistently moderated by a regard for civic responsibility and a respect for the rights of others.⁵⁹³

Quoting Gordon S. Wood⁵⁹⁴, the authors write: “In fact, for genuine "liberty" to be realized, it was essential that "citizens were virtuous - that is, willing to sacrifice their private interests for the sake of the community".⁵⁹⁵ Grabb et al. proceed by presenting historical evidence of a concept just as prevalent in post-revolutionary thought as Lipset’s individualism:

“Republicanism”. Contemporary observers would be excused for their confusion here, as “Republicanism” is only to a small extent a defining tenet of the ideologies followed by the Republican party in the U.S. and has even less to do with the present self-conceptions of most people labeling themselves as “Republicans” – just as the contemporary use of the term “liberal” has very little to do with classic liberalism. “Republicanism” in the post-revolutionary era, according to Grabb, et al. is actually a communitarian idea, the existence of which is widespread in the historical documentation and scholarly work reviewed by the authors:

In the present context, however, the term is used in the classical Greco-Roman sense, or in the Renaissance meaning associated with Rousseau. In either of these usages, republicanism rests on a belief in the responsibility of free individuals to participate in serving the public good, so as to promote both a better society and, ultimately, a form of

⁵⁹³ Grabb, Baer, and Curtis, “The Origins of American Individualism: Reconsidering the Historical Evidence The Origins of American Individualism: Reconsidering the Historical Evidence,” 513.

⁵⁹⁴ Grabb, Baer, and Curtis, 519.

⁵⁹⁵ Gordon S Wood, *The Radicalism of the American Revolution* (New York: Alfred E. Knopf, 1992), 104.

individualism that is far removed from narrow self-interest... Clearly, then, many of those who argue for individualism as a founding American value are not referring to the liberal or self-centered version suggested by Lipset's analysis.⁵⁹⁶

The authors also point to a general flaw in the Lipset's broader argument that contemporary notions of individualism can be traced back to the nation's roots. Rather convincingly, they argue that Lipset and others who present the idea of American exceptionalism and identity as one of extreme individualism and antistatism are really taking the views of the elite to be representative of the views of the nation, but "...it is misleading to assume, however, that the values of a society are basically identical with the values of its elite."⁵⁹⁷ In what can be seen as a sort of parallel between the chasm between the elite and the populace described by Yubo Kou in the chapter on China, Grabb et al. present evidence of a post-revolutionary United States in which "local communalism" was actually the dominant social belief system: "there is generally strong and consistent evidence that the predominant belief system of the time was a form of "local communalism". In other words, American culture in the Revolutionary period was steeped in a set of values that placed primary emphasis on an adherence to the standards of small-town community life, or what has been called "collectivism within a smaller group". In this setting, neither unconditional personal freedom, nor a strong commitment to a wider national polity, was

⁵⁹⁶ Grabb, Baer, and Curtis, "The Origins of American Individualism: Reconsidering the Historical Evidence The Origins of American Individualism: Reconsidering the Historical Evidence," 519.

⁵⁹⁷ Grabb, Baer, and Curtis, 519.

widely encouraged.⁵⁹⁸⁵⁹⁹⁶⁰⁰ This local communalism, the authors argue, is much more indicative of American culture, even up to their time of writing. It can be argued that the authors do not take the globalization of the 1990s and the emergence of the Internet into account, but their argument is still a strong moderation of Lipset's American Creed, simply on the strength of the evidence presented in the paper. What then, about the fact that observers of the construction of the United States as a nation, such as Alexis de Tocqueville, pointed to the individualistic nature Americans, which also helped spawn the current ideals of American exceptionalism? Grabb et al. note that "...the term, individualism, did not even appear in the English language until 1839, more than 50 years after the War of Independence" and that the word's emergence may have been based on a poor translation: "As Europeans who had never quite experienced the small-town community orientation of Revolutionary America in their own country, both Chevalier and Tocqueville chose the French word, "individualisme", in an attempt to label what was essentially local communalism. The French word easily, if mistakenly, became "individualism" in English translation."⁶⁰¹

However, the present-day sense of this idea was not the meaning that these writers wished to convey in their original descriptions of the prevailing American ethos during the period of the

⁵⁹⁸ Grabb, Baer, and Curtis, 521.

⁵⁹⁹ Grabb, Baer, and Curtis, 522.

⁶⁰⁰ Barry Alan Shain, *The Myth of American Individualism: The Protestant Origins of American Political Thought* (Princeton University Press, 1996).

⁶⁰¹ Alexander Haim Pekelis, "Law and Social Action; Selected Essays. Edited by Milton R. Konwitz" (Ithaca, Cornell University Press, 1950).

Revolution. This point seems especially clear in Chevalier's analysis, which stresses the "spirit of locality" as the utmost concern among Americans in that era, and which contrasts this orientation with the more centralized, national conception of democracy found in France at the time.

Tocqueville describes the "individualism" of Americans in similar terms, as the tendency of "each citizen to isolate himself ... and withdraw into the circle of family and friends; with this little society formed to his taste, he gladly leaves the greater society to look after itself'.

Observations by other European writers, including the Swiss-German churchman, Phillip Schaff, provide a similar image of a localized, communal, and Protestant society, in which tolerance of individual differences was far from prevalent...All of these observations by early historians and visitors parallel the documentary evidence of literate Americans noted earlier. In both instances, we are presented with an image of the American population that, on the whole, was much more strongly committed to localized, small-town collectivist values than to liberal, individualist belief..⁶⁰²

If this image is more historically correct than Lipset's, it would lend credence to the position of American neo-communitarians such as Amitai Etzioni. He has argued against the neoliberalism that came out of the 1980s and the Reagan era precisely because he sees those values as being in conflict with the original, communal values of pre-Reagan America:

⁶⁰² Grabb, Baer, and Curtis, "The Origins of American Individualism: Reconsidering the Historical Evidence The Origins of American Individualism: Reconsidering the Historical Evidence"; De Tocqueville, *Democracy in America* (1835); Michel Chevalier, *Society Manners and Politics in the United States: Letters on North America* (1840), vol. 83 (Ayer Publishing, 1969); Shain, *The Myth of American Individualism: The Protestant Origins of American Political Thought*.

Culturally, both Thatcher and Reagan promoted individual preferences over the common good, celebrating *numero uno*—that is, the self. Thatcher most famously stated: “There is no such thing as society.”⁶⁰³

Etzioni stresses that he does not advocate for a return to the “bad old days” where e.g. racism and sexism were even more rampant than today⁶⁰⁴, but rather stresses how the core concept of community can be integrated into modern society in a very beneficial way:

Old communities (e.g., traditional villages, tribes, and clans) were geographically bounded and the only communities of which people were members. In contrast, new communities are often limited in scope and reach. Members of one residential community are often also members of other communities – for example work, ethnic, or religious ones. As a result, community members have multiple sources of attachments and, if one threatens to become overwhelming, individuals will tend to pull back and turn to another community for their attachments. This multicomunity membership protects the individuals from both moral oppression and ostracism.⁶⁰⁵

⁶⁰³ Amitai Etzioni, “My Kingdom for a Wave,” *The American Scholar*, 2013, <https://theamericanscholar.org/my-kingdom-for-a-wave/#>.

⁶⁰⁴ Etzioni.

⁶⁰⁵ Amitai Etzioni, “Communitarianism,” in *Encyclopedia of Political Thought*, ed. Michael T. Gibbons (Wiley and Sons, Ltd., 2015), sec. 3, <https://doi.org/10.1002/9781118474396.wbept0184>.

The neo-communitarian movement, of which Etzioni is considered a leader with a high level of influence on center-left political leaders coming up in the 1990s such as Tony Blair, Bill Clinton and later, Barack Obama, was partially a reaction of opposition to John Rawls' theories. Rawls was viewed by neo-communitarians such as Charles Taylor as being more like what we would now call a libertarian, rather than a liberal. Taylor believed that the consequence of Rawls' world view was a splintering of society, a phenomenon he called "Atomism", and that Rawls' brand of individualism was antithetical to the idea of society as such, writing: "the free individual of the West is only what he is by virtue of the whole society and civilization which brought him to be and which nourishes him."⁶⁰⁶

Similarly, Michael Sandel believes that Rawls does not account for moral institutions a person may adhere to without having made a rational choice about it: "If we understand ourselves as free and independent selves, unbound by moral ties we haven't chosen, we can't make sense of a range of moral and political obligations that we commonly recognize, even prize."⁶⁰⁷ Michael Walzer has argued, in a more conciliatory manner, that "insofar as liberalism tends towards instability and dissociation, it requires periodic, communitarian correction".⁶⁰⁸ Another well-known communitarian, Alasdair MacIntyre, echo these sentiments in his work.⁶⁰⁹

⁶⁰⁶ Charles Taylor, "Atomism," in *Philosophy and the Human Sciences: Philosophical Papers 2*, 1985, 187–210.

⁶⁰⁷ M Sandel, "JUSTICE: What's the Right Thing to Do?," *Hong Kong Journal of Social Work*, 2009, 220, <http://www.worldscinet.com/abstract?id=pii:S0219246209000175%5Cnpapers2://publication/uuid/CA695EF0-7B53-47CB-B253-730E4095DA2E>.

⁶⁰⁸ Michael Walzer, "The Communitarian Critique of Liberalism," *Political Theory* 18, no. 1 (1990): 21, <http://journals.sagepub.com/doi/pdf/10.1177/0090591790018001002>.

⁶⁰⁹ Alasdair C MacIntyre, "After Virtue: A Study in Moral Theory," *London Duckworth* 2nd (1984): 286, <https://doi.org/10.2307/2219228>.

The neo-communitarian critique of Rawls seems to be based on a very narrow reading of *A Theory of Justice*, however, and overall, it does not account for Rawls' later work nor his emphasis on social cooperation as duty. Several scholars, such as Caney, Selznick and the aforementioned Etzioni have pointed to a multitude of positions where Rawls' theories overlap with neo-communitarianism, including the aforementioned duty of social cooperation and the idea of the individual as embedded in society.⁶¹⁰

Hence, there is evidence that contradicts the notion that the United States somehow has a national, cultural identity that is more individualistic and substantially different from other Western nations. Grabb et al. indicate that newer nations with Anglophone populations like Australia and Canada have more in common with the U.S. than Lipset acknowledges, and I would argue that the differences have only become (slightly) less prevalent after the emergence of the Internet and the partial, cultural harmonization following in its wake in the West.⁶¹¹ Furthermore, Grabb et al. point to the fact individualism as a historical and cultural phenomenon has largely been viewed anachronistically, from a modern mindset – a lens through which the neo-communitarian critique of liberalism should also be viewed.

⁶¹⁰ Philip Selznick, "Foundations of Communitarian Liberalism," *Responsive Community* 4, no. 4 (1994): 16–28; Simon Caney, "Liberalism and Communitarianism: A Misconceived Debate," *Political Studies* 40, no. 2 (1992): 273–89, <https://doi.org/10.1111/j.1467-9248.1992.tb01384.x>; Etzioni, "Communitarianism."

⁶¹¹ M. Castells, "The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance," *The ANNALS of the American Academy of Political and Social Science* 616, no. March (2008): 78–93, <https://doi.org/10.1177/0002716207311877>; Christoph Bertram, "Globalization Means Westernization by Christoph Bertram - Project Syndicate," Project Syndicate, 1998, <https://www.project-syndicate.org/commentary/globalization-means-westernization?barrier=accessreg>.

Concluding this part of the chapter, I believe that the above juxtaposition of Lipset on one side and the communitarians/Grabb et al. on the other, provides an understanding of the role individualism plays, not just in the cultural heritage of the United States, but in contemporary, Western society. We may find ourselves in a time when the concept of individual freedom is being used by both gun rights activists on the political right and privacy advocates on the left to fight for their causes, but there seems to be a strong case that an absolutist belief in freedom rights is not socioculturally or historically rooted in the U.S. In fact, the opposite may be the case. As both neo-communitarians and Grabb et al. argue, and Lipset also acknowledges in his work, the liberty tradition in the U.S. has always been accompanied by a tradition of *restricting* liberties. It could be argued that this presents that difference of “American exceptionalism” between the U.S. and other nations; i.e. the U.S. was built from a position of complete, individual liberty from which it then restricts freedoms according to necessity for social order, whereas other Western nations have emerged from monarchies and other restrictive state systems and into liberal democracies like the U.S. The U.S. have traversed a path of adding a minimum of liberty restrictions, the path of other nations is one where restrictions are lifted. However, as Grabb et al. argue, the path seems to have led to roughly the same destination, with only minor differences.

Though an ideal of optimizing the individual’s freedom may exist in the U.S., there is also an understanding of why this freedom cannot be total and absolute, in respect of others and the surrounding community. This is important when entering into a Rawlsian discourse, as I will proceed to do below, as Rawls’ entire set of ethics is contingent upon this notion. A view from

30,000 ft would show that Rawls is primarily concerned with *how* liberty can be limited in a fair and just way.

The notion of the American “character” as focused on “local communalism” helps us understand how a dual policy like the one analyzed here can emerge in spite of the freedom ideals that are purportedly held so high in American culture. Most importantly, the historical/cultural background provided above also makes it clear that the concept of extreme individualism observable in movements such as the right-wing Tea Party⁶¹² and Libertarian discourses is a relatively recent phenomenon, finding widespread popularity around the election of Ronald Reagan in 1980, after having percolated in some right-of-center intellectual circles (such as those surrounding Ayn Rand and Milton Friedman⁶¹³) for a few decades. In the almost two and half centuries since the United States was founded, the period in which this unrestricted freedom notion was popular may be as parenthetical as Mao’s attempt to get China to reject more than 2,000 years of Confucianism (see Chapter 4).

Extreme communitarianism as cultural background for policy

To put it another way: The emergence of a privacy-breaching, and thereby freedom-limiting, dual policy as described in the Rhetorical and Action Frames above may signal a future abandoning of the absolutist freedom and liberty values introduced alongside neoliberalism (as

⁶¹² Lauren Langman, “Cycles of Contention: The Rise and Fall of the Tea Party,” *Critical Sociology* 38, no. 4: 469–94, accessed March 18, 2018, <https://doi.org/10.1177/0896920511430865>.

⁶¹³ Gene H. Bell-Villada, “Who Is John Galt? Ayn Rand, Libertarians and the GOP,” *The Conversation*, 2015, <http://theconversation.com/who-is-john-galt-ayn-rand-libertarians-and-the-gop-40033>.

we currently understand that term), and that may be a result of a communitarianism run amok. By the latter, I mean the counter-reaction to globalization that has fueled the rise of the populist/nationalist movements in Europe and is at the heart of “Trumpism”. The rhetoric of the leaders heading up the movement in different European nations all have in common the nostalgia for a (selectively remembered or completely imagined) past when communities were smaller, more homogenous, more tribal.⁶¹⁴ This also fueled the Trump campaign in 2016, most visible in the official campaign slogan, “Make America Great Again”.

The rise in privacy breaches and freedom restrictions identified by the ACLU and EFF above due to the dual policy analyzed here is perhaps not really in conflict with any deeply-rooted individualism. Rather, there has been swing of the freedom pendulum: The absolutist liberty values introduced during the rise of neoliberalism, culminating in the Ronald Reagan presidency, was first compromised by the 9/11 attacks and the legislation that followed in their wake as outlined above. That the freedom pendulum has swung even further in the other direction, may reflect that what *actually* characterizes the United States, “local communalism”, has been inflated into tribalism by the political rhetoric and strategies of the Trump administration, inspired by their European counterparts. Seen through this lens, it makes complete sense how policies allowing for expanded border searches of electronic devices and registration of social media handles belonging to U.S. citizens can emerge in a country which not

⁶¹⁴ Jens Rydgren, “Explaining the Emergence of Radical Right-Wing Populist Parties: The Case of Denmark,” *West European Politics* 27, no. 3 (May 2004): 474–502, <https://doi.org/10.1080/0140238042000228103>; Cas Mudde, “The Populist Radical Right: A Pathological Normalcy,” *West European Politics* 33, no. 6 (November 20, 2010): 1167–86, <https://doi.org/10.1080/01402382.2010.508901>; Reinhard Heinisch, “Success in Opposition – Failure in Government: Explaining the Performance of Right-Wing Populist Parties in Public Office,” *West European Politics* 26, no. 3 (July 2003): 91–130, <https://doi.org/10.1080/01402380312331280608>.

too long ago was described as “exceptional” because it was founded on principles of freedom and privacy rights.

Absolutist liberty principles have thus been shown to be unsustainable in the long run, first by 9/11 and the Patriot act, and second by the policies analyzed here. But on the other hand, as shown above, organizations and activists also make a credible claim that these policies are unsustainable because they infringe on citizens’ rights. To move towards a more sustainable situation now that the cultural background has been established, I will proceed to examine the dual policy by contrasting and comparing with the Rawlsian Frame.

The DHS and the Rawlsian Frame

Utilitarianism as paternalism in policy

The most thorough and complete work on Rawlsian approaches to the relationship between government and citizen in terms of information-gathering and surveillance was done by Michelle Louise Atkin in her book *Balancing Liberty and Security*, based on her Ph.D. dissertation.

Applying an ethical analysis to three policies during the George W. Bush administration from 2001 to 2009, Atkin shows how the administration’s arguments for restriction of liberty through the Patriot and Homeland Security acts can be viewed as exercises in application of utilitarian ethics. I argue that these freedom restrictions can be seen as analogue to the dual policy under analysis here, or perhaps even as predecessors to current policies, especially because of the utilitarian approach taken in both cases. Atkin’s findings are therefore also useful in the present analysis.

The arguments made for the Patriot act by the Bush administration, which in a Frame Reflection analysis would have belonged under the Rhetorical frame, take a consequentialist approach to the public good and the prevention of harm, i.e. the most important objective is to make the consequences of the policies as beneficial to as many people as possible, even if that means sacrificing the rights of or preventing less harm for the few. As Atkin shows, this utilitarianism is so classic, that it is enshrined in John Stuart Mill's liberty principle:

... the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others...⁶¹⁵

Atkin shows that the application of Mill's liberty principle is not sustainable, simply because its application to the Patriot Act is inconsistent and without consideration of all the consequences:

The pro-Patriot Act response seemed to be that the only way to ensure the security of the majority was to curtail the freedom of some, or perhaps even all of the members of the community. That said, it was also possible to use the liberty principle against the Act, using a form of proportionality test. For example, if the outcomes of the Act resulted in (a) an excessive curtailment of liberty, relative to the threat it responded to, or (b) the curtailments of freedom involved in the Act were ineffective in protecting the community

⁶¹⁵ John Stuart Mill, "On Liberty by John Stuart Mill," *Search* 111, no. 3 (1867): 22, <https://doi.org/10.1037/12289-000>.

from genuine danger, one could use Mill's liberty principle to argue that the harms of the Act outweighed the (potential) benefits.⁶¹⁶

Schlanger agrees that such a utilitarian argument has practical difficulties in terms of evaluation of the consequences:

I think people often see the tension between privacy and security where there really isn't one. Where the security that's being bought is phony. It's a semblance of security, it's security theatre, rather than being real...to decide in advance how many "units of security" one buys or how many "units of privacy", I think is a meaningless question.⁶¹⁷

Atkin also shows that the arguments for the Patriot Act's limitations of freedom took on a paternalistic tone, as she shows through this quote from then-Attorney General John Ashcroft, testifying in front of the Senate Committee on the Judiciary about the Patriot Act: "To those who scare peace-loving people with phantoms of lost liberty, my message is this: your tactics only aid terrorists, for they erode our national unity and diminish our resolve. They give ammunition to America's enemies, and pause to America's friends."⁶¹⁸

⁶¹⁶ Michelle Louise Atkin, *Balancing Liberty and Security: An Ethical Study of US Foreign Intelligence Surveillance, 2001-2009*, vol. 15 (Rowman & Littlefield Publishers, 2013), 34.

⁶¹⁷ Schlanger, "Interview, March 15 2018."

⁶¹⁸ John Ashcroft, "Testimony of Attorney General John Ashcroft Senate Committee on the Judiciary 12-06-01" (Justice.gov, 2001), <https://www.justice.gov/archive/ag/testimony/2001/1206transcriptsenatejudiciarycommittee.htm>.

This rejection of any argument that might question the act was one way the Bush administration acted paternalistically. Another was the insistence that Americans should simply take the government's word for it when they said that the good outweighed the bad when the consequences of the post-9/11 measures were considered. Due to the classified nature of the results of these measures, it was impossible to assess their utility, thereby making a utilitarian argument difficult – unless you blindly trust the administration's word that the measures are, in fact, beneficial to more people than they are detrimental to. In a section analyzing the NSA's Terrorist Surveillance Program (TSP), Atkin writes that in wartime, giving the president increased abilities to circumvent the basic structure may be justified under a Rawlsian approach, but "this argument is harder to defend in a perpetual war on terror where the threat level is increasingly difficult to measure and relies on a paternalistic, 'trust us,' approach to information sharing."⁶¹⁹

As mentioned, the policies analyzed by Atkin's can easily be substituted by the dual DHS policies considered in this chapter. The ACLU/EFF lawsuit shows that device searches at the border have been implemented without any documentation of how they comply with the Fourth Amendment. Though the DHS has been transparent about the fact that employees from different agencies search devices at the border, and also about the extent to which it happens, it is not clear what kind of personal information is being looked at, registered or used to make determinations about the admittance of the person trying to enter the country. Not even U.S. citizens have any recourse against the search and the consequences it can have if they refuse to comply, which is

⁶¹⁹ Atkin, *Balancing Liberty and Security: An Ethical Study of US Foreign Intelligence Surveillance, 2001-2009*, 15:52–53.

made clear in the ACLU/EFF lawsuit. The same goes for naturalized U.S. citizens whose social media information is being registered in their A-file at the USCIS. It may be, as Margo Schlanger points out, simply a matter of not purging the information collected in the immigration or visa processes, but even so, the individual has no control over what is collected, no insight into how the information is being used and can only view their A-file through a FOIA request.⁶²⁰ The paternalistic “trust us” tone used by those who defended the Patriot Act is also apparent in the USA Today op-ed quoted in the Rhetorical frame above. Acting general counsel Joseph B. Maher wrote that

These electronic media searches have produced information used to combat terrorism, violations of export controls, and convictions for child pornography, intellectual property rights violations and visa fraud...Department of Homeland Security officers and agents are the nation’s front line against threats to our safety and prosperity.⁶²¹

This quote, like Ashcroft’s above, not only demands that readers believe the DHS when it states that the searches are effective, the latter part of the quote both takes on a defensive stance, assuming that the readers are skeptical towards DHS officers and agents and claims that no other mechanisms than those put in by the DHS can protect “against threats to our safety and prosperity” at the “front line”. Tools from the international diplomacy toolbox such as economic sanctions against individuals or cooperation with international law enforcement is apparently not

⁶²⁰ USCIS, “A-Files Numbered Below 8 Million,” USCIS.gov, 2018, <https://www.uscis.gov/history-and-genealogy/genealogy/files-numbered-below-8-million>.

⁶²¹ Maher, “DHS: Device Searches Improve Safety.”

worth considering, according to Maher. The 'trust us' paternalism is also evident in both the title and sub-title of his op-ed, "DHS: Device searches improve safety" and "U.S. Customs and Border Protection exercises this authority judiciously." The latter is extracted from the op-ed itself: "This authority is critical to our mission, and Customs exercises it judiciously...Our actions are consistent with our responsibilities to protect the homeland, enforce the law at our borders, and follow our oath to uphold our Constitution."⁶²² In other words, accountability measures that could justify the utilitarian argument are replaced by an insistence on opacity and "trust us" paternalism as defined by Atkin. This is echoed by Schlanger, who believes the DHS shares – although to a lesser extent – a tendency towards 'intelligence legalism' with the NSA. Schlanger defines this concept as the attempt by intelligence-driven agencies to act according to what they believe can be achieved by stretching legal boundaries as far as possible, rather than what is appropriate or good. Unfortunately, the reason why this happens at a lesser degree at the DHS may be worrying, rather than comforting:

I think it's present, but I think it might be less present than it is at the NSA because there's much less legal regulation of what goes on at the DHS. The legality question is much less salient at the DHS than at the NSA. There's no FISA process, so the involvement of courts, which is really crucial at the NSA, is absent at DHS.⁶²³

⁶²² Maher.

⁶²³ Schlanger, "Interview, March 15 2018."

This lesser involvement of the courts points to the perception that DHS needs less judicial oversight, which again can be viewed as what Atkin calls “trust us” paternalism.

In the chapter on China, I examined Rawls’ views on paternalism, and how he states that it can only be permissible in government, if it is the result of a free and informed choice by the individual. The dual DHS policy analyzed here conforms to neither of those conditions. One thing is that the individual is kept from obtaining all the information required to make the choice, but more importantly, these policies are simply imposed on the individual if that person wishes to return to their home and property, thereby exercising their human rights. To put it another way, exercising your human rights are conditioned by the compliance with these policies, and Rawls would not consider that a choice made freely.

It can be argued, however, that the U.S. is a “well-ordered society” in Rawlsian terms, and it is possible for U.S. citizens to vote out the representatives who support these policies. After all, the border searches began under the Obama administration, and it is a strong argument that if voters had wished for different policies to be enacted, they likely wouldn’t have elected Donald Trump as president. The question then becomes one of whether Rawls would actually accept the current electoral system in the U.S. as fair and just, given the amount of money that can now be spent by election campaigns after the *Citizens United* Supreme Court decision, the so-called “gerrymandering”/redistricting efforts taking place, as well as some states’ attempts at what some view as voter suppression.⁶²⁴ But this discussion is a much larger one that falls outside the scope of this dissertation.

⁶²⁴ Andrew Gumbel, “America’s Shameful History of Voter Suppression,” *The Guardian*, 2017, <https://www.theguardian.com/us-news/2017/sep/13/america-history-voter-suppression-donald-trump-election-fraud>;

The DHS' newest directive on border searches now requires reasonable suspicion to be present, before a border agent can search an individual's phone and e.g. collect or view social media information. However, there is no requirement that the suspicion be disclosed to the individual before the search takes place, and the individual still has no recourse. The individual cannot, for example, alleviate the border agent's suspicion through other means before a device search takes place.

Paternalism aside, the conflict between the Rhetorical and Action frames on one side and the Rawlsian frame on the other, boils down to a question of Rawls' view on protection of privacy rights overall. Since Rawls is not an absolutist when it comes to liberty (as can be seen in his debates with his friend Robert Nozick who was more of an absolutist), where on the spectrum between absolute freedom and government control does he draw the line and find the balance?

Rawls and privacy

According to some scholars, Rawls did not dedicate much effort directly to the matter of privacy.⁶²⁵ Attempts have been made, however, to extract a Rawlsian approach to privacy from other parts of Rawls' work. Annabelle Lever⁶²⁶ argues that Rawls' view of a right to privacy can be found through an examination of Rawls' thoughts on property ownership. She first argues,

ACLU, "Fighting Voter Suppression | American Civil Liberties Union," ACLU.org, 2018, <https://www.aclu.org/issues/voting-rights/fighting-voter-suppression>.

⁶²⁵ Annabelle Lever, "Privacy, Private Property, and Collective Property," *The Good Society* 21, no. 1 (2012): 47–60; James W Nickel, "Rethinking Rawls's Theory of Liberty and Rights," *Chi.-Kent L. Rev.* 69 (1993): 763.

⁶²⁶ Lever, "Privacy, Private Property, and Collective Property."

with references to Judith Thomson⁶²⁷ that although an invasion of privacy can often also be seen as a violation of property ownership (You own and control e.g. your body and your home and thus if anyone looks at your body within your home, it is a violation of you rights as a property-owner), it is not always the case. Hence, and after other deliberations, she concludes, “Because people’s claims to privacy cannot be reduced to claims of property ownership, a property-owning democracy will likely need distinctive ways to protect privacy.”⁶²⁸ In this way, which is also evident from a list of assumptions Lever makes in the introduction of the article in question, she argues that if one accepts the conditions of Rawls’ concept of a property-owning democracy, then one must also accept that privacy rights must be protected by the same basic structure that constitutes the property-owning democracy.

A similar conclusion is reached through other means of deliberation by Introna⁶²⁹ in an article discussing workplace surveillance. In the modern workplace, Introna argues, the person is subject to surveillance through data collection, which may be conducted for work optimization reasons, but ends up being a violation of the person’s privacy rights. Introna does not deny the value of data collection nor does he pass a normative judgment on the actual practice of workplace surveillance: “...The conflict between the individual right to privacy and the institutional right to transparency will always be there”.⁶³⁰ She suggests the use of Rawls’

⁶²⁷ Judith Jarvis Thomson, “The Right to Privacy,” in *Philosophical Dimensions of Privacy: An Anthology*, 1984, 272–89, <https://doi.org/10.1017/CBO9780511625138.012>.

⁶²⁸ Lever, “Privacy, Private Property, and Collective Property,” 7.

⁶²⁹ Introna, “Workplace Surveillance, Privacy and Distributive Justice.”

⁶³⁰ Introna, 38.

“Difference principle” as a guide for putting in place practices that can balance an organization’s need for transparency and optimization through the collection of data and the privacy rights of an individual. The difference principle states that societal inequalities are inherently unjust, unless they are in place to improve conditions for those members of society who are worst-off.

Similarly, in the case of workplace surveillance, Introna argues that “Based on the ‘difference principle’ it will be up to the collective (employer) to justify the collection of particular data in particular contexts. Furthermore, that the regimes for controlling the collected data should be biased towards the individual”.⁶³¹ To put it simply, Introna uses to Rawls to assert that the asymmetrical power relationship between employer and employee should be reflected inversely in the implementation and control of data collection in the workplace. However, it can be argued that the difference between the role of the citizen and the role of the employee are so different in nature that it may impact the validity of applying the difference principle as Introna does.

Workplaces are not well-ordered societies, nor are they necessarily democratic in nature, and there is no expectation of sharing or distribution of power.

James Nickel⁶³² argues that one can read privacy rights into Rawls’ idea of the liberty of a “person” or “citizen”. Nickel synthesizes the privacy rights from some of the basic liberties that Rawls presents in *A Theory of Justice* and *Political Liberalism*, such as the liberty of conscience and freedom of thought as well as the freedom and integrity of the person.⁶³³

⁶³¹ Introna, 38.

⁶³² Nickel, “Rethinking Rawls’s Theory of Liberty and Rights.”

⁶³³ Rawls, *Political Liberalism*; Rawls, “A Theory of Justice.”

Like Lever, Nickel seems to make the assumption that Rawls thought of privacy as being inherent in the liberty of the person and freedom of thought, as he compares Rawls' principles with the bills of rights found in many constitutionally-based democracies in the world: "Contemporary bills of rights usually covers matters of lifestyle with the following rights: (1) privacy – no arbitrary interference with family, home or correspondence..."⁶³⁴ He then continues to name five other areas of individual liberty and then asserts that "One possible strategy for Rawls to use here would be to say that these six specific liberties are all included in his third category, "liberty of the person"..."⁶³⁵ Nickel presents his own interpretation and enhancement of Rawls' basic rights and liberties in the article, and although these are both compelling and useful, I shall not enter into a discussion of them here.

Lever, Nickel and Introna all wish to fill the gap that they believe Rawls seemingly advertently left in his work on the issue of privacy. However, I believe, and will argue for in the following, that Rawls very purposefully did not engage in a discussion of privacy rights for reasons that are integral to his understanding of a well-ordered society. Let me begin with the idea put forward by Nickel that privacy is part of the liberty of the person. Rawls reminds us that his view of the free citizen is limited to the political concept of justice as fairness. In this regard, he does not concern himself with individual freedom at higher levels of abstraction:

In what sense are citizens free? Here again we must keep in mind that justice as fairness is a political conception of justice for a democratic society. The relevant meaning of free persons is

⁶³⁴ Nickel, "Rethinking Rawls's Theory of Liberty and Rights," 770.

⁶³⁵ Nickel, 770.

to be drawn from the political culture of such a society and may have little or no connection, for example, with freedom of the will as discussed in the philosophy of mind.⁶³⁶

In fact, Rawls subordinates the freedom of the citizen to the basic structure of society, which was one of his friend and colleague Robert Nozick's biggest objections to Rawls' entire conception of society.⁶³⁷ In further exploration of this, one can begin with his notion that a citizen is free because the citizen is able to form, acquire or revise their own individual perception of the good:

First, citizens are free in that they conceive of themselves and of one another as having the moral power to have a conception of the good. This is not to say that, as part of their political conception, they view themselves as inevitably tied to the pursuit of the particular conception of the good which they affirm at any given time. Rather, as citizens, they are seen as capable of revising and changing this conception on reasonable and rational grounds, and they may do this if they desire.⁶³⁸

This Socratic view is Rawls' view of how the citizen is shaped by the freedom of thought. It is separate, however, from the citizen's political freedom, which is both protective of the person's freedom of thought, but also puts limitations on this right. In Rawls' view, it is exactly the

⁶³⁶ Rawls, *Justice as Fairness: A Restatement*, 21.

⁶³⁷ Nozick, *Anarchy, State, and Utopia*.

⁶³⁸ Rawls, *Justice as Fairness: A Restatement*, 21.

separation of a citizen's freedom of thought and of mind from his or her political freedom that secures the former:

For example, when citizens convert from one religion to another, or no longer affirm an established religious faith, they do not cease to be, for questions of political justice, the same persons they were before. There is no loss of what we may call their public, or legal, identity – their identity as a matter of basic law.⁶³⁹

A citizen in Rawls' justice of fairness concept is, in other words, a citizen in the political sense, not in the sense that one is a person with freedom of thought. Within Rawls' basic structure of society, basic liberties and rights are secured for the citizen in the political sense, not in the more abstract sense. Thus, Rawls' concept of justice as fairness requires citizens to be engaged in social cooperation. He sees the social cooperation of citizens as intrinsic to the construction of a society ruled by fair justice, and defines two 'moral powers' by which citizens can express this social cooperation:

- (i) One such power is the capacity for a sense of justice: It is the capacity to understand, to apply and to act from (and not merely in accordance with) the principles of political justice that specify the fair terms of social cooperation.
- (ii) The other moral power is a capacity for a conception of the good: it is the capacity to have, to revise and rationally to pursue a conception of the good. Such a conception is an ordered family of final ends and aims which specifies a person's conception of what is

⁶³⁹ Rawls, 21–22.

of value in human life or, alternatively of what is regarded as a fully worthwhile life. The elements of such a conception are normally set within, and interpreted by, certain comprehensive religious, philosophical or moral doctrines in the light of which the various ends and aims are ordered and understood.⁶⁴⁰

Rawls adds that in possessing these two moral powers, persons have "the requisite capacities not only to engage in mutually beneficial social cooperation over a complete life but also to be moved to honor its fair terms for their own sake".⁶⁴¹ While Rawls sees the ability to engage in social cooperation as a moral power, he is not claiming that justice as fairness is a moral doctrine, nor a path towards ethics: "Justice as fairness is a political conception of justice: that is, it is designed for the special case of the basic structure of society and is not intended as a comprehensive moral doctrine".⁶⁴² This translates into his view of citizens' autonomy. Rawls suggests that the full autonomy of a person is achieved on a political level, not an ethical one: "This full autonomy of political life must be distinguished from the ethical values of autonomy and individuality, which may apply to the whole of life, both social and individual, as expressed by the comprehensive liberalism of Kant and Mill".⁶⁴³ In other words, the full autonomy and individual freedom he considers in the justice as fairness concept is autonomy within the

⁶⁴⁰ Rawls, 18.

⁶⁴¹ Rawls, 18.

⁶⁴² Rawls, 19.

⁶⁴³ Rawls, *Political Liberalism*, 78.

confines of the social contract, the fair terms of social cooperation agreed upon from the original position. A person can subscribe to the ethics of full autonomy and individual liberty or not, but if the person is to engage in the social cooperation defined in the social contract, he or she must assert the two moral powers isolated from these ethics.

Rawls thus separates what members of a just society must do to construct that same society from a position of justice and fairness. This is a political mission. As mentioned above, a person can still be beholden to a set of ethics that is separate, but to act morally within a just society based on fair terms of social cooperation, the person must pursue the political mission, even if it is in opposition to the set of ethics by which the person defines the good. In Rawls' view, the two are not incompatible, as Rawls argues for an ethical liberalism alongside political liberalism. But, as an example, according to Rawls, a person who is against abortion for ethical reasons would be acting immorally if he or she were to express his or her autonomy in ways that are contrary to the fair terms of social cooperation. In a well-ordered society, in other words, Rawls sees it as immoral to, say, resort to violence to express one's autonomy and ethical norms, if violence is not understood in the social contract as a valid method of social cooperation. In fact, according to Rawls, a citizen cannot act with full autonomy unless the citizen acts in accordance with and in full understanding of the principles of justice agreed upon from the original position in construction of the social contract: "When the principles of justice which are adopted by the parties are affirmed and acted upon by equal citizens in society, citizens then act with full autonomy"⁶⁴⁴

⁶⁴⁴ Rawls, 305.

Rawls extends the separation of ethical and political norms to the representatives of the citizens who deliberate in e.g. a democratic, parliamentary setting:

The parties in the original position are as rational representatives, rationally autonomous in two respects. First, in their deliberations they are not required to apply, or to be guided by, any prior or antecedent principles of right and justice. Second, in arriving at an agreement on which principles of justice to adopt from the alternatives available, the parties are to be guided solely by what they think is for the determinate good of the persons they represent, so far as the limits on information allow them to determine this.⁶⁴⁵

The last line is crucial. Rawls clearly acknowledges that limitations on information can exist, but that they can also be a determinant of what representatives deem as “good” for those they represent. Here, we see again how Rawls views the access to information as essential to the fair and just decision-making within democratic process, not just at the citizen level, but also at the representative level. When policies are put in place that inhibit access to information such as the policies addressed here, they can also inhibit the citizens’ ability to act according to their democratic values and express their capacity for good.

A well-ordered society is not private

Based on the above, political conception of the person as a citizen in a society founded on justice as fairness, I find it hard to accept Nickel’s insertion of the privacy element in a reading of Rawls’ basic liberties of the person. Rawls is specific in his definition of the citizen as a political

⁶⁴⁵ Rawls, 307.

entity and thereby part of a greater whole, and thus inevitably not a totally autonomous individual. Full autonomy can only be achieved when acting in accordance with the principles of justice agreed upon by the collective in the original position in Rawls' view. Rawls actually directly emphasizes that privacy is not a part of the basic structure, and that any claims to privacy rights are secondary to the social cooperation which constitutes a fair and just society. He does so in this definition of his "well-ordered society":

... to say a society is well-ordered by a conception of justice means three things: a) that it is a society in which everyone accepts, and knows that everyone else accepts and publicly endorses, the very same principles of justice; b) that its basic structure – its main political and social institutions and how they hang together as one system of cooperation – is publicly known, or with good reason believed to satisfy those principles; and c) that citizens have a normally effective sense of the principle of justice, that is, one that enables them to understand and to apply the principles of justice, and for the most part to act from them as their circumstances require⁶⁴⁶

Rawls follows this definition with two specific statements which are important to understanding how he stresses that social unity must take precedent over individual privacy in a well-ordered society. First, he states that a well-ordered society, in which everyone acknowledges, accepts and lives by the agreed-upon principles of justice, is a normative preference: "I believe that social unity so understood is the most desirable conception of unity available to us; it is the limit of the

⁶⁴⁶ Rawls, *Justice as Fairness: A Restatement*, 201–2.

practical best.”⁶⁴⁷ And then, he states more directly his (lower) prioritization of privacy within the well-ordered society: “A well-ordered society, as thus specified, is not, then, a *private* society; for in the well-ordered society of justice as fairness, citizens do have final ends in common”⁶⁴⁸ (emphasis mine).

This, in my view, invalidates the claims of Lever and Introna that Rawls’ theory of justice can be, respectively, used as an argument for an intrinsic protection of privacy rights in the basic structure of society, or used as a method to achieve fairness in workplace surveillance. Introna’s claim that the Difference principle can be used to determine the regulation and methods of data collection in the workplace may be valid. But Rawls’ concept of a well-ordered society based on justice as fairness cannot be used as a model for privacy protection in the workplace, because the individual’s privacy is subordinate to the principles of justice upheld by social cooperation. Could the right to privacy be considered a principle of justice that should be part of the basic structure, agreed upon in the original position by the parties? It could indeed. But the question then becomes one of degrees. How far does one’s right to privacy go?

I would argue, based on what I have shown above, that Rawls’ well-ordered society could never allow for an amount of privacy that is detrimental to others’ ability to exercise their moral powers. This would be an infringement of several Rawlsian principles, not least the two principles of Justice as Fairness. If one person’s privacy claims inhibit another person’s acting with full autonomy (and thereby in accordance with the basic principles agreed upon by all), I

⁶⁴⁷ Rawls, 202.

⁶⁴⁸ Rawls, 202.

would argue that Rawls would let the privacy claims take a back seat to the other person's right to full autonomy. In fact, it is doubtful whether the parties constructing the basic structure in the original position would even allow for such privacy rights. After all, privacy rights are always given in relation to something. One has the right to keep secrets from...others, the government, one's employer, corporations etc. These are all instances the veil of ignorance was put in place to eliminate from the discussion of the basic structure. In other words, it is possible to allow for privacy claims within a Rawlsian framework, but the basic principles of a well-ordered society will always take preference over those rights to privacy.

Does this impede upon the ideal of intellectual freedom as discussed earlier in the chapter? Does Rawls' acknowledgement of social cooperation outranking privacy stand in contradiction of intellectual freedom as it is discussed by the ALA and Richards above? I think not. The mission of the library system has never been to grant access to *all* information in existence, quite the contrary. Information professionals and librarians "significantly influence or control the selection, organization, preservation, and dissemination of information", as the ALA Code of Ethics states.⁶⁴⁹ It is a mission of curation with significant ethical considerations in the selection process. While the mission certainly entails making subversive information available to those who wish to study it, it would also be against the ALA Code of Ethics to engage in activities that may break social cooperation in society. Such an effort would per definition be political, in the interest of one or a few individuals, rather than society as a whole, and this is a violation of

⁶⁴⁹ ALA, "Code of Ethics of the American Library Association."

principle VI and VII of the ALA Code of Ethics, which prohibit the advancing of private interests or personal convictions.

Richards also acknowledges that “surveillance can sometimes be necessary, even helpful”, but that it “must be constrained by legal and social rules”.⁶⁵⁰ This is an echo of Rawls’ principles. It is not so much a question of *whether* there must be limitations on privacy in the name of social cooperation, but *how* those limitations are agreed upon and implemented. For Rawls, intellectual freedom exists within the same boundaries as all other freedoms: It can only be restricted if the result is that citizens gain more freedom to express their capacity for good, thereby cooperating socially. It can even be argued that the ethical curation and selection of information that is central to the mission of any information professional is precisely a limitation that facilitates greater intellectual freedom. As scholars such as Bawden and Robinson have shown, the availability of too much information tends to limit the overall value of said information as overload sets in. It is through the processes of sorting, organizing and selecting – all limitations in some form or another – that information achieves its emancipatory qualities. Intellectual freedom is not impeded by limits constructed and imposed in ways that society regards as fair and just per Rawls. Intellectual freedom is *enabled* by those restrictions.

⁶⁵⁰ Richards, “The Dangers of Surveillance,” 1964.

When and how privacy rights should be surrendered

With the determination that Rawls will always put the basic principles of a well-ordered society above the individual's privacy rights, is it fair to conclude that Rawls would approve of the DHS policies analyzed here? I do not believe so. I believe Rawls would see them as going too far in the other direction.

Although Rawls does not view liberty and privacy as absolute and would likely (as Atkin also points out above) approve of some restrictions of liberty at the border to uphold national security, the dual DHS policy fails to live up to Rawlsian criteria with regards to how it was constructed and implemented. It is the process by which it came about that makes it unethical, not necessarily the policy itself. For Rawls, as I have shown in this last section, any type of privacy – including that pertaining to property – can be limited by government, as long as this:

- A. Does not happen in violation of human rights
- B. Happens within the confines of a well-ordered society
- C. Happens with the consent of the citizens through a transparent process
- D. Does not reduce individual liberty unnecessarily or without reason
- E. Does not impede the methods of social cooperation determined in basic structure of the given society, constructed fairly and according to Rawlsian criteria, or any constitution of law agreed upon under the same conditions.

However, as described above, several of these rules were broken during the making of these policies. With regard to A., some have argued that the border searches may be a human rights violation, since privacy is protected in the U.N. Declaration of Human Rights under article

12.⁶⁵¹With regards to C., though both the Obama and Trump administrations were elected by population who consented to their policies, i.e. also to the dual policy in question, the actual policy construction and implementation happened without much consultation of the population. The new A-file policy was, as a DHS spokesperson told journalist Matt Novak above, enacted before it was actually put into law. When the latter happened, it was as an unannounced notice in the Federal Register, and the population were given 30 days to consider the consequences of the policy and file a complaint. Although this can to some extent be seen as complying with a principle of transparency, it is important to remember the environment in which this occurred: A society suffering from information overload, with citizens being exposed to new information at an exponentially higher rate than when Rawls was alive. At the same time, since this is a policy that relates to the personal lives of immigrants and already naturalized U.S. citizens, it does not seem sufficient to place a notice in a somewhat (for citizens) obscure government journal, as it can be argued that this is similar to not disclosing it at all. So even if the DHS had not already implemented the policy before making it public, their announcement of it was clearly insufficient. The process was anything but transparent.

With regards to D., I have shown that, just as in the case of the Patriot Act, the argument for this dual policy presented by the DHS was a utilitarian one. Rawls' general arguments against utilitarianism (as laid out in chapter 2) apply, of course. But even setting those aside, the utilitarian approach in this case was so extreme that it essentially turned into a paternalism that

⁶⁵¹ McFadden et al., "American Citizens: U.S. Border Agents Can Search Your Cellphone"; United Nations, "Universal Declaration of Human Rights | United Nations"; Coalition, "Coalition Letter Opposing DHS Social Media Retention | Center for Democracy & Technology," cdt.org, 2017, <https://cdt.org/insight/coalition-letter-opposing-dhs-social-media-retention/>.

was forced upon the population, rather than chosen by it. In other words, no reason or substantial evidence of effectiveness was given to justify the limitations on privacy and liberty imposed by the dual policy, and as such, it violates Rawlsian principles.

With regards to E., the ACLU and EFF argue that the border searches of electronic devices are unconstitutional, and if the courts agree, it can be seen as a violation of Rawlsian principles, if it is assumed the U.S. constitution is accepted by U.S. citizens as a document worth adhering to. But even if this is not the case, the dual policy is still in violation of E. As I have argued elsewhere⁶⁵², and also referenced above, Rawls allows for invasions of individual privacy if inhibiting those invasions would lead to a breakdown of the social cooperation inherent in the basic structure. But this has to happen according to Rawlsian principles of citizens' rights, which includes universal applicability. Particularly now that the "suspicion" condition has been entered into the policy of electronic device border searches, it is clear that not everyone will be subject to the searches. The in its most recent CBP directive on border searches, the DHS has not defined very clearly what "reasonable suspicion" means or what can cause it. It merely states:

Many factors may create reasonable suspicion or constitute a national security concern; examples include the existence of a relevant national security-related lookout in combination with other articulable factors as appropriate, or the presence of an individual on a government-operated and government-vetted terrorist watch list.⁶⁵³

⁶⁵² Bay, "The Ethics of Unbreakable Encryption: Rawlsian Privacy and the San Bernardino iPhone."

⁶⁵³ U.S. Customs and Border Protection, "Border Search of Electronic Devices," Pub. L. No. CBP Directive No. 3340-049A (2018), 5, <https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf>.

To reiterate, “suspicion” is only necessary to perform an advanced search. A basic search can be done with or without suspicion: “In the course of a basic search, with or without suspicion, an Officer may examine an electronic device and may review and analyze information encountered at the border, subject to the requirements and limitations provided herein and applicable law.”⁶⁵⁴

To put it another way, any CBP officer can request an inspection of an electronic device and require that it be unlocked by the user – or the password/code for it handed over to the officer⁶⁵⁵ - without having to account for the decision about whose devices are chosen for inspection. This widened authority with little accountability worries Schlanger, who points out that the CBP does not distinguish between directly border-related searches and searches that may have a broader law enforcement objective:

It seems to me that there are two kinds of border searches: There are border searches on matters that have a border nexus, and there are border searches where the authority to conduct a border search is being used because there is an occasion where searches are less regulated. I am much more troubled by that last category than I am by the first.

Searches that has to do with introduction of contraband across the border or admissibility it strikes me as less troubling than if the idea is “Wow we have this great moment where we have immense search authority, we’re going to take advantage of that. Our interest in you is actually not border-related, but you just happen to be here, so we’re going to use

⁶⁵⁴ U.S. Customs and Border Protection, 4.

⁶⁵⁵ U.S. Customs and Border Protection, 7.

that moment”. The CBP doesn’t really draw a distinction between the two, and I really think they should. That’s my position, that even things with a border nexus should be regulated in a way that perhaps they no longer are. It should not be available to the CBP to use the occasion of a border search to conduct law enforcement searches that it normally would need a warrant for.⁶⁵⁶

In the ACLU/EFF case, only three of the eleven plaintiffs are not people of color with Middle-eastern- or Indian- sounding names. Without accurate information about the persons who were subjected to these border searches, it is impossible to ascertain whether any type of selection bias is present. But the point is that such a selection bias need not even be present, just the fact that it is *possible* under the law to discriminate, makes it a violation of the Rawlsian principle of universal applicability. Rawls would argue that a law that can undermine its own universal applicability by being applied discriminatorily is unjust per definition. Furthermore, Rawls argues that decisions made about basic structures in society must be made based on fact and not on likelihood. That is, decisions are not to be made based on what the individuals in the original position *think* will happen, but what they *know* will happen. Schlanger describes this in a privacy/security context:

So, what you need is a process that reaches an acceptable balance...that has people with the right sort of commitments and the right sorts of knowledge and who really insists that

⁶⁵⁶ Schlanger, “Interview, March 15 2018.”

the security benefit be demonstrable, not just hypothetical, particularly when the privacy loss is demonstrable and not hypothetical.⁶⁵⁷

Chapter conclusion

To sum up: For the border search policy to be ethical in Rawlsian sense, it must not only be applied equally to all (e.g. with a randomized selection system if a search of all electronic devices is impractical), there must also be a general consensus that it will have the desired effect. Because of the way the policy was constructed and enacted, and because of the lack of a requirement to disclose its results, a general consensus cannot be achieved on the basis of the directive alone.

The same Rawlsian critiques apply to the USCIS policy of storing social media information and “search results”, and it clearly also violates E. It is not universally applicable, as all U.S. citizens are not subject to this type of information collection by the government, only naturalized U.S. citizens. In almost all other instances of U.S. law, a citizenship is a citizenship – but not in this one. Thus, again, the policy is justified through a utilitarian argument, which violates the equality principles inherent to Rawls’ theory of justice as fairness. It is definitely not based on a certainty of consequences, in fact it is based on the opposite: The USCIS are keeping the records because they *think* something might happen, rather than *knowing* it. In this case, as in the border search case, there’s no information available to evaluate the policy by, thus invalidating any utilitarian support argument.

⁶⁵⁷

Finally, the question remains whether all of these violations could be justified through a respect for the cultural background of the society in question, in this case the U.S.? As I put forth in the chapter on China, Rawls does allow exceptions to some of his principles in the case of burdened societies or societies whose cultural and historical background makes it disproportionately difficult for that society to become well-ordered. This is the reason I included a section on American individualism above. First, it is of course, ridiculous to consider the U.S. a burdened society, even if there might be severely burdened areas in the nation. The latter is the case because of political decisions, not natural disasters or the like. And as mentioned above, there's an argument to be had that the U.S. may no longer be well-ordered, but it certainly isn't its history or culture that has made it so, on the contrary. Though Lipset's "American Creed" may be focused on self-interest, and there may be more validity to the arguments against it, and that the U.S. really is a nation of small communities that hold the interest of the individual, both these positions are characterized by a historical commitment to democracy and equality of opportunity (and to an extent, to equality of result).

If the communitarianism-run-amok scenario described previously does have some explanatory power over the paradox between American ideals of freedom and the emergence of the dual policy studied here, it is just another argument against utilitarianism as foundation for policy-making, at least if liberty is a priority. If Mill's "civilized community" is a small, closed community, in which "preventing harm to others" is the only valid motivation for restricting liberty, how do you set the boundaries between what "harms" members inside the community or "others" on the outside? And does any harm done to a majority of "others" *outside* the community not overrule the harm done to a majority *inside* the community, according to the

principles of utilitarianism? Using utilitarianism as a foundation for policy-making in isolationist communities (which will almost always be embedded in larger communities, i.e. international alliances such as the UN, the EU or NATO) would be the equivalent of the white ruling class during the Apartheid era in South Africa claiming that any harm felt within their community would take precedent over any harm felt by the much larger, and oppressed, black community.

To put it another way: The core values of the United States may not be as rooted in individualism as Lipset claims. But if the “local communalism” described by Grabb et al. becomes an extreme communitarianism with a plurality of closed-off communities, any privacy-breaching policies such the dual social media policy studied here can be justified through un-universalized, utilitarian arguments.

Rawls’ work can be viewed as being in opposition to this, not least because the actual historical and cultural background of the U.S. was the foundation and inspiration for Rawls. He did not create his theory of justice in opposition to this foundation. Rawls’ theories emerged during a time when the Vietnam war, nationalist populism, racial tensions, violent uprisings and assassinations of political leaders and violent uprisings filled the public consciousness. The zeitgeist provided an important motive for Rawls to explore what justice really means in the modern era, and what a society built on justice and fairness would look like. The Nixon era, during which Rawls worked on and published *A Theory of Justice*, was a departure from the values described above as being solidly American, not a reinforcement of them. It is a similar departure that have fostered the dual policy analyzed in this chapter and is the main motivation for their inclusion in this dissertation.

Chapter 6: The Rawls Test – Discussion and Conclusion

One of the main contributions of this dissertation has to do with timeliness. As I showed in the literature review part of Chapter 2, very little literature had been published on the matters discussed here when work on this dissertation began. It is to be expected, however, that the events of 2015-2018 related to social media and national security will lead to much academic analysis and policy debate in the coming years, and this dissertation contributes both a historical and cultural background upon which analyses can be made and policy debates can be had. The findings presented here should also at least consolidate some positions from which further policy debate can flourish. Thus, the work that lies ahead on how social media should be regulated or what policies should be adopted in this regard, now has at least a partial foundation to build upon, instead of having to establish that first as part of the process. When I state that it is partial, it is because this dissertation shows how a contractarian position based on the work of John Rawls would be a very reasonable and productive starting point for the debate. Future studies may succeed in showing that, for example, a consequentialist/utilitarian approach, or a virtue ethics model could be equally useful.

Summary of findings and responses to research questions

To build the Rawlsian framework, I have used Schön and Rein's frame reflection policy analysis method to construct contextual policy frames that describe three different types of social media-oriented national security policies from three different nations. One uses foreign social

media offensives as national defense (Russia), one implements the strictly defensive national security strategies in social media (China) and one utilizes the collection of social media information as part of a larger national security strategy (U.S.). I have then compared these frames with the Rawlsian frame that was constructed as part of the literature review in Chapter 2.

National social media policies

The findings of these case study-based policy provide answers to the research questions that this study is designed to answer. Three of these questions can be answered by summing up the findings of each chapter:

- *What national security policies encompassing social media platforms exist at present in Russia, China and the US?*
- *What is the balance of state security measures versus citizens' rights in each of the three sets of policies and their implementation?*
- *To what extent do these existing policies reflect Rawls' conceptions of liberty, justice as fairness and the Law of Peoples?*

In chapter 3, I briefly gave an overview of Russian domestic policies regarding social media as part of the larger information strategy. I focused, however on Russia's foreign social media policy and how actors within the Russian Federation use social media as part of a larger disinformation campaign designed to influence other nations and promote Russian interests. I described how both strategically and tactically, the methods used are inspired by a long tradition of narratives, storytelling and deception as a virtue in Russian culture, and how disinformation methods were developed in the tsarist era, but skillfully honed to perfection by the KGB in the

20th century. From the interviews and the document analysis, it was evident that the difference between the KGB tactics of the 20th century and the ones employed today by the Russian Federation is the lack of ideology in the latter. Whereas the Soviet Union had an interest in promoting their ideological position in order to further their interests and garner support, the Russian Federation is strictly focused on strengthening their geopolitical power through the disruption of social cooperation and democratic processes of their counterparts and adversaries. To this end, I find, their policy of using social media as an instrument of information warfare has been largely successful. However, when held up against the Rawlsian frame, it becomes clear that it is difficult to defend the policy from an ethical standpoint. It is not universally applicable. It creates obstacles in the political discourse which disrupts the free flow of and access to the information needed to make an informed decision as a voter. And it is not a reciprocal approach in which respect and tolerance for other parties is a basis for cooperation. All of these are Rawlsian principles violated by Russia's offensive strategy on social media.

In Chapter 4, I described how China uses their national social media policy as a means of social control meant to ensure stability and national security. The chapter contains a description of China's "Golden Shield" program which blocks access to social media platforms outside China, prohibiting users from accessing information not approved by the government through these channels. I have described how Chinese government workers monitors social media for what the government considers undesirable opinions or sharing of unsanctioned information, and takes action to remove it or, as in the case of the "50 cent" workers, drown it in government-friendly utterances from what appears to be private citizens. I have also described how freedom of expression is oppressed in China, not just by the means I just mentioned, but also through

arrests and other legal sanctions targeting dissidents who voice their opinion on social media or attempt to use technology that might help them access foreign social media. These are violations of many Rawlsian principles, including the basic liberties (among others, freedom of speech, freedom of assembly, freedom of association and political liberties), as well as lack of consultation and violations of human rights. In the chapter, I also showed how these policies are aligned with both a tradition and millennia-old history of Confucianism and the paternalism it entails – something Rawls also argues against. I find that even though China might live up to Rawls' criteria for being a society whose lack of compliance with Rawlsian principles of justice as fairness could be tolerated due to a history of hardship or a certain, engrained belief system, it does not make their social media policies acceptable in a Rawlsian sense, even within the boundaries of such tolerance.

In Chapter 5, I show how social media-oriented national security policies in the U.S. have been mostly influenced by the Internet surveillance performed under the ECHELON program revealed in the late 90s, and by the Patriot Act, which was passed in 2001 and the Homeland Security act passed in 2002. Though the Patriot Act has since been retired and replaced by the USA FREEDOM act, I show how the general view of how social media fits into the information-gathering activities of the government's law enforcement and national security agencies is still the same: Government agencies collect information from public sources as open source intelligence gathering, including from public social media profiles. What you disclose on social media, even if this is in private and only meant to address a select number of people, is considered valuable in terms of criminal investigations as well as national security initiatives.

Thus, the U.S. government collects information on social media in the same manner and under the same legal restrictions as any other source of private information. But, as I show in the chapter, there are at least two policies that go beyond that and gather information on U.S. citizens and permanent residents through means that are less constricted in terms of legal requirements. Customs and Border Patrol (CBP) agents can search electronic devices at the border in order to study an individual's social media posts to ascertain any connections to criminal activity or activities that can be considered national security threats. It has become the Department of Homeland Security's (DHS) stated policy to increase the number of such searches, although – according to the department – it is still a very small fraction of travelers who have their electronic devices searched and their social media communication studied.

However, this is a violation of Rawls' principle of universal applicability as well as the maximin principle, as not everyone is equally subject to these searches and the DHS has yet to provide any evidence that this inequality benefits those most disadvantaged in American society. These arguments can also be aimed at a similar policy at the U.S. Citizen and Immigration Services (USCIS) in which the agency registers and stores the social media handles and other social media-related information of naturalized U.S. citizens, even long after their naturalization. In the chapter, I also show how these policies are not just in violation of Rawlsian principles, but also of the foundational, American tradition of liberty that Rawls is mired in. I show how the American post-revolutionary concept of individualism is not necessarily the root of the freedom-oriented culture that often is described as inherent to the United States' national identity, and that pillars of this culture, such as freedom of speech and privacy have never been seen as completely absolute.

Thus, Rawls' argument that a well-ordered society is not a private one is important here, in the sense that absolute liberty would be a hindrance to social cooperation. The most important findings of the chapter, thus, is that the DHS (or any other government agency) does not violate any Rawlsian principles by surveilling and studying the social media information posted by private citizens. But the way it is done is essential. For it to be in compliance with Rawls (and, some would argue, constitutional), searches of social media must be part of investigations that are conducted in accordance with legislation that has come to be through a transparent, democratic process. My findings indicate that such transparency may be lacking in the case of the two policies analyzed in chapter 5, making them unethical. I also find that the policies may be in violation of the privacy clause in the U.N. Declaration of Human rights, which would also make them unethical in Rawlsian terms.

Social media, the state and the citizen

The fourth research question for this study is divided up into three subquestions:

Given what we know from RQ3, from a Rawlsian perspective:

- *Under what circumstances should citizens be entitled to national security from the state on social media platforms?*
- *Which liberties can a state ethically require a citizen to surrender on social media to achieve national security?*
- *Which methods can states employ to protect citizens from misuse of their social media data without compromising Rawlsian justice as fairness?*

The answer to the first subquestion is distributed throughout the previous four chapters. The most important Rawlsian principles in this regard are his notions of equality, duty and universal applicability. But first, it should be emphasized that there is a difference between national security and personal security (e.g. cybersecurity) in this regard. Although a state can dedicate resources to the identification and removal of cyberthreats that may cause damage to personal property or give cybercriminals access to compromising, personal information, this work lies in a different part of the cybersecurity domain. As several of the interviewees in this dissertation have stated⁶⁵⁸, social media should be considered as part of cybersecurity strategies for several reasons. On the personal level, social media can be used to spread malware through spearphishing techniques and sockpuppeting⁶⁵⁹ and that can certainly create problems for the individual. But when it comes to national cybersecurity policies, social media should be considered part of cybersecurity because of the ability for mobilization or targeting of large numbers of users in a given country (voluntarily, as in the ISIS cases or involuntarily, as it was often the case in the Russian influence campaign), social media's extended capabilities for spreading of disinformation, and finally, because social media can be used as a bridge to more traditional cybersecurity activities by massively multiplying actions like the malware-spreading operation mentioned above.

⁶⁵⁸ Nissen, "Interview, May 31"; Slayton, "Interview, August 24."

⁶⁵⁹ Spencer Wolfe, "The Top 10 Worst Social Media Cyber-Attacks - Infosecurity Magazine," InfoSecurity, 2017, <https://www.infosecurity-magazine.com/blogs/top-10-worst-social-media-cyber/>; Kacy Zurkus, "Social Media, the Gateway for Malware," CSO, 2016, <https://www.csoonline.com/article/3106292/social-networking/social-media-the-gateway-for-malware.html>.

In other words, it can be argued that if a citizen has a right to be protected from massive cyberattacks by the government (either in the form of national cybersecurity defense or protection against cybercrime by law enforcement agencies), it follows that equally damaging events on social media would warrant the same protection. Just because the application is a different one, they are still Internet/network-based attacks. In Rawlsian terms, those who have created the basic structure from the original position would likely have agreed to a national security component⁶⁶⁰, and if so, this must be applicable to every person in the society. If you accept the argument put forth several times in this dissertation that social media – for better or worse – now constitute integral venues for democratic discourse in many countries, particularly in the U.S. and Europe, these platforms should enjoy the same protection against attacks as other media institutions of similar importance, and the same goes for the users of them.

Could this not be a private endeavor, since the social media platforms are private companies? It could, but it presents a challenge that may violate Rawls' principles: If the protection initiative lies with the consumer, it can become marketized, meaning that it may cost money to participate in or observe one of the most important venues for political debate. This is detrimental to democracy and against Rawlsian principles, simply because it may prohibit some citizens from participating. The protection could lie with the social media companies themselves, but this hasn't proven to be very effective so far. But more importantly, it can be argued that the democratic discourse is so important for society that it should not be subject to the whims of the

⁶⁶⁰ Thomas E Doyle, "When Liberal Peoples Turn into Outlaw States: John Rawls' Law of Peoples and Liberal Nuclearism," *Journal of International Political Theory* 11, no. 2 (June 9, 2015): 257–73, <https://doi.org/10.1177/1755088215571648>; Rawls, *The Law of Peoples: With "The Idea of Public Reason Revisited"*.

market, shareholders and non-elected CEOs and managers. It seems that some social media companies themselves are now realizing this, with their CEOs opening up for regulation that they have previously been opposed to.⁶⁶¹ So, to answer the first research subquestion in briefer way: When national interests and democracy are at stake, all users of social media platforms in a given nation should be able to expect protection from the government.

Drawing the line

Based on the work in this study however, it is clear that national security is difficult to achieve on social media (or perhaps in the entire cyber-domain) without compromising personal liberties somewhat. The three case studies/policy analyses in the previous chapters are very revealing when it comes to ascertaining where to draw the line, i.e. how far can the government go when it comes to asking citizens to sacrifice liberties for the sake of national security. It is clear from Chapter 4 that there is a limit to these sacrifices, unless the government wants, as Rebecca Slayton points out above, to turn the country into something different than what they originally wanted to protect. I have clearly shown how China's close monitoring and censorship of social media has a chilling effect on public discourse, and if Rawls is right, this is both unethical and unsustainable for a fair and just society. It may very well be that China's citizens are willing to accept and live with this trade-off to gain order and stability, but justice as fairness it is not. The U.S. case is less invasive (and also less pervasive), but I would argue that the findings presented

⁶⁶¹ Brian Feldman, "Zuckerberg Says He Is Open To Regulation in CNN Interview," New York Magazine, 2018, <http://nymag.com/selectall/2018/03/zuckerberg-says-he-is-open-to-regulation-in-cnn-interview.html>.

here show that “reasonable suspicion” is not sufficient reason to conduct a search of social media without obtaining a warrant or, at a minimum, leaving the search to someone with better training than CBP officers.

The issue here is what can be gleaned from social media compared to, say, the frisking in the *Terry* case. A frisking does not produce even a fraction of the information that can be collected from a quick look at a social media profile, not least because the social media search may involve information about your friends, family and other connections. It also may provide an officer with insight into conversations during which you are developing an opinion that may not be fully formed and you therefore do not wish to be held to. This latter example is one of the basic problems with the breach of privacy rights in social media investigations conducted at the border through electronic device searches and cannot be compared with what may result from a frisking. Rawlsian principles discussed elsewhere in this dissertation can be used here to make some important points that may sum up the answer to the research question:

- Liberties can be restricted to achieve national security justly and fairly.
- But such restrictions must be made through a transparent, democratic legal process.
- The restrictions must be universally applicable.
- The restrictions cannot impede democratic discourse.
- The restrictions must be of a nature, performed in a way and motivated by reasons that all citizens in society can accept and agree to.

In other words, the short answer to the question is: Any liberties can be surrendered *under the right conditions* to ensure social cooperation.

But those conditions are essential, and not always apparent. To test for the conditions mentioned above, as well as others, I propose The Rawls Test for social media policy below. This ties into the final research subquestion about which methods can be used by states to ensure national security on social media. The short answer here, parallel to the previous question is: Any method that passes The Rawls Test.

The fact is that technology is evolving constantly, and technologies that may be applicable today, may lose their value tomorrow. Instead, states should go one abstraction level higher and ask whether their methods are just and fair as established by The Rawls Test. Thus, the test itself becomes the method. As will become clear in the following, the test is rigorous, but also effective in testing for ethicality of proposed policies regarding social media.

Developing a Rawlsian ethics test for social media policy

Although online social interactivity slowly began with the Web 2.0 movement, massive decentralization of the distribution of information did not start to happen before the emergence of social media. It is the peer-trust value system and the ease of sharing built into these media platforms that signifies the paradigmatic shift they represent in terms of communication and distribution of information, and particularly news. The latter became very evident during the events described in chapter 3, that also showed how pervasive this user-based structure for dissemination of both data and information really is. Any communicator wishing to convey a message or spread information must now consider social media platforms alongside traditional media forms to do so, either using a way to lead consumers and users to deeper information

resources or as information resources in themselves. Online services, whether on the Internet, the Web or elsewhere, decentralized the production dimension of media. Social media decentralized the distribution dimension, and the two are co-dependent.

But it is crucial to understand, as numerous scholars have been demonstrating for a several years now,⁶⁶² that decentralization does not mean democratization. Decentralization and flattening of hierarchies into networks are merely structural changes. A distributed network is merely a more robust and efficient structure. It is value-neutral in the sense that this structure can be used just as maliciously as it can be used for good. A distributed network may equalize users' *abilities* of communication, access and influence, but if they employ information seeded with malicious intent when using these abilities (perhaps unwillingly, as described in chapter 3, the structure simply becomes a highly efficient tool of detriment. And then there's the question of ownership. Distribution of information may be decentralized within social media platforms, but ownership and control are not, which contributes to what some consider a tech-induced inequality on a previously unparalleled scale⁶⁶³

It is in this light that the findings of the previous chapters must be understood. The decentralized information distribution structure that social media platforms represent has

⁶⁶² Loader and Mercea, "Networking Democracy? Social Media Innovations and Participatory Politics"; Srinivasan, *Whose Global Village?: Rethinking How Technology Shapes Our World*; Napoli and Obar, "The Emerging Mobile Internet Underclass: A Critique of Mobile Internet Access"; Roberts, "Commercial Content Moderation: Digital Laborers' Dirty Work"; Zeynep Tufekci, "'Not This One' Social Movements, the Attention Economy, and Microcelebrity Networked Activism," *American Behavioral Scientist* 57, no. 7 (2013): 848–70.

⁶⁶³ Staff, "Engine Failure"; Jackie Snow, "Algorithms Are Making American Inequality Worse - MIT Technology Review," MIT Technology Review, 2018, <https://www.technologyreview.com/s/610026/algorithms-are-making-american-inequality-worse/>.

potential for good and bad (whether the potential is larger on either side is an important discussion, but outside the scope of this dissertation), which is why the discussion of its use has a significant ethical dimension, and why I have dedicated this dissertation to the study of one aspect of this dimension.

Atkin's expanded Oakes test

It is integral to John Rawls' model of a fair and just society that every person in it has equal rights to the benefits that the inhabitants of that society agree should be part of the basic structure. This is also the case for national security. In a well-ordered society, everyone has a right to their government's protection from destructive intrusions of any kind by a foreign state or non-state actor. The challenge lies in determining what *national* means in that sense. What is it in society that needs to be protected by the government? And, more importantly, when do security measures put in place alter society so much that it is no longer worth securing? As Rebecca Slayton puts it: "When you single out groups systematically, the question is whether you actually erode security and erode what the country exists for? Security is not an end, in and of itself. What are you securing? You're supposed to be securing a particular kind of society and when security starts to undermine that, it no longer seems very valid"⁶⁶⁴

One of the main purposes of this dissertation is to present a Rawlsian framework within which the policy debate surrounding balancing national security with privacy and civil rights can exist. Though it is always wise to be slightly reluctant when reducing frameworks to simple rules or tests, I will nonetheless proceed to describe a rule, distilled from Rawls, that may be a guide

⁶⁶⁴ Slayton, "Interview, August 24."

when constructing policies in the national security domain that may impact social media – or indeed, other communication forms used by citizens.

In her work, Atkin proposes a test for proportionality of privacy intrusions with regards to national security. She is motivated by what she regards as the insufficiency of the so-called *Terry stop* test. The Terry stop test is named after the 1968 U.S. Supreme Court case *Terry vs Ohio*, which established that “reasonable suspicion” was sufficient reason that the Fourth Amendment had not been violated when a police officer stopped and frisked two individuals who he believed were about to commit armed robbery of a store. Weapons were found during the frisking. The court ruled that if the “reasonable suspicion” was based on “specific and articulable facts”⁶⁶⁵, it would constitute sufficient probable cause that the search was also “reasonable” and thus not in violation of the Fourth Amendment. This is also basis of the claims to constitutionality of the border searches studied in Chapter 5. The court found that “there is no ready test for determining reasonableness other than balancing the need to search (or seize) against the infringement of the right in question”⁶⁶⁶

The problem, as Atkin notes, is proportionality. When are “facts” “specific and articulate” enough to warrant “reasonable suspicion”? And to what degree can an individual be searched based on that suspicion? There is a rather large distance between a pat-down and an in-depth search of your home and all of your property. Christopher Slobogin (quoted by Atkin) builds a framework around *Terry* that extends to government surveillance writ large. It is constructed

⁶⁶⁵ Atkin, *Balancing Liberty and Security: An Ethical Study of US Foreign Intelligence Surveillance, 2001-2009*, 15:81.

⁶⁶⁶ Atkin, 15:81.

around two propositions, the first being that the Fourth Amendment protects against “unjustified government infringement on individuals’ property, autonomy and privacy”. The second is that “the greater the threat to that security, the greater the justification the government should have to show”.⁶⁶⁷ This is still a somewhat vague rule of thumb, and Atkin proposes a more rigorous proportionality test, inspired by the Canadian government’s *Oakes test*.

This test was developed by the Supreme Court of Canada after a legal case in which the Canadian Charter of Rights and Freedoms had to be balanced against the country’s narcotics laws.⁶⁶⁸ The test is used to determine the reasonability of any limitation of the rights given in the Charter. Atkin modifies the original test to fit with the U.S. system and the Fourth Amendment in cases of government surveillance. Writing during the time when the Patriot Act was still the law of the land, she specifically suggests that the modified *Oakes test* can e.g. be used to determine proportionality in FISA cases granting permission for electronic surveillance. Atkin suggests the following form for the test:

1. Purpose of objective of the law: the law must be a response to a “pressing and substantial” problem in order to reduce the standard of probable cause to one of reasonable suspicion under the Fourth Amendment.
2. Proportionality: in order to determine the suitability of this lowered standard, the infringing statute must:
 - a. Be rational and nonarbitrary

⁶⁶⁷ Atkin, 15:81.

⁶⁶⁸ Atkin, 15:83.

- b. Result in minimal impairment to the right
- c. Demonstrate that the good that will be achieved by such infringement sufficiently outweighs any deleterious effect on the Fourth Amendment.⁶⁶⁹

In her work, Atkin generally employs a contractarian approach, and most of the study quoted above is concerned with Rawlsian ethics in that regard. However, note that in 2c, Atkin proposes a utilitarian demonstration, making the test “essentially a combination of contractarian and utilitarian tests”⁶⁷⁰

Rawls’ arguments against utilitarianism

Thought Atkin’s work is certainly convincing and may very well be beneficially applicable to general policy-making in this area, Rawls’ arguments against utilitarianism complicates Atkins’ utilitarian compromise, at least when it is applied to social media policy.

Rawls’ main argument against utilitarianism is that it opens up society to unfair inequality.

Rawls generally only allows for inequality when it benefits those who are most burdened or underserved in society, whereas utilitarianism allows for a minority to have to make even harsh sacrifices and give up certain rights, if it benefits a larger group.

The issue here is one of epistemology and prediction: How can you actually know whether the sacrifices made by the minority will benefit the larger group? And for how long? A short-term benefit may turn into a long-term disadvantage, invalidating the utilitarian basis upon which

⁶⁶⁹ Atkin, 15:87.

⁶⁷⁰ Atkin, 15:87.

the policy was constructed. The burka ban in France may well solve a current problem and create a sense of cultural cohesiveness in the country, but if the ban later creates a legal precedent for banning other religious clothing, the law transcends its original, practical origins and becomes a question of freedom of religion, and by extension, of thought. Another, more likely consequence of the ban could be the marginalization of certain social groups, cutting them off as sources for information collected in the prevention of terrorism, or making individuals easy targets for self-radicalization via social media. The question of certainty of the consequences is one of the main critiques against the aptly named consequentialist utilitarianism (utilitarianism is generally seen as variant of consequentialist philosophy)⁶⁷¹, and at the same time one of its main tenets. Utilitarianist philosophy relies heavily on calculations of probability, often employing the expected-utility hypothesis, thereby bringing utilitarianism into the domain of rational-choice theory. The expected-utility hypothesis (in the normative sense) describes the relationship between perceived utility and probability of outcomes.⁶⁷²

Maximin

Of course, it is an exaggeration to assume that all utilitarianists and consequentialists perform deep probability calculations before taking any kind of action, and some explain this apparent contradiction by reminding critics that neither of the two are decision processes. Utilitarianism,

⁶⁷¹ William Haines, "Consequentialism," The internet encyclopedia of philosophy (Internet Encyclopedia of Philosophy Pub, 2018), <https://www.iep.utm.edu/conseque/>.

⁶⁷² Jonathan Baron and Brian Cohen, "Why Expected Utility Theory Is Normative, but Not Prescriptive," *Medical Decision Making* 16, no. 1 (1996): 7–9, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.903.4852&rep=rep1&type=pdf>.

writes Sinnott-Armstrong, is a “*criterion or standard* of what is morally right or morally ought to be done”⁶⁷³ (emphasis in original). It lies at the ethical level. But even so, at this higher level of abstraction, particularly modern utilitarians employ probability projections to reach ethical maxims.⁶⁷⁴

Instead of relying on probability calculation and projection, Rawls proposes the “maximin” principle. The idea is to “maximize the minimum”, i.e. “rank alternatives by their worst possible outcomes: we are to adopt the alternative the worst outcome of which is superior to the worst outcome of the others”.⁶⁷⁵ This, of course, still requires some kind of prediction of outcomes (Rawls writes that “all ethical doctrines take consequences into account in judging rightness. One which did not would simply be irrational, crazy”⁶⁷⁶) but notably, it does not require an evaluation of probability. The maximin rule merely asks to imagine the worst possible outcomes with what is possible to know at the given time, and then choose the one which is least bad. This is a cautious, risk-adverse approach, and Rawls acknowledges this. He states specifically that the maximin rule “is not, in general, a suitable guide for choices under uncertainty”⁶⁷⁷, but rather, “it is attractive in situations marked by special features”. These features include:

⁶⁷³ Walter Sinnott-Armstrong, “Consequentialism,” *Stanford Encyclopedia of Philosophy* (Stanford University, 2015).

⁶⁷⁴ John C Harsanyi, “Bayesian Decision Theory and Utilitarian Ethics,” *The American Economic Review* 68, no. 2 (1978): 223–28.

⁶⁷⁵ Rawls, “A Theory of Justice,” 152.

⁶⁷⁶ Rawls, 26.

⁶⁷⁷ Rawls, 153.

1. The probabilities are discountable for some reason, e.g. “the knowledge of likelihoods is impossible, or at best extremely insecure”.⁶⁷⁸
2. Gaining extra benefits from not acting in accordance with the maximin rule is unattractive: “The person choosing has a conception of the good such that he cares very little, if anything, for what he might gain above the minimum stipend that he can, in fact, be sure of when following the maximin rule”.⁶⁷⁹
3. The rejected alternatives have “outcomes that one can hardly accept”.⁶⁸⁰

As an example, consider the DHS policies analyzed in chapter 5. The DHS may very well have conducted large studies that describe the likelihoods of different outcomes of increasing the border searches in the manner that is described here. But if they have, these studies have not been made public, nor have they been used in the arguments for the policy. Only post-hoc reports with vague indications of how some crimes have been stopped by implementing the policy have emerged, such as in the op-ed by the DHS’ general counsel in chapter 5. The same can be said about the DHS keeping social media information about naturalized citizens in their A-files for perpetuity. This violates the transparency required by Rawls in well-ordered societies. As described in chapter 5, Rawls acknowledges the need for secrecy and classification of files in law enforcement and national security, but only under the condition that laws and

⁶⁷⁸ Rawls, 154.

⁶⁷⁹ Rawls, 154.

⁶⁸⁰ Rawls, 154.

policies enabling the obfuscation are transparent and democratic. If the DHS chooses to base its policies on studies that are kept secret from the populace, it goes against this Rawlsian principle.

In either case, the policies in question are marked by all three of the features Rawls describes as making a pending decision a candidate for the application of maximin:

The probabilities are discountable: First, since no serious studies have been made public about the eventual outcomes of the policies. Second, the CBP officer making a decision to conduct a search of an electronic device or asking for social media login information does not have the time, the means nor (necessarily) the education to perform a detailed outcome probability analysis on the spot and will have to rely on other methods to make a determination. Third, it is debatable whether it is at all epistemologically possible to find realistic and fairly calculated outcomes of such a policy. There are multiple categories of variables at play. from the privacy-violating effects of giving CBP officers with a minimum of training access to personal information of citizens, over the consequences for CBP officers risking exposure to psychologically harmful material in a similar fashion as commercial content moderators do⁶⁸¹ to the geopolitical and ideological implications of how the U.S. is viewed by foreigners, allies and enemies, etc. Even with advanced AI and machine learning at hand, it is doubtful that the DHS has had the resources or the time to calculate outcomes with an accuracy that is anything but fairly low.

⁶⁸¹ Roberts, “Commercial Content Moderation: Digital Laborers’ Dirty Work.”

The extra benefits are unattractive: In this policy question, it is not so much a matter of the extra benefits not being attractive as it is a question of it not being appropriate. It seems fairly obvious that public policy decisions should not be made on the merits of beneficial side effects if the main effect of the policy is not acceptable.

The outcomes of the rejected alternatives are unacceptable: Again, the question here is whether maximin should be employed when deciding upon a policy of searching electronic devices at the border – either in its enforcement or its implementation. If maximin is not employed and consequentialist utilitarianism is used to argue for it instead, the outcome can be seen as both a violation of the privacy clause in the U.N. Declaration of Human Rights as well as a Fourth Amendment violation as described above. Now, that these interpretations exist might be acceptable for the DHS under a utilitarianist approach, but human rights violations and unconstitutionality would normally be considered unacceptable by lawmakers in well-ordered societies.

How maximin applies to the U.S., China and Russia cases

In other words, the DHS policy described above is a prime candidate for the maximin rule, which raises new questions: How would the maximin rule actually apply to this dual policy? Or more specifically: What are the worst imaginable outcomes? The first, obvious answer which comes to mind is that, in lieu of electronic device border searches, a swarm of terrorists will slip through the border and commit acts of terror with mass casualties as a result. However, even without calculating likelihoods, but simply using reason, this is easy to dismiss.

First of all, a search of the open source court opinion database Court Listener reveals that there have been no recent decisions in federal court cases related to national security in which a defendant has been charged due to a border search of an electronic device. Since the increase in border searches began, the only two such federal cases that have been decided are *U.S. vs Maria Molina-Isidoro* and *United States vs Hernando Javier Vergara*. In the latter case, the defendant was a convicted sex offender who was on a watch list for this reason.⁶⁸² A search of his luggage upon returning from a trip to Cozumel, Mexico revealed three cellphones, and upon conducting a “basic” search (see Chapter 5), the CBP found evidence of child pornography, and a later forensic search revealed more than a 100 such videos and images.⁶⁸³ In *Molina-Isidoro*, a drug-sniffing dog alerted CBP officers to the defendants’ luggage, in which they found 4.32 kilograms/9.5 pounds of methamphetamine hidden in a secret compartment. This brought the CBP officers to also inspect her cell phone, something that has compelled the EFF, The Brennan Center for Democracy and several other advocacy organizations to file amicus briefs in the case, arguing that the phone search was unconstitutional.

In both cases, the electronic device searches may be contested on privacy grounds, but it is hard to argue against the CBP officers’ claim to “reasonable suspicion”. They were following the policy directives at they were laid out. Yet, it would be a bit of stretch to attempt to portray these cases as national security threats. This does not exclude national security-related charges from

⁶⁸² Ken Wallentine, “Officer’s Warrantless Smartphone Search Permitted by Border Search Doctrine,” Lexipol, 2018, <http://www.lexipol.com/news/officers-warrantless-smartphone-search-permitted-border-search-doctrine/>.

⁶⁸³ William Pryor, “United States v. Vergara, 2018 WL 1324589 (11th Cir. 2018),” 2018, <http://media.ca11.uscourts.gov/opinions/pub/files/201615059.pdf>.

being brought in the future based on electronic device border searches, of course, but so far, there is no empirical evidence of the policy being effective in that regard.

Second, studies point to the fact that terrorists increasingly use encrypted technologies to communicate and depend less on open communication such as social media communication or e-mails. Techniques include steganography (which has been in use at least since 2001⁶⁸⁴, but is now growing in use due to apps such as MuslimCrypt⁶⁸⁵), in which messages are hidden in e.g. image files. These messages are not visible to the naked eye and would therefore not be found by a CBP officer conducting a basic search.

Third, policy-makers could rightfully ask whether it would be a better use of taxpayer dollars to simply expand the FBI's investigative work on social media, which would also be in closer compliance with the Fourth Amendment, since there is an established legal precedent in place. If, hypothetically, the FBI's work is more effective in this regard, it weakens the argument that stopping border device searches on suspicion of national security threats would result in a rise of terrorist incidents because more terrorists are allowed to enter the country. Fourth, and finally, as the DHS themselves have admitted, the border searches of electronic devices amount to less than 1% of those crossing the borders into the U.S. That in itself, even if we do consider probability, makes the likelihood of checking the right person's phone negligible. It is the terror equivalent of finding a needle in a haystack without a highly effective magnet.

⁶⁸⁴ Gina Kolata, "Veiled Messages of Terror May Lurk in Cyberspace," The New York Times, 2001, <https://www.nytimes.com/2001/10/30/science/veiled-messages-of-terror-may-lurk-in-cyberspace.html>.

⁶⁸⁵ Lily Hay Newman, "MuslimCrypt Steganography App Helps Jihadists Send Secret Messages," Wired, 2018, <https://www.wired.com/story/muslimcrypt-steganography>.

So, it is not just improbable, but implausible from a reason-based point of view that the worst outcome of not implementing the electronic device border search policy would be a massive rise in terrorists entering the country. Another argument against the policy in this regard concerns borders more generally: The large majority of terrorists convicted for attacks on U.S. soil since 9/11 are/were U.S. citizens,⁶⁸⁶ many of whom were radicalized here or in an allied country.⁶⁸⁷ Could the worst outcome then be that the intelligence community (IC) would lose access to valuable information? No, because, as mentioned above, the exchange of information between the DHS and other agencies is complicated by legal obstacles which basically makes it easier for the IC to collect the information itself.

The worst outcome of not implementing the policy, it seems, is that the CBP would no longer be able to contribute to the reduction of non-national security-related crimes such as distribution of child pornography or drugs as mentioned above (which also happen to be the DHS' main argument for the policy's success⁶⁸⁸) and continue their extremely limited participation in upholding national security.

This should then be held up against the worst outcome of implementing the policy. In Rawlsian/Kantian terms, the universality principle would apply, which would mean that it would

⁶⁸⁶ U.S. Department of Justice, "DOJ, DHS Report: Three Out of Four Individuals Convicted of International Terrorism and Terrorism-Related Offenses Were Foreign-Born," Justice.gov, accessed April 2, 2018, <https://www.justice.gov/opa/pr/doj-dhs-report-three-out-four-individuals-convicted-international-terrorism-and-terrorism>; Julia Ainsley and Robert Windrem, "New Report Says Most U.S. Terrorists Foreign Born, but Check the Fine Print," NBC News, 2018, <https://www.nbcnews.com/news/us-news/new-report-says-most-u-s-terrorists-foreign-born-check-n838041>.

⁶⁸⁷ Windrem, "Terror in the Family: When Radicalization Begins at Home"; Wright, "Domestic Terrorism, Cyber-Radicalization, U.S. College Students."

⁶⁸⁸ Maher, "DHS: Device Searches Improve Safety."

be not legally (yet), but ethically defensible to apply the same type of searches to regular law enforcement. In other words, a “reasonable suspicion”-based search by a police officer on the street as described in *Terry* above could include an electronic device search without this being seen as disproportional. If the current policy has not already had a chilling effect on freedom of speech, then such a policy is almost certain to have it.⁶⁸⁹ And, of course, it would be a significant change in the current interpretation of the Fourth Amendment.

In other words, the maximin rule would clearly point to not implementing such a policy. The doubtful constitutionality, but more importantly, the chilling effect on freedom of speech would be in violation of the basic liberties suggested by Rawls.⁶⁹⁰ More importantly, the universality principle is also violated, since not everyone’s phones are being searched. In essence, the policy in question is a very clear example of why utilitarian principles should not be considered for policies involving rights that may impact the way democracy works (i.e. the ability to develop thoughts and express opinions in private and maintaining some control of how your expressions are being used). In the electronic device border search example, a small minority must suffer extra scrutiny under the pretense of securing the larger majority - a clear utilitarian principle. But the consequences are not evident. Some utilitarians such as John Harsanyi or Jonathan Baron argue that if it is indeed impossible to know the outcome of a

⁶⁸⁹ Frederick Schauer, “Fear, Risk and the First Amendment: Unraveling the ‘Chilling Effect,’” *Faculty Publications, College of William and Mary*, 1978, <http://scholarship.law.wm.edu/facpubs>; Leslie Kendrick, “Speech, Intent and the Chilling Effect,” *William and Mary Law Review* 54, no. 5 (2013): 1633–92, <https://doi.org/10.3366/ajicl.2011.0005>.

⁶⁹⁰ Rawls, “A Theory of Justice,” 61.

decision, equal probability should be ascribed to all outcomes.⁶⁹¹ In this case, that would be the same as opening up for the use of maximin, since probability can effectively be disregarded – so why not just skip straight to Rawls?

Applying maximin to the Chinese and Russian policies requires setting aside the other Rawlsian objections against the policies that I have laid out in chapters 3 and 4. If we do that for the sake of argument, it becomes even more apparent how useful maximin is as a basis for considering ethics in the social media realm when it comes to regulation, public policy and information access.

In China, not censoring and monitoring social media would perhaps enable a free dialogue where opinions does not need to be conveyed though coded language. The Confucianist roots in the country are deep, and the paternalism and thoughtful conduct would likely prevail for many years to come. Mao’s cultural revolution couldn’t change this, so why would social media, at least in the short term? Long term, the variables are too many to predict what might happen with a China that has access to international social media platforms and a free press. The country already has a totalitarian regime, so what is the worst outcome? Democracy?

The question then, is the price of democracy. Is a fast transition to democracy worth the lives of millions who may falter if China’s economy suffers because of massive, systemic change in government? Perhaps not. The problem is that it is impossible to *know*. This would again be a

⁶⁹¹ Harsanyi, “Bayesian Decision Theory and Utilitarian Ethics”; John C Harsanyi, “Bayesian Decision Theory, Rule Utilitarianism, and Arrow’s Impossibility Theorem,” *Theory and Decision* 11, no. 3 (September 1979): 289–317, <https://doi.org/10.1007/BF00126382>; Baron and Cohen, “Why Expected Utility Theory Is Normative, but Not Prescriptive.”

case in which probability calculations would be wildly uncertain, and so decisions must be based on other information or principles.

In either case, lifting the repressive social media policies in China may be consequential for a small elite, but would likely not change the general conduct of the Chinese people. Western influences would likely grow immensely, but it seems implausible that the Confucianist roots of the Chinese people would disappear over brief period of time. Interestingly, this is the exact opposite of utilitarianism: Protecting a small elite by repressing a large majority. It can be argued that this is an effect of Confucian ethics, a type of Role Ethics.⁶⁹² The latter is a theory of ethics based around roles in the community or the family, and morality is determined through the fulfillment of your role in society.⁶⁹³ The role is given by the relationship with the community, thus in China, the general populace represents the “children” of the “family” and the government leaders are the “parents” – fitting with the paternalist tenets of Chinese society. Rawls would likely find that reinstating the ability to have privacy to develop thoughts and express them without being associated with the thoughts until you decide it is time, would be worth the sacrifice of a temporary economic downturn that is bound to appear at some point anyway. The question is how to make such a transition as smooth and peaceful as possible, but that’s a different question than whether it should happen or not.

⁶⁹² Roger T Ames, *Confucian Role Ethics: A Vocabulary* (Chinese University Press, 2011).

⁶⁹³ Christine Swanton, *Virtue Ethics, Role Ethics, and Business Ethics* (Oxford: Oxford University Press, 2007).

The Rawls Test for ethics in social media policy

As mentioned above, within the Rawlsian frame, Atkin's version of the Oakes test may not work as well for social media policies as it does for its original purpose. But her notion of the necessity of a proportionality test is hard to argue against. I propose that such a test could simply be based on the Rawlsian frame that I have used in the three policy analyses in this paper and could consist solely of a selection of Rawls' most foundational principles. The test would not just be for proportionality, however. It would test how well a policy overall satisfies the criteria of Rawlsian ethics. The test would be used to transcend real-life scenarios into a higher level of abstraction to understand the broader, ethical consequences of a proposed policy. However, because it is intended for application on real-life policies, it is prudent to avoid some of Rawls' most transcendent concepts, such as the original position and the veil of ignorance. In such a test, it must be assumed that there is already a basic structure in place, whether it lives up to Rawls' requirements for such a structure or not. It will also be assumed that the test is applied within the confines of a decent (in Rawlsian terms), well-ordered society, in which there is a sufficient level of transparency with regards to legislative procedures and enforcement of laws, and where a citizens' right to Rawls' primary goods is respected.

Such a test would first establish that the policy does not violate any of Rawls' basic liberties. It would then make use of the maximin principle in concert with the difference principle, i.e. the second principle of Rawls' justice as fairness concept. The combination of these two principles would safeguard personal liberties in a situation where these are at risk of being infringed upon by a new policy. It is easy enough to construct a test that simply protects privacy or citizens' rights by not allowing for any sacrifices of these to serve a higher purpose

for society at large. For Rawls, it is not a question of whether rights should be compromised to ensure justice and fairness in society, he is very clear that this is necessary, but how to choose which rights to surrender. The latter is precisely the big challenge addressed in this dissertation, and so the test must also contain affordances for social cooperation, even if those infringe on certain rights. To achieve this, the combination of maximin principle and difference principles will be balanced with Rawls' criterion of reciprocity within public reason. I have described this criterion in the context of international relations with regards to Russia in Chapter 3, but as I also mentioned there, the principle is originally stated as part of Rawls' principles of justice for a constitutional regime. This will be combined with Rawls' notions of duty to bolster the social cooperation aspect of the test, firmly rooting the test in the deontological tradition to which Rawls belongs. Finally, the universality principle will be a crucial part of the test ensuring that it is fair and just for all, also in future situations where we cannot know the outcome.

To pass "The Rawls Test" for ethical social media policy, a proposed policy would thus have to answer these six questions in the affirmative:

1. Does the policy enable freedom of thought, liberty of conscience and belief systems, political liberties including freedom of speech, freedom of the press and freedom of assembly, freedom of association, freedoms specified by the liberty and integrity of the person and rights and liberties covered by the rule of law?
2. Is the worst imaginable outcome of the policy the least unattractive one, considering all other imaginable outcomes?

3. Are social and economic inequalities created by the policy afforded as equal opportunities accessible to all, and do the least advantaged members of society benefit the most from them?
4. Does the policy enable reasonable, reciprocal terms of social cooperation?
5. Does the policy enable a person to use their capacities for a sense of justice and conception of good to further social cooperation?
6. Can the policy be extended to all persons in any conceivable condition and still comply with the above five principles?

It can be argued that such a test is very rigorous and that it expresses a risk-aversity that may impede economic growth and technological innovation. But it must be understood that this test, as suggested here (I shall discuss its validity outside the domain later) is specific to policies that concern social media. As mentioned above, social media constitute a communications infrastructure which is integral to societies the world over and, as shown in the previous chapters, an essential part of the information infrastructure that makes democracy possible. Considering these stakes, it can be argued that some risk-aversity in policy-making with regard to social media may be appropriate. In an information-based society, the regulation of social media may be seen as partially changing the very fabric of that society, as it is one of the dominant infrastructures that constitutes it.

Applying The Rawls Test to policies described in the previous chapters helps demonstrate the validity of such a test. It seems fairly obvious that the Chinese monitoring and censoring (and sometimes prosecution) of government criticism on social media cannot satisfy 1. (and thereby also 6.), but the Chinese insistence on a respectful, truthful tone on social media would actually

satisfy 4. and 5 (this is achieved through coercion, though.) However, Chinese social media policies would not live up to 2. and 3. The latter because there are free-trade zones in some Chinese cities⁶⁹⁴, where the restrictions on use of foreign social media by, say, business travelers are less strict, thereby creating an inequality that doesn't seem to be to much benefit overall for poverty-stricken parts of China. Yes, the country's economy is better off more broadly because of the influx of foreign money brought into these free-trade zones, but this is only secondarily related to the ability to use foreign social media platforms there. More importantly, and this also violates 2., it can be argued that there may be even larger benefits to the economy if users in less economically successful areas of China could market their digital products directly on international social media platforms. The only way this outcome can be viewed as worse than violating the Rawlsian equality expressed in 3. is if you employ the type of paternalistic role ethics that inform Chinese regulation overall (which then fails to satisfy 1. and 6. again). If the government wishes to forcefully implement a certain, uniform value system to be adhered to by the population, then it may be seen as the worst outcome that differing opinions outside the control of the government reaches the broader population through foreign social media, relative to creating some inequality that doesn't necessarily do much for the entire population. But as mentioned, either way you frame this policy, it fails the test.

With regard to Russia's offensive social media operations, they can actually be seen as satisfying 2. It may be a decidedly positive outcome for Russia, not just the least bad one, if they

⁶⁹⁴ George Chen, "China to Lift Ban on Facebook – but Only within Shanghai Free-Trade Zone," South China Morning Post, 2013, <http://www.scmp.com/news/china/article/1316598/exclusive-china-lift-ban-facebook-only-within-shanghai-free-trade-zone>.

are able to influence foreign elections on a very small budget, and if that influence results in the election of officials who would enact more Russia-friendly policies. But the remainder of this social media information warfare policy does not fare well in the rest of the test. The Russian influence campaign of 2016 can superficially be viewed as enabling differing points of view by spreading information representing positions from both the extreme right and extreme left. This could (again, on the surface) be seen as an expression of many of the freedoms mentioned in 1., for example. The issue here is the crowding-out effect and the erosion of truth discussed in Chapter 4. By targeting voters in certain areas very closely, these voters may not have been exposed to real election information on social media, simply because the misinformation dominated the platforms, and this puts them at a disadvantage compared to other areas where the Russian influence campaign was less prevalent. It is a violation of 3., as this inequality obviously cannot be said to be to the targeted society's advantage, as it impedes the targeted citizens' ability to perform democratic duties, thereby also violating 5. It can be argued that creating inequality somewhere else may be to Russia's advantage, but that is a violation of the reciprocity principle stated in 4. (as is the entire policy of meddling in other countries' elections, of course). Finally, the policy does not satisfy the criteria in 6. It is doubtful that the Russian Federation as a nation would be interested in having a foreign power intervene in their already allegedly fraud-ridden elections⁶⁹⁵ through social media.

⁶⁹⁵ Henry Meyer, "Russian Observers Charge Fraud in Putin's Landslide Re-Election," Bloomberg Politics, 2018, <https://www.bloomberg.com/news/articles/2018-03-19/russian-observers-charge-fraud-in-putin-s-landslide-re-election>.

Then, there are the two U.S. policies discussed in Chapter 5. Because these are already implemented in a nation that for the most part is seen to conform with Rawls' notions of a decent and well-ordered society, it shouldn't be as easy as in the Russia and China cases to dismiss the policies by putting them through the test. Thus, this is where the test shows its real utility. I have already discussed above how the electronic device border search policy can be seen as problematic in terms of the maximin principle, and the answer to 2. may therefore not be an affirmative one when the test is applied to this policy. I have also laid out how the chilling effect may lead to self-imposed restrictions on freedom of speech, and the policy therefore doesn't comply with 1., either. But the electronic device border search policy runs into further trouble in 3. Though the first part of this question can be answered in the affirmative – it is possible for all citizens to vote for politicians who will change the CBP, citizens have the right to take legal action against the CBP, and anyone can apply to join the CBP – the second part is less easy to answer yes to. The DHS' argument for the policy, as mentioned in the previous chapter, is that it protects the nation. But this is, as also mentioned earlier, a utilitarian argument. It does not comply with Rawls' principle, stated in 3., that the *least* advantaged in society should gain the *most* from the inequality created by the policy. There is no minority of least advantaged members of society who benefits more from the policy than others. At best, they benefit the same as everyone else, which is exactly why the DHS uses a utilitarian argument to defend the policy.

If, as the ACLU purports, it is most often people of Middle-Eastern descent and Muslims who have their devices searched, it can be argued that the minority that suffers the inequality is also a minority that is among the least advantaged in American society, which is not just a violation of 3., but an inversion of it. From the reports of how the electronic border searches are

conducted, the reciprocity principle's notion of civility and tolerance is apparently also violated by the way the CBP officers express their suspicion and treat the persons of interest.⁶⁹⁶ This is violation of 4. With regards to 5., it can be argued that complying with law enforcement in a well-ordered society is seen by Rawls as being dutiful and expressing your capacities for good and for justice. The question is whether the CBP officers, as citizens working in law enforcement, comport themselves in ways that would also comply with these principles? In either case, there is still the matter of the chilling effect. Esha Bhandari mentioned this effect above as her main concern about the policy⁶⁹⁷, and if a chilling effect on freedom of expression is indeed the result of the policy, it violates 4. and 5., and as mentioned above, 2. Extending the policy beyond its original scope, as in 6., does not make a difference here. Since the policy fails all the other points in the test, it is reasonable to assume that it would also fail them when extended beyond its original scope.

What, then, about the registration of social media information about naturalized citizens and permanent residents in their A-files? The chilling effect is still a factor, and thus no affirmative answer can be given to 1. It can be argued that loss of freedom of speech due to the chilling effect is in conflict with the First Amendment, and even it isn't directly unconstitutional, broad self-censorship is a considerably worse outcome than any loss of intelligence that might result of e.g. not registering the social media handles of naturalized citizens and permanent residents (particularly because these handles are so easily and, for some, frequently changed).

⁶⁹⁶ Cope et al., "Digital Privacy at the U.S. Border: Protecting the Data On Your Devices | Electronic Frontier Foundation"; McFadden et al., "American Citizens: U.S. Border Agents Can Search Your Cellphone."

⁶⁹⁷ Bhandari, "Interview March 8, 2018."

Thus, 2. is most certainly violated by this policy. It is also hard to find a good argument to support how the least socially and economically advantaged Americans would benefit more than everyone else from the inequality of only keeping records of personal information belonging to a specific group of people, especially if government protection against national security is equal for all. This violates 3. Questions 4. and 5. in the test are once again violated by the chilling effect, but even if it wasn't, it is hard to argue that keeping records of this personal information about certain people directly enables social cooperation, other than it gives the targeted group an opportunity to be dutiful to the nation. And with regards to 6., the policy actually cannot be extended to everyone without re-violating the rules, but also, there are naturalized citizens working in the intelligence and law enforcement communities for whom it could be life-threatening to have their social media information exposed to others, if the CBP was hacked, for example. It would also likely be Fourth Amendment violation to extend this policy to everyone living in the U.S. When you apply for lawful permanent residency or naturalized U.S. citizenship, you consent to the sort of background check that would provide social media information and search engine results to the USCIS. Extending the policy would either mean that everyone living in the U.S. would have to provide a similar consent or accept that the government collected their social media handles and stored them without such consent. The latter would, as mentioned, likely be a Fourth Amendment violation. The former would, based on the sociocultural traditions laid out in Chapter 5, almost certainly result in a large group of people not giving their consent, and then the principle is violated again.

The Rawls Test can also function as an analytical tool, providing information about aspects of the policy that might not have been considered under a utilitarian decision-making process.

Into the future

How contractarian deontology may reduce the “law lag”

I also want to point to a broader point that may be extracted from the findings of this dissertation but will require much further research. Some believe technology develops so fast that regulators and policymakers have trouble keeping up, and several commentators and scholars have discussed this “law lag” between technological development and regulation.⁶⁹⁸ Particularly Democratic lawmakers argue that this is in fact the issue that led to the calamities surrounding Facebook and the 2016 presidential election⁶⁹⁹, suggesting that earlier implementation of sufficient regulation of political social media advertising could have limited the harm done. China has solved this by tightening the government’s grip on technology producers, foreign influences and how people are able to use the technology. But, as argued above, this is not a just and fair way of going about solving such a problem, at least not in Rawlsian terms.

The challenge is that even though technology journalists, market analysts, scholars, book authors and filmmakers all try to predict how technology will develop, they are very often wrong. Let me use a few popular examples to illustrate this. The 1982 film *Blade Runner* was

⁶⁹⁸ Vivek Wadhwa, “Laws and Ethics Can’t Keep Pace with Technology,” MIT Technology Review, 2014, <https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/>; Caroline Brown, Anna Kraus, and Philip Pesich, “Regulations Lag Behind ‘Telehealth’ Technology | National Law Journal,” The National Law Journal, 2015, <https://www.law.com/nationallawjournal/almID/1202719886237/?slreturn=20180302141303>; Wulf Kaal, “What Happens When Technology Is Faster Than the Law? | CLS Blue Sky Blog,” Columbia Law School Blue Sky, 2016, <http://clsbluesky.law.columbia.edu/2016/09/22/what-happens-when-technology-is-faster-than-the-law/>.

⁶⁹⁹ Natasha Bertrand, “After Facebook-Russia Bombshell, Dems Urge FEC to Regulate Political Ads - Business Insider,” Business Insider, 2017, <http://www.businessinsider.com/facebook-russia-investigation-fec-political-ads-2017-9>.

supposed to show a colorful future (one year from when this dissertation is being finalized) where humanoid robots work as slaves and cars fly. Though these two technological wonders were perhaps less expected by the filmmakers, it is interesting to note that the film contains no mobile telephones or flat screens. Instead, the filmmakers expected that 37 years into the future, CRT screens would still be everywhere, as would payphones – the latter would just be video-based. It should be noted that both the mobile phone and flat screen technologies existed at the time and was slowly making their way to the early market adopters. But even those who predict technological advances for a living are often more wrong than right. In 2012, the technology market analysis firm IDC predicted that within four years, Microsoft Windows Phone platform would be bigger than Apples iOS, meaning that Windows Phones would sell more than iPhones and become the second largest platform after Android.⁷⁰⁰ Only three years later, Microsoft launched what would be the final version of the software before abandoning the platform which never took off.⁷⁰¹ Á propos mobile phones, the prominent technology journalist David Pogue, writing for The New York Times in 2006, wrote “Everyone’s always asking me when Apple will come out with a cell phone. My answer is, ‘Probably never.’”⁷⁰² The Apple iPhone was launched in 2007. Internet pioneer and creator of Ethernet, Robert Metcalfe said in 1995, as the World Wide Web was causing millions of people to subscribe to Internet services: “I predict the Internet

⁷⁰⁰ Alexandra Chang, “Why IDC Predicts Windows Phone Will Surpass IOS by 2016,” Wired.com, 2012, <https://www.wired.com/2012/06/why-idc-predicts-windows-phone-will-surpass-ios-by-2016/>.

⁷⁰¹ Tom Warren, “Did Microsoft Just Give up on Windows Phone?,” The Verge, 2015, <https://www.theverge.com/2015/7/8/8913365/microsoft-lumia-windows-phones-strategy-2015>.

⁷⁰² Robert J. Szczerba, “15 Worst Tech Predictions Of All Time,” Forbes.com, 2015, <https://www.forbes.com/sites/robertszczerba/2015/01/05/15-worst-tech-predictions-of-all-time/#6915ac041299>.

will soon go spectacularly supernova and in 1996 catastrophically collapse.”⁷⁰³ In 1960, in his groundbreaking paper *Man-Computer Symbiosis*, J.C.R. Licklider wrote that he estimated it would take five years for computers to obtain “practically significant speech recognition”.⁷⁰⁴ I doubt anyone working with computers in 1965 would argue that significant speech recognition had been achieved. Amara’s law, attributed to researcher and futurist Roy Amara, states that “We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run”.⁷⁰⁵ The collected quotes above are no evidence of consistent failure of technological prediction, of course, but there have been studies that show a similar pattern of inaccuracies in different types of forecasting due to inherent biases and other influences⁷⁰⁶ The difficulty associated with predicting the development of technology has a direct impact on what kind of ethics we should employ when constructing technology policy. Western policy-making is still dominated by probabilistic utilitarianism⁷⁰⁷, and it has become a heuristic relied

⁷⁰³ Szczerba.

⁷⁰⁴ J. C. R. Licklider, “Man-Computer Symbiosis,” *IRE Transactions on Human Factors in Electronics* HFE-1, no. 1 (1960): 11, <https://doi.org/10.1109/THFE2.1960.4503259>.

⁷⁰⁵ Susan (Ed.) Radcliffe, “Amara, Roy,” *Oxford Essential Quotations*, 2016.

⁷⁰⁶ Petter Naess et al., “Forecasting Inaccuracies: A Result of Unexpected Events, Optimism Bias, Technical Problems, or Strategic Misrepresentation?,” *Journal of Transport and Land Use*, 2015, 39–55, <https://doi.org/10.5198/jtlu.2015.719>; Nigel Meade and Towhidul Islam, “Modelling and Forecasting the Diffusion of Innovation – A 25-Year Review,” *International Journal of Forecasting* 22 (2006): 519–45, <https://doi.org/10.1016/j.ijforecast.2006.01.005>; Morten Welde and James Odeck, “Do Planners Get It Right? The Accuracy of Travel Demand Forecasting in Norway,” *EJTIR Issue* 11, no. 1 (2011): 80–95, www.ejtir.tbm.tudelft.nl.

⁷⁰⁷ Ben Eggleston and Dale E Miller, *The Cambridge Companion to Utilitarianism* (Cambridge University Press, 2014); George Diepenbrock, “Professor Studies How Utilitarianism Provides Framework for Major Policy Decisions | The University of Kansas,” *Kansas University News*, 2014, <https://news.ku.edu/2014/06/02/professor-studies-how-utilitarianism-provides-framework-major-policy-decisions>; N. Gregory Mankiw, “When the Scientist Is

on by policy- and lawmakers when regulating technology as well. But because technologies develop faster or in unexpected directions, regulation often arrives too late or in a form that does not encompass all the effects of the technology in question. Furthermore, the work that goes into calculating probabilities and researching the possible outcomes in a utilitarian approach is very time- and resource-consuming, which further delays legislation and/or regulation.

It is outside the scope of this dissertation to argue for superiority of one set of ethics over another, and I make no claims that deontology is preferable over utilitarianism in this regard. It also requires much more development than it is appropriate to include in this dissertation to ascertain its viability, but never the less, I would like to briefly introduce the notion of how a deontological approach to technology policy-making may reduce the “law lag”. By requiring developing technologies to adhere to certain already developed principles of justice and fairness, evaluation of the technology’s value to society may be less time-consuming. Of course, as in Rawlsian contractarianism, these principles would have to be adjusted over time, according to how society develops, but they would still be grounded in principles that have been set for the desired structure in society. Conceptual evaluations based on methods such as The Rawls Test could be employed to get to an understanding of a technology’s immediate value for society and how it should be regulated. Pervasive use of such methods would likely force technology companies to think these kinds of principles into their development, so that compliance would not have to be implemented afterwards, which is a much more expensive process. Another effect would likely be a slowdown of technological development and innovation, and there are those

Also a Philosopher,” The New York Times, 2014, https://www.nytimes.com/2014/03/23/business/economic-view-when-the-scientist-is-also-a-philosopher.html?_r=0.

that would argue that this should exclude deontology from consideration as a foundation for policy-making in technology. But the question is whether that trade-off is such a bad thing, considering the worries and critiques of artificial intelligence and algorithms that is currently being leveled at the tech industry.⁷⁰⁸ It is not a question of holding back technological development, but doing it right the first time around, rather than having to spend resources on corrections later.

This is naturally a much more complex issue than I am able to describe in a section of a conclusion in a dissertation about something else. But it is a compelling case for further research work that could take into account these economic and political aspects of adopting Rawlsian principles when regulating technology.

The Return of Rawls

As mentioned at the outset of this dissertation, Rawls' work is having something of a renaissance, after having been slightly unfashionable in academic circles since Rawls' death in 2002. As mentioned in Chapter 2, I attribute much of this to new developments in technology leading to changes in the ways we consume and produce data and information (or the other way around, depending on your view of technological determinism). After a period of exuberant fascination over the prospects as well as results of technological achievements, enough events have now occurred of a less desirable nature to raise questions about how we wish to understand and live with technology. At the time of writing, the debate about ethics in Computer Science

⁷⁰⁸ Roberts, "Commercial Content Moderation: Digital Laborers' Dirty Work"; Staff, "Engine Failure"; Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*.

fills the media, but rarely does the debate ask which ethics should be employed. As this study shows, there are many different value sets at play when it comes to regulating media and technology in general, and social media in particular.

My mission with this study has been to show the viability of basing technology ethics on Rawls' contractarian/deontological work. But even if my arguments here have not been convincing, I have at least shown that there are alternatives to the current, dominant heuristic of utilitarianism worth considering. Additionally, this dissertation shows that national social media policies reach beyond protecting the personal information of the user, beyond regional national security interests. Because social media have become as pervasive and integral to the way the world communicates, the ethics we apply to them addresses and raises questions on topics of the most basic kind about being a citizen of the modern world: Freedom, personhood, identity and human rights.

On those subjects, this work constitutes only very few of the first words spoken in what will be a very long conversation.

Appendix A: List of Interviewees with biographies

Esha Bhandari

Esha Bhandari is a staff attorney with the ACLU Speech, Privacy, and Technology Project, where she focuses on litigation and advocacy relating to online speech, academic freedom, privacy rights, and the impact of big data. Esha was previously an Equal Justice Works fellow with the ACLU Immigrants' Rights Project, where she was involved in litigating cases concerning a right to counsel in immigration proceedings, detainer policies, and discriminatory state and local laws. She has also been a staff attorney at the Center for Reproductive Rights, where she worked on two trials challenging a Texas law limiting women's access to reproductive health care. Esha is a graduate of McGill University, the Columbia University Graduate School of Journalism, and Columbia Law School, and served as a law clerk to the Hon. Amalya L. Kearsse of the U.S. Court of Appeals for the Second Circuit.

Susanne Chan

Susanne Chan is a Senior Lecturer in Sociology at Hong Kong University's HKU Space. She has written extensively in American media about the effects of newly introduced cybersecurity legislation in China as well as the organization of the Chinese agencies, ministries and organizations that regulate the Internet in the country. She holds master's degrees in sociology from both Hong Kong University and University of California Los Angeles.

Dr. Yubo Kou

Yubo Kou is a Chinese postdoctoral research associate in the UX Pedagogy and Practice Lab at Purdue University. Kou has done extensive research in HCI, online communities, and social media with qualitative and quantitative methods with a focus on China. He received a Ph.D. degree in information and computer sciences under the supervision of Dr. Bonnie Nardi from the Department of Informatics at the University of California, Irvine. In his dissertation research, he explored how the behavior and attitudes of Chinese social media users is influenced by Confucianism. He has a M.S. degree in computer science under the supervision of Dr. Xiaofeng Meng from Renmin University of China, and a B.A. degree in linguistics from Peking University.

Dr. Martin Libicki

Martin Libicki (Ph.D., U.C. Berkeley 1978) holds the Keyser Chair of cybersecurity studies at the U.S. Naval Academy and is adjunct senior management scientist at the RAND Corporation. He carries out research in cyberwar and the general impact of information technology on domestic and national security. He is the author of a 2016 textbook on cyberwar, *Cyberspace in Peace and War*, as well as two others commercially published books, *Conquest in Cyberspace: National Security and Information Warfare*, and *Information Technology Standards: Quest for the Common Byte*). He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, *Crisis and Escalation in Cyberspace*, *Global Demographic Change and its Implications for Military Power*, *Cyberdeterrence and Cyberwar*, *How Insurgencies End* (with Ben Connable), and *How Terrorist Groups End* (with Seth Jones).

Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

Henrik Moltke

Henrik Moltke is an award-winning investigative journalist, researcher, and filmmaker. He is one of a very few select researchers to have access to the Snowden archive, the trove of documents obtained and leaked by former defense contractor Edward Snowden in 2013. Moltke works for the news outlet ProPublica, but his recent work has also appeared in The New York Times and The Intercept. He has formerly worked for a number of Danish news outlets such as national broadcaster DR and the newspaper Information. As a filmmaker and artist, his work has been exhibited at the Whitney Museum and at the Sundance Film Festival. Moltke won the 2014 Danish Investigative Journalism Award and co-directed Project X, with Laura Poitras. He also worked with Poitras on the Academy Award-winning documentary, Citizen Four.

Thomas Elkjer Nissen

Thomas Elkjer Nissen, MA, has worked at the Royal Danish Defence College (RDDC) since 2001 as a Subject Matter Expert responsible for Strategic Communication (StratCom), Information Operations (Info Ops) and Psychological Operations (PsyOps). He conducts research, advises and teaches in the fields of Info Ops, PsyOps, Media Operations (Public Affairs) and the military's role in Strategic Communications and Public/Defence Diplomacy. As the author of what is the most authoritative textbook currently available on warfare and social media, #TheWeaponizationOfSocialMedia , he is considered one of the world's foremost experts on that subject.

Dr. Margaret E. Roberts

Margaret E. Roberts is an Assistant Professor in the Department of Political Science at the University of California, San Diego. Her research interests lie in the intersection of political methodology and the politics of information, with a specific focus on methods of automated content analysis and the politics of censorship in China. She is the author of the 2018 book *Censored: Distraction and Diversion Inside China's Great Firewall* and is the author or co-author of numerous published studies exploring the impact of Chinese censorship on citizens' rights and access to information inside China.

The Hon. Adam Schiff

Congressman Adam Schiff represents California's 28th Congressional District. In his 9th term in the House of Representatives, Schiff currently serves as the Ranking Member, or top Democrat, of the House Permanent Select Committee on Intelligence and as a Member of the Benghazi Select Committee. The House Permanent Select Committee on Intelligence oversees the nation's intelligence agencies including components of the Departments of Defense, Homeland Security, Justice, State and Energy. Schiff is currently on a leave of absence from the House Appropriations Committee. Prior to serving in the House of Representatives, Schiff completed a four-year term as State Senator for California's 21st State Senate District, chairing the Senate Judiciary Committee, the Senate Select Committee on Juvenile Justice and the Joint Committee on the Arts. Before serving in the Legislature, Schiff served with the U.S. Attorney's Office in Los Angeles for six years, most notably prosecuting the first FBI agent ever to be indicted for espionage. He is a graduate of Stanford University and Harvard Law School.

Dr. Margo Schlanger

Margo Schlanger is the Wade H. and Dores M. McCree Collegiate Professor of Law at the University of Michigan's Law School. She is a leading authority on civil rights issues and civil and criminal detention. Her teaching and research deal with civil rights, prison reform, torts, and surveillance. She also founded and heads the Civil Rights Litigation Clearinghouse. She is the court-appointed settlement monitor for *Adams v. Kentucky Department of Corrections*, a statewide civil rights lawsuit dealing with conditions of confinement for Kentucky's deaf prisoners. Before starting at Michigan, she was a professor at Washington University in St. Louis and an assistant professor at Harvard Law School. In 2010 and 2011, Professor Schlanger was on leave, serving as the presidentially appointed Officer for Civil Rights and Civil Liberties at the U.S. Department of Homeland Security (DHS). As the head of civil rights and civil liberties for DHS, she was the secretary's lead adviser on civil rights and civil liberties issues

Dr. Rebecca Slayton

Rebecca Slayton is associate professor of Science and Technology Studies at Cornell University. Her research and teaching examine the relationships between and among risk, governance, and expertise, with a focus on international security and cooperation since World War II. Her first book, *Arguments that Count: Physics, Computing, and Missile Defense, 1949-2012* (MIT Press, 2013), shows how the rise of a new field of expertise in computing reshaped public policies and perceptions about the risks of missile defense in the United States. In 2015, *Arguments that*

Count won the Computer History Museum Prize. Slayton's second book project, *Shadowing Cybersecurity*, examines the emergence of cybersecurity expertise through the interplay of innovation and repair. Slayton is also working on a third project which examines tensions intrinsic to the creation of a "smart" electrical power grid—i.e. a more sustainable, reliable, and secure grid. Both of these current projects are supported by a five-year National Science Foundation CAREER award, "Enacting Cybersecurity Expertise." Slayton is also a project lead on research funded by a Department of Homeland Security Center of Excellence, the Critical Infrastructure Resilience Institute.

Bibliography

- Abizadeh, Arash. "Historical Truth, National Myths and Liberal Democracy: On the Coherence of Liberal Nationalism." *Journal of Political Philosophy* 12, no. 3 (2004): 291–313.
<https://doi.org/10.1111/j.1467-9760.2004.00201.x>.
- ACLU. "Fighting Voter Suppression | American Civil Liberties Union." ACLU.org, 2018.
<https://www.aclu.org/issues/voting-rights/fighting-voter-suppression>.
- . "Surveillance Under the Patriot Act | American Civil Liberties Union." ACLU.org. Accessed March 11, 2018. <https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>.
- Acquisti, Alessandro, and Christina M. Fong. "An Experiment in Hiring Discrimination Via Online Social Networks." *SSRN Electronic Journal*, July 17, 2012.
<https://doi.org/10.2139/ssrn.2031979>.
- Acquisti, Alessandro, Allan Friedman, and Rahul Telang. "Is There a Cost to Privacy Breaches? An Events Study." *Fifth Workshop on the Economics of Information Security*, 2006, 1--20.
<https://doi.org/10.1.1.73.2942>.
- Aichner, Thomas, and Frank Jacob. "Measuring the Degree of Corporate Social Media Use." *International Journal of Market Research* 57, no. 2 (March 1, 2015): 257–76.
<https://doi.org/10.2501/IJMR-2015-018>.
- Ainsley, Julia, and Robert Windrem. "New Report Says Most U.S. Terrorists Foreign Born, but Check the Fine Print." NBC News, 2018. <https://www.nbcnews.com/news/us-news/new-report-says-most-u-s-terrorists-foreign-born-check-n838041>.

- ALA. "Code of Ethics of the American Library Association." *ALA Code of Ethics*, 2008, 1.
<http://www.ala.org/advocacy/proethics/codeofethics/codeethics>.
- Albrechtslund, Anders. "Online Social Networking as Participatory Surveillance." *First Monday*, 2008. <http://journals.uic.edu/ojs/index.php/fm/article/view/2142/1949>.
- Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives—Volume 31*, no. 2—Spring (2017): 211–36.
<https://doi.org/10.1257/jep.31.2.211>.
- American Library Association Office for Intellectual Freedom. *Intellectual Freedom Manual Ninth Edition. Intellectual Freedom Manual (9th Edition)*, 2015. https://carleton-primo.hosted.exlibrisgroup.com/primo-explore/fulldisplay?docid=01BRC_CCO_ALMA51385855100002971&vid=01BRC_CCO&search_scope=Everything&tab=default_tab&lang=en_US.
- Ames, Roger T. *Confucian Role Ethics: A Vocabulary*. Chinese University Press, 2011.
- Amnesty International. "Russian Federation 2016/2017." Accessed February 4, 2018.
<https://www.amnesty.org/en/countries/europe-and-central-asia/russian-federation/report-russian-federation/>.
- Anzuoni, Mario. "Report: San Bernardino Shooter Made Social Media Contact with Extremists." *Newsweek*, 2015. <http://www.newsweek.com/report-san-bernardino-shooter-made-social-media-contact-extremists-400708>.
- Armerding Taylor. "NSA Surveillance Controversy: Much Ado about Nothing New?" *CSO*, 2013. <https://www.csoonline.com/article/2133558/strategic-planning-erm/nsa-surveillance-controversy--much-ado-about-nothing-new-.html>.

Arrow, Kenneth J. "Some Ordinalist-Utilitarian Notes on Rawls's Theory of Justice." *The Journal of Philosophy* 70, no. 9 (1973): 245–63. <http://www.jstor.org/stable/2025006>.

Ash, Lucy. "How Russia Outfoxes Its Enemies." BBC News Magazine Online, 2015. <http://www.bbc.com/news/magazine-31020283>.

Ashcroft, John. "Testimony of Attorney General John Ashcroft Senate Committee on the Judiciary 12-06-01." 2001. <https://www.justice.gov/archive/ag/testimony/2001/1206transcriptsenatejudiciarycommittee.htm>.

Atkin, Michelle Louise. *Balancing Liberty and Security: An Ethical Study of US Foreign Intelligence Surveillance, 2001-2009*. Vol. 15. Rowman & Littlefield Publishers, 2013.

Audenhove, Leo Van, Debra M Clarke, Banu Durda, Nova M Gordon-Bell, Rob Heyman, Ilse Mariën, Glenn W Muschert, et al. *Social Inequalities, Media, and Communication: Theory and Roots*. Lexington Books, 2016.

Australian Law Reform Commission. "A Common Law Right." ALRC.gov.au, 2018. <https://www.alrc.gov.au/publications/common-law-right>.

Ayres, Sabra. "Putin Denies a Russian State Role in U.S. Election, but Says 'patriotic' Hackers May Have Mounted Attacks." LATimes.com, 2017. <http://www.latimes.com/world/la-fg-putin-russia-hacking-20170601-story.html>.

Azari, Julia. "From Wallace To Trump, The Evolution of 'Law And Order.'" FiveThirtyEight, 2016. <https://fivethirtyeight.com/features/from-wallace-to-trump-the-evolution-of-law-and-order/>.

Azrael, Jeremy. "The KGB in Kremlin Politics," 1989.

- Bailyn, Bernard. *The Ideological Origins of the American Revolution*. Harvard University Press, 2017.
- Bandurski, David. "Supervising Supervision." China Media Project, 2016.
<https://medium.com/china-media-project/supervising-supervision-6812858d5828>.
- Barmé, Geremie, and Sang Ye. "The Great Firewall of China." *Wired*, 1997.
<https://www.wired.com/1997/06/china-3/>.
- Baron, Jonathan. "Nonconsequentialist Decisions." *Behavioral and Brain Sciences* 17, no. 01 (March 4, 1994): 1. <https://doi.org/10.1017/S0140525X0003301X>.
- Baron, Jonathan, and Brian Cohen. "Why Expected Utility Theory Is Normative, but Not Prescriptive." *Medical Decision Making* 16, no. 1 (1996): 7–9.
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.903.4852&rep=rep1&type=pdf>.
- Barron, John. "KGB." In *The Penguin Book of Lies*, edited by Hodder and Stoughton, 420–23. Penguin, 1974.
- Bartles, Charles K. "Getting Gerasimov Right." *Military Review*, no. January-February (2016).
http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf.
- Bauman, Zygmunt. "Glocalization and Hybridity." *Glocalism: Journal of Culture, Politics and Innovation* 1, no. 1 (2013): 1–5. <https://doi.org/10.12893/gjcpi.2013.1.9>.
- Bawden, David, and Lyn Robinson. "The Dark Side of Information: Overload, Anxiety and Other Paradoxes and Pathologies." *Journal of Information Science* 35, no. 2 (2009): 180–91. <https://doi.org/10.1177/0165551508095781>.
- Bay, Morten. *Homo Conexus*. Lulu. com, 2013.

- . “The Ethics of Psychometrics in Social Media: A Rawlsian Approach.” In *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.
- . “The Ethics of Unbreakable Encryption: Rawlsian Privacy and the San Bernardino iPhone.” *First Monday* 22, no. 2 (2017).
- . “What Is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era.” *French Journal For Media Research Special Is*, no. 6 (2016): 1–28.
- Bay, Morten, and Isaac R. Porsche III. “West Can’t Ignore Islamic State Social Media War | World Report | US News.” U.S. News and World Report, 2015.
<https://www.usnews.com/opinion/blogs/world-report/2015/07/23/west-cant-ignore-islamic-state-social-media-war>.
- Bay, Morten, and Julie Ralund. *Generation Netværk*. Copenhagen, Denmark: DR, 2006.
- Baym, Nancy K. *Tune in, Log on: Soaps, Fandom, and Online Community*. Vol. 3. Sage, 2000.
- Beauchamp, Zack. “Brexit Was Fueled by Irrational Xenophobia, Not Real Economic Grievances - Vox.” Vox.com, 2016. <https://www.vox.com/2016/6/25/12029786/brexit-uk-eu-immigration-xenophobia>.
- Beck, Ulrich. “Risk Society: Towards a New Modernity.” *Nation*, 1992.
<https://doi.org/10.2307/2579937>.
- Beckett, Nick, and Amanda Ge. “CNNIC Publishes the 41st Statistical Report on China’s Internet Development in China.” Lexology, 2018.
<https://www.lexology.com/library/detail.aspx?g=911ae57f-50da-4c53-ab75-2376272b2021>.
- Bell-Villada, Gene H. “Who Is John Galt? Ayn Rand, Libertarians and the GOP.” *The Conversation*, 2015. <http://theconversation.com/who-is-john-galt-ayn-rand-libertarians-and->

the-gop-40033.

Bender, Jacqueline Lorene, Alaina B Cyr, Luk Arbuckle, and Lorraine E Ferris. “Ethics and Privacy Implications of Using the Internet and Social Media to Recruit Participants for Health Research: A Privacy-by-Design Framework for Online Recruitment.” *Journal of Medical Internet Research* 19, no. 4 (April 6, 2017): e104.
<https://doi.org/10.2196/jmir.7029>.

Bertram, Christoph. “Globalization Means Westernization by Christoph Bertram - Project Syndicate.” Project Syndicate, 1998. <https://www.project-syndicate.org/commentary/globalization-means-westernization?barrier=accessreg>.

Bertram, Christopher. “Jean Jacques Rousseau.” Stanford Encyclopedia of Philosophy. Stanford University, 2017. <https://plato.stanford.edu/entries/rousseau/>.

Bertrand, Natasha. “After Facebook-Russia Bombshell, Dems Urge FEC to Regulate Political Ads - Business Insider.” Business Insider, 2017. <http://www.businessinsider.com/facebook-russia-investigation-fec-political-ads-2017-9>.

Bessi, Alessandro, and Emilio Ferrara. “Social Bots Distort the 2016 U.S. Presidential Election Online Discussion.” *First Monday* 21, no. 11 (2016).
<https://doi.org/10.5210/fm.v21i11.7090>.

Best, Michael L. “The Internet That Facebook Built.” *Communications of the ACM* 57, no. 12 (November 26, 2014): 21–23. <https://doi.org/10.1145/2676857>.

Bhandari, Esha. “Interview March 8, 2018,” 2018.

Bittman, Ladislav. “The Use of Disinformation by Democracies.” *International Journal of Intelligence and CounterIntelligence*, 1990. <https://doi.org/10.1080/08850609008435142>.

- Bixby, Scott, and David Agren. "Trump Reveals Plan to Finance Mexico Border Wall with Threat to Cut off Funds." *The Guardian*, 2016. <https://www.theguardian.com/us-news/2016/apr/05/donald-trump-mexico-border-wall-plan-remittances>.
- Boczek, Boleslaw A. "Resource Rivalry in the Third World," 1984.
- Boer, Roland. "Confucius and Chairman Mao: Towards a Study of Religion and Chinese Marxism." Accessed February 24, 2018. <http://crisiscritique.org/uploads-new/BOER.pdf>.
- Bogdan-Martin, Doreen, Christophe Larouer, Catalin Marinescu, Francois Rancy of ITU, Joe Hironaka, Bullet Harald Edquist, Heather Johnson, et al. "The State of Broadband 2017: Broadband Catalyzing Sustainable Development," 2017. https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf.
- Boghardt, Thomas. "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign." *Studies in Intelligence* 53, no. 4 (2009).
- Bolger, Daniel T. "Book Review: Guerrilla Warfare and Counterinsurgency: U.S.-Soviet Policy in the Third World." *Parameters - US Army War College Quarterly*, no. June (1990).
- Bomford, Andrew. "Echelon Spy Network Revealed." BBC, 1999.
<http://news.bbc.co.uk/2/hi/503224.stm>.
- Bonilla, Yarimar, and Jonathan Rosa. "# Ferguson: Digital Protest, Hashtag Ethnography, and the Racial Politics of Social Media in the United States." *American Ethnologist* 42, no. 1 (2015): 4–17.
- Bose, Utpal. "An Ethical Framework in Information Systems Decision Making Using Normative Theories of Business Ethics." *Ethics and Information Technology* 14, no. 1 (2012): 17–26.
<https://doi.org/10.1007/s10676-011-9283-5>.

- Boyd, Danah, and Kate Crawford. "CRITICAL QUESTIONS FOR BIG DATA Provocations for a Cultural, Technological, and Scholarly Phenomenon." *Communication & Society* 15, no. 5 (1986): 545–662. <https://doi.org/10.1080/1369118X.2012.678878>.
- boyd, danah m., and Nicole B. Ellison. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13, no. 1 (October 1, 2007): 210–30. <https://doi.org/10.1111/j.1083-6101.2007.00393.x>.
- Boym, Svetlana. *Common Places: Mythologies of Everyday Life in Russia*. Harvard University Press, 2009.
- Bradshaw, P, and P Bradshaw. "Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation" 2017.12 (2017): 1–37. <https://doi.org/http://comprop.oii.ox.ac.uk/>.
- Brettel, Malte, Jens Christian Reich, Jose M. Gavilanes, and Tessa C. Flatten. "What Drives Advertising Success on Facebook? An Advertising-Effectiveness Model: Measuring the Effects on Sales of 'Likes' and Other Social-Network Stimuli." *Journal of Advertising Research* 55, no. 2 (2015): 162–75. <https://doi.org/10.2501/JAR-55-2-162-175>.
- Brown, Caroline, Anna Kraus, and Philip Pesich. "Regulations Lag Behind 'Telehealth' Technology | National Law Journal." *The National Law Journal*, 2015. <https://www.law.com/nationallawjournal/almID/1202719886237/?slreturn=20180302141303>.
- Brown, Gary, and Christopher D Yung. "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace | The Diplomat." *The Diplomat*, 2017. <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1->

the-us-approach-to-cyberspace/.

Buckley, Chris, and Keith Bradsher. “China Moves to Let President Xi Stay In Power, Ending Term Limit.” *The New York Times*, 2018.

Buijs, Arjen E. “Public Support for River Restoration. A Mixed-Method Study into Local Residents’ Support for and Framing of River Management and Ecological Restoration in the Dutch Floodplains.” *Journal of Environmental Management* 90, no. 8 (2009): 2680–89. <https://doi.org/10.1016/j.jenvman.2009.02.006>.

Burrell, Jenna. “How the Machine ‘Thinks’: Understanding Opacity in Machine Learning Algorithms.” Accessed April 4, 2018. <https://doi.org/10.1177/2053951715622512>.

Butsenko, Anton. “Тролли Из Ольгино Переехали в Новый Четырехэтажный Офис На Савушкина.” *DP.ru*, 2014. https://m.dp.ru/a/2014/10/27/Borotsja_s_omerzeniem_mo.

Byrne, Dara N. “Public Discourse, Community Concerns, and Civic Engagement: Exploring Black Social Networking Traditions on BlackPlanet.Com.” Accessed March 18, 2018. <https://doi.org/10.1111/j.1083-6101.2007.00398.x>.

Campbell, Duncan. “Global Spy System ECHELON Confirmed at Last – by Leaked Snowden Files • The Register.” *The Register*, 2015. http://www.theregister.co.uk/2015/08/03/gchq_duncan_campbell/.

Caney, Simon. “Liberalism and Communitarianism: A Misconceived Debate.” *Political Studies* 40, no. 2 (1992): 273–89. <https://doi.org/10.1111/j.1467-9248.1992.tb01384.x>.

Cantú, Aaron, and George Joseph. “Trump’s Border Security May Search Your Social Media by ‘Tone.’” *The Nation*, 2017. <https://www.thenation.com/article/trumps-border-security-may-search-your-social-media-by-tone/>.

- Carbaugh, Donal. "'Soul' and 'Self': Soviet and American Cultures in Conversation." *Quarterly Journal of Speech* 79 (1993): 182–200.
<http://www.tandfonline.com/doi/pdf/10.1080/00335639309384028>.
- Carney, Nikita. "All Lives Matter, but so Does Race." *Humanity & Society* 40, no. 2 (May 13, 2016): 180–99. <https://doi.org/10.1177/0160597616643868>.
- Cashmore, Pete. "MySpace Hits 100 Million Accounts." Mashable, 2006.
<https://mashable.com/2006/08/09/myspace-hits-100-million-accounts/#vRglqLpSS5qj>.
- Castells, M. "The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance." *The ANNALS of the American Academy of Political and Social Science* 616, no. March (2008): 78–93. <https://doi.org/10.1177/0002716207311877>.
- Central Intelligence Agency. "Russia." The World Factbook. Accessed February 4, 2018.
<https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html>.
- Chafkin, Max. "How to Kill a Great Idea." Inc., 2007.
<https://www.inc.com/magazine/20070601/features-how-to-kill-a-great-idea.html>.
- Chan, Alex. "From Propaganda to Hegemony: Jiaodian Fangtan and China's Media Policy." *Journal of Contemporary China* 11, no. 30 (2002): 35–51.
<https://doi.org/10.1080/10670560120091138>.
- Chan, Susanne. "Cybersecurity under Xi Jinping: A New Model for Broad Control in China." Center for the Digital Future, 2018. <http://www.digitalcenter.org/columns/cybersecurity-under-xi/>.
- . "Interview, 2/27/2018," 2018.
- Chang, Alexandra. "Why IDC Predicts Windows Phone Will Surpass IOS by 2016." Wired.com,

2012. <https://www.wired.com/2012/06/why-idc-predicts-windows-phone-will-surpass-ios-by-2016/>.

Chapman, Steve. "Trump, the Wimp - Chicago Tribune." Chicago Tribune, 2018.

<http://www.chicagotribune.com/news/opinion/chapman/ct-perspec-chapman-trump-weak-russia-north-korea-201803186-story.html>.

Chen, Adrian. "The Agency." The New York Times Magazine, 2015.

<https://www.nytimes.com/2015/06/07/magazine/the-agency.html>.

Chen, Celia, and Iris Deng. "Weibo, Tencent Volunteer to Clean up Content as China Intensifies

Crackdown." South China Morning Post, 2018. [http://www.scmp.com/tech/china-](http://www.scmp.com/tech/china-tech/article/2141375/chinese-social-media-platforms-volunteer-clean-content-crackdown)

[tech/article/2141375/chinese-social-media-platforms-volunteer-clean-content-crackdown](http://www.scmp.com/tech/china-tech/article/2141375/chinese-social-media-platforms-volunteer-clean-content-crackdown).

Chen, George. "China to Lift Ban on Facebook – but Only within Shanghai Free-Trade Zone."

South China Morning Post, 2013.

<http://www.scmp.com/news/china/article/1316598/exclusive-china-lift-ban-facebook-only-within-shanghai-free-trade-zone>.

Chevalier, Michel. *Society Manners and Politics in the United States: Letters on North America (1840)*. Vol. 83. Ayer Publishing, 1969.

Choptiany, Leonard. "A Critique of John Rawls's Principles of Justice." *Ethics* 83, no. 2

(January 19, 1973): 146–50. <https://doi.org/10.1086/291872>.

Chotikul, Ddiane. "The Soviet Theory of Reflexive Control in Historical and Psychocultural

Perspective: Preliminary Study," 1986.

Chu, Leonard L. "Continuity and Change in China's Media Reform." *Journal of Communication*

44, no. 3 (1994): 4–21.

Coalition. “Coalition Letter Opposing DHS Social Media Retention | Center for Democracy & Technology.” cdt.org, 2017. <https://cdt.org/insight/coalition-letter-opposing-dhs-social-media-retention/>.

Coleman, E. Gabriella. “Ethnographic Approaches to Digital Media.” *Annual Review of Anthropology* 39, no. 1 (October 21, 2010): 487–505.
<https://doi.org/10.1146/annurev.anthro.012809.104945>.

Communist Party of China. “The Decision on Major Issues Concerning Comprehensively Deepening Reforms in Brief- China.Org.Cn.” China Daily, 2013.
http://china.org.cn/china/third_plenary_session/2013-11/16/content_30620736_3.htm.

“Compelled Speech - Dictionary Definition of Compelled Speech.” *Encyclopedia of the American Constitution*. The Gale Group, 2000.
<https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/compelled-speech>.

Condon, Madison. “China in Africa: What the Policy of Nonintervention Adds to the Western Development Dilemma.” *PRAXIS The Fletcher Journal of Human Security* 27 (2012).
<http://fletcher.tufts.edu/~media/Fletcher/Microsites/praxis/xxvii/2CondonChinaAfrica.pdf>.

Connelly, Patrick. “John Locke.” The internet encyclopedia of philosophy. Internet Encyclopedia of Philosophy Pub. Accessed April 4, 2018. <http://www.iep.utm.edu/locke/>.

Cooney, Maureen. “Data Mining Report DHS Privacy Office Response to House Report 108-774 Report to Congress on the Impact of Data Mining Technologies on Privacy and Civil Liberties Respectfully Submitted,” 2006.
https://www.dhs.gov/sites/default/files/publications/privacy_data_mining_report_0.pdf.

- Cope, Sophia, Amul Kalia, Seth Schoen, and Adam Schwartz. “Digital Privacy at the U.S. Border: Protecting the Data On Your Devices | Electronic Frontier Foundation.” *Eff.Org*, 2017. <https://www.eff.org/wp/digital-privacy-us-border-2017>.
- Cope, Sophia, and Adam Schwartz. “DHS Should Stop the Social Media Surveillance of Immigrants | Electronic Frontier Foundation.” EFF.org, 2017. <https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants>.
- Cox, James. “Canada and the Five Eyes Intelligence Community,” 2012. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.357.5576&rep=rep1&type=pdf>.
- Crowcroft, Jon, and Philippe Oechslin. “Differentiated End-to-End Internet Services Using a Weighted Proportional Fair Sharing TCP.” *ACM SIGCOMM Computer Communication Review* 28, no. 3 (1998): 53–69. <https://doi.org/10.1145/293927.293930>.
- Crowley, Michael. “The Kremlin’s Candidate.” *POLITICO Magazine*, 2016. <https://www.politico.com/magazine/story/2016/04/donald-trump-2016-russia-today-rt-kremlin-media-vladimir-putin-213833>.
- Cruz, Ted. “Letter to Secretary Johnson.” U.S. Senate, 2016. https://www.cruz.senate.gov/files/documents/Letters/20160122_TerrorismLetterUSCISFDNSSocialMediaUsage.pdf.
- Cui, Di, and Fang Wu. “Moral Goodness and Social Orderliness: An Analysis of the Official Media Discourse about Internet Governance in China.” *Telecommunications Policy* 40, no. 2–3 (2016): 265–76. <https://doi.org/10.1016/j.telpol.2015.11.010>.
- Dasgupta, Saibal. “China Reducing Massive Influence of Social Media Celebrities.”

VOAnews.com, 2017. <https://www.voanews.com/a/china-social-media-celebrities/3942435.html>.

Daviter, Falk. "Policy Framing in the European Union." *Journal of European Public Policy* 14, no. 4 (2007): 654–66. <https://doi.org/10.1080/13501760701314474>.

Dean, Geoff, Peter Bell, and Jack Newman. "The Dark Side of Social Media: Review of Online Terrorism." *Pakistan Journal of Criminology* 3/4 (2012): 191–210.

<http://search.ebscohost.com/login.aspx?direct=true&db=i3h&AN=89690880&site=ehost-live>.

Dehghani, Milad, and Mustafa Tumer. "A Research on Effectiveness of Facebook Advertising on Enhancing Purchase Intention of Consumers." *Computers in Human Behavior* 49 (2015): 597–600. <https://doi.org/10.1016/j.chb.2015.03.051>.

Delaney, James. "Jean-Jacques Rousseau (1712—1778)." *The Internet Encyclopedia of Philosophy*. Internet Encyclopedia of Philosophy Pub. Accessed March 10, 2018. <https://www.iep.utm.edu/rousseau/>.

Department of Homeland Security. "DHS Media Monitoring Desktop Reference Manual | Public Intelligence." *Public Intelligence*, 2012. <https://publicintelligence.net/dhs-media-monitoring-desktop-reference-manual/>.

———. "History | Homeland Security." *DHS.gov*. Accessed March 12, 2018. <https://www.dhs.gov/history>.

———. "Privacy Act of 1974; System of Records." *Federal Register*, 2017. <https://www.federalregister.gov/documents/2017/09/18/2017-19365/privacy-act-of-1974-system-of-records>.

- DHS.gov. "Who Joined DHS | Homeland Security." DHS.gov. Accessed March 12, 2018.
<https://www.dhs.gov/who-joined-dhs>.
- Diamond, Jeremy. "Donald Trump: Ban All Muslim Travel to U.S." CNN.com, 2015.
<https://www.cnn.com/2015/12/07/politics/donald-trump-muslim-ban-immigration/index.html>.
- Dickinson Steve. "China's New Online Publishing Rules." China Law Blog, 2016.
<https://www.chinalawblog.com/2016/03/chinas-new-online-publishing-rules-another-nail-in-the-vie-coffin.html>.
- Diepenbrock, George. "Professor Studies How Utilitarianism Provides Framework for Major Policy Decisions | The University of Kansas." Kansas University News, 2014.
<https://news.ku.edu/2014/06/02/professor-studies-how-utilitarianism-provides-framework-major-policy-decisions>.
- Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT press, 2010.
- Dijk, José van. "'You Have One Identity': Performing the Self on Facebook and LinkedIn." *Media, Culture and Society* 35, no. 2 (2013): 199–215.
<https://doi.org/10.1177/0163443712468605>.
- Dijk, José Van. *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press, 2013.
- Dirlik, Arif. "Confucius in the Borderlands : Global Capitalism and the Reinvention of Confucianism." *Boundary* 2 22, no. 3 (1995): 229–73.
- Diuk, Nadia. *The next Generation in Russia, Ukraine, and Azerbaijan: Youth, Politics, Identity*,

- and Change*. Rowman & Littlefield, 2012.
- Dogcow, laslo, and Robert Kemp. “Jam Echelon Day - 21st Oct 1999.” Thing.net, 1999.
<https://www.thing.net/~rdom/ecd/jam.html>.
- Donnelly, Brendan. “A Chaotic Brexit Is Still a Possibility.” *LSE Brexit*, 2017, 1–4.
- Dostal, Jörg Michael. “Campaigning on Expertise: How the OECD Framed EU Welfare and Labour Market Policies - And Why Success Could Trigger Failure.” *Journal of European Public Policy*, 2004. <https://doi.org/10.1080/13501760410001694255>.
- Doyle, Thomas E. “When Liberal Peoples Turn into Outlaw States: John Rawls’ Law of Peoples and Liberal Nuclearism.” *Journal of International Political Theory* 11, no. 2 (June 9, 2015): 257–73. <https://doi.org/10.1177/1755088215571648>.
- Drahos, Peter. “A Philosophy of Intellectual Property, Dartmouth.” *Aldershot, UK and Brookfield, US*, 1996.
- Duff, Alistair. “Neo-Rawlsian Co-Ordinates: Notes on A Theory of Justice for the Information Age.” *International Review of Information Ethics* 6 (2006): 12. <http://fiz1.fh-potsdam.de/volltext/ijie/07243.pdf>.
- Dui Hua Foundation. “Article 293: Deeming Free Speech Disorder in Internet Space.” *Dui Hua Human Rights Journal*, 2015. <https://www.duihuahrjournal.org/2015/03/article-293-deeming-free-speech.html>.
- Duncan, Stewart. “Thomas Hobbes.” *Stanfor Encyclopedia of Philosophy*. Stanford University, 2017. <https://plato.stanford.edu/entries/hobbes/>.
- Dunlap Jr., Charles J. “‘Cybervandalism’ or ‘Digital Act of War?’ America’s Muddled Approach to Cyber Incidents Will Not Deter More Crises.” *North Carolina Journal of International*

Law 42, no. 4 (2017): 989–1012.

https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=6455&context=faculty_scholarship.

Dzhirkvelov, Ilya. *Secret Servant My Life with the KGB and the Soviet Elite*. London: Collins, 1987.

Eggleston, Ben, and Dale E Miller. *The Cambridge Companion to Utilitarianism*. Cambridge University Press, 2014.

Elgebeily, Sherif A. “How China’s Foreign Policy of Non-Intervention Is All about Selective Action.” *South China Morning Post*, 2017. <http://www.scmp.com/comment/insight-opinion/article/2091502/how-chinas-foreign-policy-non-intervention-all-about>.

EPIC. “‘National Network’ of Fusion Centers Raises Specter of COINTELPRO.” *Spotlight on Surveillance*, 2007. <https://epic.org/privacy/surveillance/spotlight/0607/>.

Erickson, Amanda. “If Russia Today Is Moscow’s Propaganda Arm, It’s Not Very Good at Its Job.” *The Washington Post*, 2017.

https://www.washingtonpost.com/news/worldviews/wp/2017/01/12/if-russia-today-is-moscows-propaganda-arm-its-not-very-good-at-its-job/?utm_term=.0aa08dbd15f4.

Eschenfelder, Kristin R., Robert Glenn Howard, and Anuj C. Desai. “Who Posts DeCSS and Why?: A Content Analysis of Web Sites Posting DVD Circumvention Software.” *Journal of the American Society for Information Science and Technology* 56, no. 13 (2005): 1405–18. <https://doi.org/10.1002/asi.20234>.

Etzioni, Amitai. “Communitarianism.” In *Encyclopedia of Political Thought*, edited by Michael T. Gibbons. Wiley and Sons, Ltd., 2015.

<https://doi.org/10.1002/9781118474396.wbept0184>.

———. “My Kingdom for a Wave.” *The American Scholar*, 2013.

<https://theamericanscholar.org/my-kingdom-for-a-wave/#>.

Evans, Stephen. “China Passes Controversial New Anti-Terror Laws.” BBC, 2015.

<http://www.bbc.com/news/world-asia-china-35188137>.

Fallis, Don. “Information Ethics for Twenty-First Century Library Professionals.” *Library Hi Tech* 25, no. 1 (2007): 23–36.

———. “Social Epistemology and Information Science.” *Annual Review of Information Science and Technology* 40 (2006): 475–519.

Fallis, Don, and Dennis Whitcomb. “Epistemic Values and Information Management.”

Information Society 25, no. 3 (2009): 175–89. <https://doi.org/10.1080/01972240902848831>.

Fan, Yang, and Qiao Long. “Guangdong Police Swoop on Chat Group Moderator, Activist Who Scaled ‘Great Firewall.’” Radio Free Asia, 2017.

<https://www.rfa.org/english/news/china/guangdong-police-swoop-on-chat-group-moderator-activist-who-scaled-great-firewall-10052017113158.html>.

FBI National Press Office. “FBI — Statement on Brandon Mayfield Case.” FBI National Press Releases, 2004. <https://archives.fbi.gov/archives/news/pressrel/press-releases/statement-on-brandon-mayfield-case>.

FDP - Die Liberalen. “Free Democratic Party - The German Liberals - English Brochure.”

Berlin. Accessed February 4, 2018.

https://www.fdp.de/files/646/270881_FDP_welcome_berlin.indd.pdf.

Feldman, Brian. “Zuckerberg Says He Is Open To Regulation in CNN Interview.” New York

- Magazine, 2018. <http://nymag.com/selectall/2018/03/zuckerberg-says-he-is-open-to-regulation-in-cnn-interview.html>.
- Fisher, Eran. "Class Struggles in the Digital Frontier: Audience Labour Theory and Social Media Users." *Information, Communication & Society* 18, no. 9 (September 2, 2015): 1108–22. <https://doi.org/10.1080/1369118X.2015.1018300>.
- Flaxman, Seth, Sharad Goel, and Justin M. Rao. "Filter Bubbles, Echo Chambers, and Online News Consumption." *Public Opinion Quarterly* 80, no. S1 (January 1, 2016): 298–320. <https://doi.org/10.1093/poq/nfw006>.
- Fletcher, Richard, and Rasmus Kleis Nielsen. "Are People Incidentally Exposed to News on Social Media? A Comparative Analysis." *New Media & Society*, August 17, 2017, 146144481772417. <https://doi.org/10.1177/1461444817724170>.
- Flores, Adolfo. "People Are Worried About DHS Plans To Gather Social Media Info." BuzzFeed, 2017. https://www.buzzfeed.com/adolfoflores/people-are-worried-about-dhs-plans-to-gather-social-media?utm_term=.gq0Xgr8Jm#.kxeLdzR2a.
- Floridi, Luciano. "Understanding Epistemic Relevance." *Erkenntnis* 69, no. 1 (2008): 69–92.
- Forrest, Conner. "Trump's Cybersecurity Executive Order: 4 Things You Need to Know." TechRepublic, 2017. <https://www.techrepublic.com/article/trumps-cybersecurity-executive-order-4-things-you-need-to-know/>.
- Forsyth, Bart. "Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection." *Washington and Lee Law Review* 72 (2015). <http://heinonline.org/HOL/Page?handle=hein.journals/waslee72&id=1349&div=31&collection=journals>.

- Friedland, Joan. "DHS Is Collecting Information on Immigrants' and Citizens' Social Media Use and Making It Part of Their Permanent Records." National Immigration Law Center, 2017. <https://www.nilc.org/news/the-torch/11-30-17/>.
- Fuchs, Christian. *Social Media: A Critical Introduction*. Sage, 2017.
- . "Social Media and Capitalism." *Analysis*, 2011.
- . "Written Evidence - University of Westminster - Communication and Media Research Institute & Westminster Institute for Advanced Studies," 2017. <http://westminsterresearch.wmin.ac.uk/20505/1/73970.pdf>.
- Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. Vol. 16. Routledge, 2013.
- Gao, Charlotte. "China Fines Its Top 3 Internet Giants for Violating Cybersecurity Law | The Diplomat." The Diplomat, 2017. <https://thediplomat.com/2017/09/china-fines-its-top-3-internet-giants-for-violating-cybersecurity-law/>.
- Garmazhapova, Alexandra. "Yevgeny Prigozhin: Caterer to the Kremlin." OpenDemocracy.net, 2014. <https://www.opendemocracy.net/od-russia/alexandra-garmazhapova/yevgeny-prigozhin-caterer-to-kremlin>.
- Garossino, Sandy. "Who the Hell Is @RVAwonk and How Is She Cracking the Kremlin's Code?" National Observer. Accessed February 4, 2018. <https://www.nationalobserver.com/2017/12/28/opinion/who-hell-rvawonk-and-how-she-cracking-kremlins-code>.
- Gehl, Robert W. *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism*. Temple University Press, 2014.

- Giddens, Anthony. "The Consequences of Modernity." *The British Journal of Sociology*, 1991.
<https://doi.org/10.2307/591454>.
- Giles, Keir. "Russia's 'New' Tools for Confronting the West." *Chatham House*, 2016.
<https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf>.
- Gillespie, Tarleton. "Algorithmically Recognizable: Santorum's Google Problem, and Google's Santorum Problem." *Information, Communication & Society* 20, no. 1 (January 2, 2017): 63–80. <https://doi.org/10.1080/1369118X.2016.1199721>.
- . "The Relevance of Algorithms." *Media Technologies: Essays on Communication, Materiality, and Society* 167 (2014).
- Glantz, David M. "Surprise and Maskirovka in Contemporary War." *Military Review*, no. December (1988): 19. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA216491>.
- Goble, Paul A. "Survey: Most Russians Say They Want a Democracy but Don't Support Democratic Values." Euromaidan Press, 2016.
<http://euromaidanpress.com/2016/10/04/survey-most-russians-say-they-want-a-democracy-but-dont-support-democratic-values/#arvlbdata>.
- Goffman, Erving. *The Presentation of Self in Everyday Life*. New York: Anchor Books, 1959.
- Gold, David, Elihu Katz, Paul F. Lazarsfeld, and Elmo Roper. "Personal Influence: The Part Played by People in the Flow of Mass Communications." *American Sociological Review*, 1956. <https://doi.org/10.2307/2088435>.
- Gompert, David C., and Martin Libicki. "Waging Cyber War the American Way." *Survival* 57,

no. 4 (2015): 7–28.

<http://www.tandfonline.com/doi/pdf/10.1080/00396338.2015.1068551?needAccess=true>.

Google Trends. “John Rawls.” Google Trends, 2018.

<https://trends.google.com/trends/explore?date=all&geo=US&q=%2Fm%2F0x3r3>.

Gordon, Thomas F. “The Pleadings Game; Formalizing Procedural Justice.” In *Proceedings of the Fourth International Conference on Artificial Intelligence and Law*, 10–19, 1993.

<https://doi.org/10.1145/158976.158978>.

Gorman, Siobhan, and Julian E. Barnes. “Pentagon: Online Cyber Attacks Can Count as Acts of War.” *The Wall Street Journal*, 2011.

<https://www.wsj.com/articles/SB10001424052702304563104576355623135782718>.

Governatori, Guido, Antonino Rotolo, Régis Riveret, Monica Palmirani, and Giovanni Sartor.

“Variants of Temporal Defeasible Logics for Modelling Norm Modifications.” In *Proceedings of the 11th International Conference on Artificial Intelligence and Law - ICAIL '07*, 155, 2007. <https://doi.org/10.1145/1276318.1276347>.

Grabb, Edward, Douglas Baer, and James Curtis. “The Origins of American Individualism:

Reconsidering the Historical Evidence The Origins of American Individualism:

Reconsidering the Historical Evidence.” *Source The Canadian Journal of Sociology /*

Cahiers Canadiens de Sociologie 24, no. 4 (1999): 511–33.

<http://www.jstor.org/stable/3341789>.

Granville, Kevin. “Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens.” *The New York Times*, 2018.

<https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica->

explained.html.

Guess, Andrew, Brendan Nyhan, and Jason Reifler. "Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 U.S. Presidential Campaign," 2018. <https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf>.

Gumbel, Andrew. "America's Shameful History of Voter Suppression." *The Guardian*, 2017. <https://www.theguardian.com/us-news/2017/sep/13/america-history-voter-suppression-donald-trump-election-fraud>.

Gunkel, Cristoph. "50th Anniversary of the SPIEGEL Affair - SPIEGEL ONLINE." *Spiegel Online*, 2012. <http://www.spiegel.de/international/germany/50th-anniversary-of-the-spiegel-affair-a-857030.html>.

Guo, Martin. "Kantar China Social Media Impact Report 2017 - Kantar." *Kantar China Insights*, 2017. <https://cn-en.kantar.com/media/social/2017/kantar-china-social-media-impact-report-2017/>.

Guynn, Jessica. "Facebook Says 146 Million Americans Reached by Russia Campaign." *USA Today*, 2017. <https://www.usatoday.com/story/tech/2017/11/01/facebook-says-146-million-americans-targeted-russia-campaign/821306001/>.

Habermas, Jürgen. "Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research." *Communication Theory* 16, no. 4 (2006): 411–26. <https://doi.org/10.1111/j.1468-2885.2006.00280.x>.

Hager, Nicky. "Secret Power. New Zealand's Role in the International Spy Network." *Nelson: Neuseeland*, 1996.

- Haines, William. "Consequentialism." The internet encyclopedia of philosophy. Internet Encyclopedia of Philosophy Pub, 2018. <https://www.iep.utm.edu/conseque/>.
- Hamilton, Matt. "Families of San Bernardino Attack Victims Accuse Facebook, Google and Twitter of Aiding Terrorism in Lawsuit." Los Angeles Times, 2017. <http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-tech-lawsuit-20170503-story.html>.
- Hanna, Nagy K., Christine Zhen-Wei Qiang, Asheeta Bhavnani, Kaoru Kimura, and Randeep Sudan. *Rural Informatization in China*. World Bank Working Papers. The World Bank, 2009. <https://doi.org/10.1596/978-0-8213-8018-5>.
- Hannah Levintova. "The US Military Is Set to Meet With the Russian General Who Called For Cyberattacks Against the West." Mother Jones, 2018. <https://www.motherjones.com/politics/2018/01/the-us-military-is-set-to-meet-with-a-prominent-russian-booster-of-cyberattacks/>.
- Hare. "Rawls' Theory of Justice." *The Philosophical Quarterly*, 1973. <http://www.ditext.com/hare/rawls1.html>.
- Harper, Ruth A. "The Social Media Revolution: Exploring the Impact on Journalism and News Media Organizations." *Inquiries - Social Sciences, Arts and Humanities*, 2010.
- Harsanyi, John C. "Can the Maximin Principle Serve as a Basis for Morality? A Critique of John Rawls's Theory." *American Political Science Review* 69, no. 02 (June 1, 1975): 594–606. <https://doi.org/10.2307/1959090>.
- . "Normative Validity and Meaning of von Neumann-Morgenstern Utilities." *Studies in Logic and the Foundations of Mathematics* 134, no. C (1995): 947–59.

[https://doi.org/10.1016/S0049-237X\(06\)80083-2](https://doi.org/10.1016/S0049-237X(06)80083-2).

Harsanyi, John C. “Bayesian Decision Theory, Rule Utilitarianism, and Arrow’s Impossibility Theorem.” *Theory and Decision* 11, no. 3 (September 1979): 289–317.

<https://doi.org/10.1007/BF00126382>.

———. “Bayesian Decision Theory and Utilitarian Ethics.” *The American Economic Review* 68, no. 2 (1978): 223–28.

Hartz, Louis. *The Liberal Tradition in America*. Houghton Mifflin Harcourt, 1991.

Harwit, Eric, and Duncan Clark. “SHAPING THE INTERNET IN CHINA Evolution of Political Control over Network Infrastructure and Content.” Accessed February 22, 2018.

<http://as.ucpress.edu/content/ucpas/41/3/377.full.pdf>.

Hausmanninger, T. “Controlling the Net: Pragmatic Actions or Ethics Needed?” *International Review of Information Ethics* 1, no. 6 (2004): 19–28.

http://container.zkm.de/ijie/ijie/no001/ijie_001_04_hausmanninger.pdf.

Haworth, Alan. “Obama’s Debt to Rawls?” *Practical Ethics*, 2012.

<http://blog.practicaethics.ox.ac.uk/2012/11/obamas-debt-to-rawls/>.

Heinisch, Reinhard. “Success in Opposition – Failure in Government: Explaining the Performance of Right-Wing Populist Parties in Public Office.” *West European Politics* 26, no. 3 (July 2003): 91–130. <https://doi.org/10.1080/01402380312331280608>.

Hermida, Alfred. “Tweets and Truth.” *Journalism Practice* 6, no. 5–6 (October 2012): 659–68.

<https://doi.org/10.1080/17512786.2012.667269>.

Hermida, Alfred, Fred Fletcher, Darryl Korell, and Donna Logan. “SHARE, LIKE, RECOMMEND: Decoding the Social Media News Consumer.” *Journalism Studies* 13, no.

5–6 (2012): 815–24. <https://doi.org/10.1080/1461670X.2012.664430>.

Hern, Alex. “North Korea Is a Bigger Cyber-Attack Threat than Russia, Says Expert.” *The Guardian*, 2018. <https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia>.

Hernández, Javier C., and Zoe Mou. “Chinese Social Media Site Reverses Gay Content Ban After Uproar.” *The New York Times*, 2018.

<https://www.nytimes.com/2018/04/16/world/asia/china-weibo-gay.html>.

———. “‘I Am Gay, Not a Pervert’: Furor in China as Sina Weibo Bans Gay Content.” *The New York Times*, 2018. <https://www.nytimes.com/2018/04/15/world/asia/china-gay-ban-sina-weibo-.html>.

Hindman, Matthew. “This Is How Cambridge Analytica’s Facebook Targeting Model Really Worked — According to the Person Who Built It.” *Nieman Lab*, 2018.

<http://www.niemanlab.org/2018/03/this-is-how-cambridge-analyticas-facebook-targeting-model-really-worked-according-to-the-person-who-built-it/>.

Hintz, Arne. “From Media Niche to Policy Spotlight: Mapping Community-Media Policy Change in Latin America.” *Canadian Journal of Communication*, 2011.

Hirst, Martin., and Martin. *News 2.0 : Can Journalism Survive the Internet?* Allen & Unwin, 2011. <http://dro.deakin.edu.au/view/DU:30041209>.

Hodel-Widmer, Thomas B. “Designing Databases That Enhance People’s Privacy without Hindering Organizations.” *Ethics and Information Technology* 8, no. 1 (2006): 3–15.

<https://doi.org/10.1007/s10676-006-9105-3>.

Hoffman, Anna Lauren. “Beyond Distributions and Primary Goods: Assessing Applications of

- Rawls in Information Science and Technology Literature since 1990.” *Journal of the Association for Information Science and Technology* 68, no. 7 (2017): 1601–18.
<https://doi.org/10.1002/asi.23747>.
- Hoffman, Chris. “How the ‘Great Firewall of China’ Works to Censor China’s Internet.” *How-to Geek*, 2016. <https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/>.
- Hofstede, Geert, and Michael Harris Bond. “The Confucius Connection: From Cultural Roots to Economic Growth.” *Organizational Dynamics* 16, no. 4 (1988): 5–21.
[https://doi.org/10.1016/0090-2616\(88\)90009-5](https://doi.org/10.1016/0090-2616(88)90009-5).
- Hofstede, Geert J. “Cultures and Organizations: Software of the Mind.” *McGraw-Hill, London*, 1991.
- Hood, Cameron. “No Truth in News, and No News in Truth.” *Latterly*, 2017.
<https://cameronghood.com/2017/04/20/no-truth-in-news-and-no-news-in-truth/>.
- Hornby, Lucy. “China’s VPN Crackdown Is about Money as Much as Censorship.” *Financial Times*, 2018. <https://www.ft.com/content/35eafc9a-fcf8-11e7-9b32-d7d59aace167>.
- Hoven, Jeroen Van den, and Emma Rooksby. “Distributive Justice and the Value of Information: A (Broadly) Rawlsian Approach.” In *Information Technology and Moral Philosophy*, edited by Jeroen Van Den Hoven and John Weckert. New York: Cambridge University Press New York, NY, 2008.
- Howard, Philip N, Samantha Bradshaw, Gillian Bolsover, Lisa-Maria Neudert, and Bence Kollanyi. “Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?,” 2017. <http://275rzy1ul4252pt1hv2dqyuf.wpengine.netdna->

cdn.com/wp-content/uploads/2017/07/2206.pdf.

Huang, Cary, and Keith Zhai. “Xi Jinping Rallies Party for Propaganda War on Internet.” *South China Morning Post*, 2013. <http://www.scmp.com/news/china/article/1302857/president-xi-jinping-rallies-party-propaganda-war-internet>.

Huang, Zheping. “China Censorship: Chinese Citizens Are Being Arrested for Sharing News about the Wukan Village Rebellion Online.” *Quartz*, 2016. <https://qz.com/783026/china-censorship-chinese-citizens-are-being-arrested-for-sharing-news-about-the-wukan-village-rebellion-online/>.

Hudgins, Jackson, and Alyssa Newcomb. “Google, Facebook, Twitter and Russia: A Timeline on the ’16 Election.” *NBC News*, 2017. <https://www.nbcnews.com/news/us-news/google-facebook-twitter-russia-timeline-16-election-n816036>.

Hulst, Merlijn van, and Dvora Yanow. “From Policy ‘Frames’ to ‘Framing’: Theorizing a More Dynamic, Political Approach.” *American Review of Public Administration* 46, no. 1 (2016): 92–112. <https://doi.org/10.1177/0275074014533142>.

Human Rights Watch. “World Report 2016: China | Human Rights Watch.” *World Report 2016*, 2015. <https://www.hrw.org/world-report/2016/country-chapters/china-and-tibet>.

———. “World Report 2017: China | Human Rights Watch.” *World Report 2017*, 2017. <https://www.hrw.org/world-report/2017/country-chapters/china-and-tibet>.

———. “World Report 2018: China | Human Rights Watch.” *World Report 2018*, 2018. <https://www.hrw.org/world-report/2018/country-chapters/china-and-tibet>.

Ihlen, Øyvind, Tine Ustad Figenschou, and Anna Grøndahl Larsen. “Behind the Framing Scenes: Challenges and Opportunities for NGOs and Authorities Framing Irregular Immigration.”

American Behavioral Scientist 59, no. 7 (2015): 822–38.

<https://doi.org/10.1177/0002764215573254>.

Inkster, Nigel. “Information Warfare and the US Presidential Election.” *Survival - Global Politics and Strategy* 58, no. 5 (2016): 23–32.

<http://www.tandfonline.com/doi/pdf/10.1080/00396338.2016.1231527?needAccess=true>.

Introna, Lucas D. “Workplace Surveillance, Privacy and Distributive Justice.” *ACM SIGCAS Computers and Society* 30, no. 4 (2000): 33. <https://doi.org/10.1145/572260.572267>.

Introna, Lucas, and Athanasia Pouloudi. “Privacy in the Information Age: Stakeholders, Interests and Values.” *Journal of Business Ethics* 22, no. 1 (1999): 27–38.

<https://doi.org/10.1023/A:1006151900807>.

Irani, Lilly. “The Hidden Faces of Automation.” *XRDS: Crossroads, The ACM Magazine for Students* 23, no. 2 (December 15, 2016): 34–37. <https://doi.org/10.1145/3014390>.

Jinping, Xi. “Explanatory Notes for the ‘Decision of the Central Committee of the Communist Party of China on Some Major Issues Concerning Comprehensively Deepening the Reform’ (2) - People’s Daily Online.” People.cn, 2014. <http://en.people.cn/102774/8525245.html>.

Jintao, Hu. “Hu Jintao’s Report at 18th Party Congress.” China-embassy.org, 2012.

http://www.china-embassy.org/eng/zt/18th_CPC_National_Congress_Eng/t992917.htm.

Jones, Harvey, and Hiram Soltren. “Facebook: Threats to Privacy,” 2005.

<https://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf>.

Jordan, Bryant. “US Still Has No Definition for Cyber Act of War | Military.Com.”

Military.com, 2016. <https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html>.

- Jung, A-Reum. "The Influence of Perceived Ad Relevance on Social Media Advertising: An Empirical Examination of a Mediating Role of Privacy Concern." *Computers in Human Behavior* 70 (May 1, 2017): 303–9. <https://doi.org/10.1016/J.CHB.2017.01.008>.
- Kaal, Wulf. "What Happens When Technology Is Faster Than the Law? | CLS Blue Sky Blog." Columbia Law School Blue Sky, 2016.
<http://clsbluesky.law.columbia.edu/2016/09/22/what-happens-when-technology-is-faster-than-the-law/>.
- Kahn, Matthew. "Document: December 2017 National Security Strategy and Transcript of Remarks - Lawfare." Lawfare, 2017. <https://www.lawfareblog.com/document-december-2017-national-security-strategy-and-transcript-remarks>.
- Kahneman, Daniel, Jack L Knetsch, and Richard H Thaler. "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias." *Journal of Economic Perspectives*, 1991.
<https://doi.org/10.1257/jep.5.1.193>.
- Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision under Risk." *Econometrica*, 1979. <https://doi.org/10.2307/1914185>.
- Kang, Minah, and Jiho Jang. "NIMBY or NIABY? Who Defines a Policy Problem and Why: Analysis of Framing in Radioactive Waste Disposal Facility Placement in South Korea." *Asia Pacific Viewpoint* 54, no. 1 (2013): 49–60. <https://doi.org/10.1111/apv.12007>.
- Kant, Immanuel. "Groundwork for the Metaphysic of Morals (1785)." *Practical Philosophy*, 2005, 37–108. <https://doi.org/10.4324/9780203981948>.
- Katz, Daniel. "The Functional Approach to the Study of Attitudes." *Public Opinion Quarterly*, 1960. <https://doi.org/10.1086/266945>.

- Kaufman, Sanda, and Janet Smith. "Framing and Reframing in Land Use Change Conflicts." *Journal of Architectural and Planning Research* 16, no. 2 (1999): 164–80.
- Kendrick, Leslie. "Speech, Intent and the Chilling Effect." *William and Mary Law Review* 54, no. 5 (2013): 1633–92. <https://doi.org/10.3366/ajicl.2011.0005>.
- Kets de Vries, Manfred F.R. "The Anarchist within: Clinical Refelctions on Russian Character and Leadership Style." *Human Relations* 54, no. 5 (2001): 585–627. <http://journals.sagepub.com/doi/pdf/10.1177/0018726701545003>.
- Kilzer, Lou. "Snowden's 'secrets' Should Not Surprise." TribLive, 2013. <http://triblive.com/news/editorspicks/4408043-74/nsa-snowden-program>.
- King, Gary. "How Censorship in China Allows Government Criticism but Silences Collective Expression." *American Political Science Review*, 2013. <https://doi.org/10.1017/S0003055413000014>.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. "Reverse-Engineering Censorship in China: Randomized Experimentation and Participant Observation." *Science* 345, no. 6199 (2014). <https://gking.harvard.edu/publications/randomized-Experimental-Study-Censorship-China>.
- King, Gary, Jennifer Pan, and Margaret E Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111, no. 3 (2017): 484–501. <https://doi.org/10.1017/S0003055417000144>.
- Kolata, Gina. "Veiled Messages of Terror May Lurk in Cyberspace." *The New York Times*, 2001. <https://www.nytimes.com/2001/10/30/science/veiled-messages-of-terror-may-lurk-in-cyberspace.html>.
- Korotkov, Denis. "Hundreds of Trolls for Millions - Society - Новости Санкт-Петербурга -

- ФОНТАНКА.РУ.” Fontank.ru, 2014. <http://www.fontanka.ru/2014/05/29/170/>.
- Korsgaard, Christine. “The Right to Lie : Kant on Dealing with Evil.” *Philosophy and Public Affairs* 15, no. 4 (1986): 325–49.
- Korte, Gregory. “U.S. Sanctions on Russia Remain Largely Symbolic.” USA Today, 2018. <https://www.usatoday.com/story/news/politics/2018/03/15/trump-sanctions-russia-following-poisoning-british-spy/427464002/>.
- Kou. “Interview, February 16,” 2018.
- Kou, Yubo, Bryan Semaan, and Bonnie Nardi. “Human-Computer Interaction – INTERACT 2017” 10516, no. May (2017). <https://doi.org/10.1007/978-3-319-68059-0>.
- Kovalev, Alexey. “Russia’s Infamous ‘Troll Factory’ Is Now Posing as a Media Empire.” The Moscow Times, 2017. <https://themoscowtimes.com/articles/russias-infamous-troll-factory-is-now-posing-as-a-media-empire-57534>.
- Kuhn, Anthony. “VPNs In China: Behind Internet Crackdown, ‘Game Of Cat And Mouse’ Continues.” NPR.org, 2017. <https://www.npr.org/sections/alltechconsidered/2017/08/04/541554438/behind-chinas-vpn-crackdown-a-game-of-cat-and-mouse-continues>.
- Kuss, Daria J., and Mark D. Griffiths. “Online Social Networking and Addiction—A Review of the Psychological Literature.” *International Journal of Environmental Research and Public Health* 8, no. 9 (August 29, 2011): 3528–52. <https://doi.org/10.3390/ijerph8093528>.
- Kymlicka, Will. “Rawls on Teleology and Deontology.” *Philosophy & Public Affairs*. Wiley. Accessed April 4, 2018. <https://doi.org/10.2307/2265243>.
- Langman, Lauren. “Cycles of Contention: The Rise and Fall of the Tea Party.” *Critical*

Sociology 38, no. 4: 469–94. Accessed March 18, 2018.

<https://doi.org/10.1177/0896920511430865>.

Lapowsky, Issie. “Facebook May Have More Russian Troll Farms to Worry About.” *Wired*, 2017. <https://www.wired.com/story/facebook-may-have-more-russian-troll-farms-to-worry-about/>.

Lawfare. “Snowden Revelations.” *Lawfare Blog*, 2018. <https://lawfareblog.com/snowden-revelations>.

Lee, Bandi. *The Dangerous Case of Donald Trump: 27 Psychiatrists and Mental Health Experts Assess a President*. *The Dangerous Case of Donald Trump: 27 Psychiatrists and Mental Health Experts Assess a President.*, 2017.

Lee, Carol E., and Jo Ling Kent. “Facebook Says Russian-Backed Election Content Reached 126 Million Americans.” *NBC News*, 2017. <https://www.nbcnews.com/news/us-news/russian-backed-election-content-reached-126-million-americans-facebook-says-n815791>.

Lee, Caroline W. “The Roots of Astroturfing.” *Contexts* 9, no. 1 (2010): 73–75. <https://doi.org/10.1525/ctx.2010.9.1.73>.

Lee, Chei Sian, and Long Ma. “News Sharing in Social Media: The Effect of Gratifications and Prior Experience.” *Computers in Human Behavior*, no. 28 (2012). <https://doi.org/10.1016/j.chb.2011.10.002>.

Leenes, Ronald E. “Burden of Proof in Dialogue Games and Dutch Civil Procedure.” In *Proceedings of the 8th International Conference on Artificial Intelligence and Law - ICAIL '01*, 109–18, 2001. <https://doi.org/10.1145/383535.383549>.

Lesley Stahl. “RT’s Editor-in-Chief on Election Meddling, Being Labeled Russian Propaganda.”

- CBSnews.com, 2018. <https://www.cbsnews.com/news/rt-editor-in-chief-on-election-meddling-russian-propaganda-label/>.
- Lever, Annabelle. "Privacy, Private Property, and Collective Property." *The Good Society* 21, no. 1 (2012): 47–60.
- Liao, Rita. "WeChat's Older Sibling QQ Plans to Stay Forever Young · TechNode." Technode, 2017. <http://technode.com/2017/08/07/wechats-older-sibling-qq-plans-to-stay-forever-young/>.
- Libicki, Martin C. "Cyberspace Is Not a Warfighting Domain." *Journal of Law and Policy* 8 (2012): 325–36.
- . "Interview, August 28." Annapolis, MA, 2017.
- Licklider, J. C. R. "Man-Computer Symbiosis." *IRE Transactions on Human Factors in Electronics* HFE-1, no. 1 (1960): 4–11. <https://doi.org/10.1109/THFE2.1960.4503259>.
- Lievrouw, Leah A., and Sharon E. Farb. "Information and Equity." *Annual Review of Information Science and Technology* 37, no. 1 (January 31, 2005): 499–540. <https://doi.org/10.1002/aris.1440370112>.
- Ling, Rich, and Naomi S. Baron. "Text Messaging and IM: Linguistic Comparison of American College Data." *Journal of Language and Social Psychology*, 2007. <https://doi.org/10.1177/0261927X06303480>.
- Lipset, Seymour Martin. "Historical Traditions and National Characteristics: A Comparative Analysis of Canada and the United States Historical Traditions and National Characteristics: A Comparative Analysis of Canada and the United States." *The Canadian Journal of Sociology / Cahiers Canadiens de Sociologie* 11, no. 2 (1986): 113–55.

<http://www.jstor.org/stable/3340795>.

———. “Neoconservatism: Myth and Reality.” *Society*, no. July/August (1988): 29–37.

<https://link.springer.com/content/pdf/10.1007/BF02695739.pdf>.

———. *The First New Nation: The United States in Historical and Comparative Perspective*.

Heinemann, 1963.

Loader, Brian D, and Dan Mercea. “Networking Democracy? Social Media Innovations and Participatory Politics.” *Information, Communication & Society* 14, no. 6 (2011): 757–69.

Lodder, Arno R, and Aimée Herczog. “DiaLaw: A Dialogical Framework for Modeling Legal Reasoning.” In *Proceedings of the 5th International Conference on Artificial Intelligence and Law*, 146–55, 1995. <https://doi.org/10.1145/222092.222225>.

Lubbers, Marcel, and Marcel Coenders. “Nationalistic Attitudes and Voting for the Radical Right in Europe.” *European Union Politics* 18, no. 1 (2017): 98–118.

<https://doi.org/10.1177/1465116516678932>.

“Lunarstorm.” *Nationalencyklopedin*. National Swedish Encyclopedia. Accessed March 11, 2018. <https://www.ne.se/uppslagsverk/encyklopedi/lang/lunarstorm>.

Lynch, Michael. *Mao*. Taylor & Francis, 2017.

Lyon, David. “Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique.” *Big Data & Society* 1, no. 2 (2014): 2053951714541861.

Macaskill, Ewen, and Gabriel Dance. “NSA Files Decoded: Edward Snowden’s Surveillance Revelations Explained | US News | Theguardian.Com.” *The Guardian*, 2013.

<https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>.

- MacIntyre, Alasdair C. "After Virtue: A Study in Moral Theory." *London Duckworth* 2nd (1984): 286. <https://doi.org/10.2307/2219228>.
- Maffettone, Sebastiano. "Sen's Idea of Justice versus Rawls' Theory of Justice." *Indian Journal of Human Development* 5, no. 1 (2011): 119–32.
- Magdol, Lynn, and Diane R Bessel. "Social Capital, Social Currency, and Portable Assets: The Impact of Residential Mobility on Exchanges of Social Support." *Personal Relationships* 10, no. 2 (2003): 149–70.
- Maher, Joseph B. "DHS: Device Searches Improve Safety." USA Today, 2017. <https://www.usatoday.com/story/opinion/2017/03/27/dhs-device-searches-improve-safety-editorials-debates/99697022/>.
- Manca, Stefania, and Maria Ranieri. "Facebook and the Others. Potentials and Obstacles of Social Media for Teaching in Higher Education." *Computers & Education* 95 (April 1, 2016): 216–30. <https://doi.org/10.1016/J.COMPEDU.2016.01.012>.
- Mankiw, N. Gregory. "When the Scientist Is Also a Philosopher." The New York Times, 2014. https://www.nytimes.com/2014/03/23/business/economic-view-when-the-scientist-is-also-a-philosopher.html?_r=0.
- Martin, Douglas. "Seymour Martin Lipset, Sociologist, Dies at 84." The New York Times, 2007. <http://www.nytimes.com/2007/01/04/obituaries/04lipset.html>.
- Mason, Robert M, Karine Barzilai-Nahon, and Nancy Lou. "The Organizational Impact of Digital Natives: How Organizations Are Responding to the Next Generation of Knowledge Workers." *Proceedings of the 17th International Conference on Management of Technology*, 2008.

http://faculty.washington.edu/rmmason/Publications/IAMOT_DN_2008.pdf.

Mateescu, Alexandra, Douglas Brunton, Alex Rosenblat, Desmond Patton, Zachary Gold, and

Danah Boyd. "Social Media Surveillance and Law Enforcement," 2015.

<http://www.datacivilrights.org/pubs/2015->

[1027/Social_Media_Surveillance_and_Law_Enforcement.pdf](http://www.datacivilrights.org/pubs/2015-1027/Social_Media_Surveillance_and_Law_Enforcement.pdf).

Mathiesen, Kay. "The Human Right to a Public Library." *Journal of Information Ethics* 22, no. 1

(2013): 60–79. <https://doi.org/10.3172/JIE.22.1.60>.

MAVISE. "Company: TV-NOVOSTI." MAVISE. Accessed February 4, 2018.

<http://mavise.obs.coe.int/company?id=8973>.

McFadden, Cynthia, E.D. Cauchi, William Arkin, and Kevin Monahan. "American Citizens:

U.S. Border Agents Can Search Your Cellphone." NBC News, 2017.

<https://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746>.

McGuire, William J. "Personality and Attitude Change: An Information-Processing Theory." In

Psychological Foundations of Attitudes, 1968. <https://doi.org/10.1016/B978-1-4832-3071-9.50013-1>.

Meade, Nigel, and Towhidul Islam. "Modelling and Forecasting the Diffusion of Innovation – A

25-Year Review." *International Journal of Forecasting* 22 (2006): 519–45.

<https://doi.org/10.1016/j.ijforecast.2006.01.005>.

Mercer, Joyce Ann. "The Dangerous Case of Donald Trump: A Case Study in Contested Ethics

and the Public Uses of Professional Expertise." *Pastoral Psychology*, 2018.

<https://doi.org/10.1007/s11089-018-0810-8>.

- Metzger, Miriam J., and Andrew J. Flanagin. "Credibility and Trust of Information in Online Environments: The Use of Cognitive Heuristics." *Journal of Pragmatics* 59 (2013): 210–20. <https://doi.org/10.1016/j.pragma.2013.07.012>.
- Meyer, Henry. "Russian Observers Charge Fraud in Putin's Landslide Re-Election." Bloomberg Politics, 2018. <https://www.bloomberg.com/news/articles/2018-03-19/russian-observers-charge-fraud-in-putin-s-landslide-re-election>.
- Michel, Casey. "How the Russians Pretended to Be Texans — and Texans Believed Them." The Washington Post, 2017. https://www.washingtonpost.com/news/democracy-post/wp/2017/10/17/how-the-russians-pretended-to-be-texans-and-texans-believed-them/?utm_term=.fedcd9c86b35.
- Mill, John Stuart. "On Liberty by John Stuart Mill." *Search* 111, no. 3 (1867): 82–91. <https://doi.org/10.1037/12289-000>.
- Minzner, Carl. "China Is Again Slowly Turning in on Itself." Los Angeles Times, 2014. <http://www.latimes.com/opinion/op-ed/la-oe-1019-minzner-end-of-china-reform-20141019-story.html>.
- Misra, H. "E-Governance and Millennium Development Goals: Sustainable Development Perspective in Rural India." In *ACM International Conference Proceeding Series*, 354–64, 2012. <https://doi.org/10.1145/2463728.2463796>.
- Mitrokhin, Vasili. *KGB Lexicon: The Soviet Intelligence Officers Handbook*. Routledge, 2013.
- Mkono, Muchazondida. "Sustainability and Indigenous Tourism Insights from Social Media: Worldview Differences, Cultural Friction and Negotiation." *Journal of Sustainable Tourism* 24, no. 8–9 (September 19, 2016): 1315–30.

<https://doi.org/10.1080/09669582.2016.1177066>.

Molly K. McKew. "The Gerasimov Doctrine." *POLITICO Magazine*, 2017.

<https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538>.

Moltke, Henrik. "Interview, 3/29/2018," 2018.

Moor, James. "Towards a Theory of Privacy in the Information Age." *Computers and Society* 27 (1997): 27–32.

Mudde, Cas. "The Populist Radical Right: A Pathological Normalcy." *West European Politics* 33, no. 6 (November 20, 2010): 1167–86. <https://doi.org/10.1080/01402382.2010.508901>.

Mueller, Dennis C., Robert D. Tollison, and Thomas D. Willett. "The Utilitarian Contract: A Generalization of Rawls' Theory of Justice." *Theory and Decision* 4, no. 3–4 (1974): 345–67. <https://doi.org/10.1007/BF00136654>.

MySpace.com. "MySpace 2005 Law Enforcement Guide." EFF.org, 2005.

<https://www.eff.org/document/myspace-2005-guide>.

Naess, Petter, Jeppe Astrup Andersen, Morten Skou Nicolaisen, and Arvid Strand. "Forecasting Inaccuracies: A Result of Unexpected Events, Optimism Bias, Technical Problems, or Strategic Misrepresentation?" *Journal of Transport and Land Use*, 2015, 39–55.

<https://doi.org/10.5198/jtlu.2015.719>.

Nagourney, Adam, Salman Masood, and Michael S. Schmidt. "Killers Were Long Radicalized, F.B.I. Investigators Say." *New York Times*, 2015.

<https://www.nytimes.com/2015/12/08/us/fbi-says-san-bernardino-assailants-were-radicalized.html?mtrref=www.google.com>.

- Napoli, Philip M., and Jonathan A. Obar. "The Emerging Mobile Internet Underclass: A Critique of Mobile Internet Access." *The Information Society* 30, no. 5 (October 20, 2014): 323–34. <https://doi.org/10.1080/01972243.2014.944726>.
- Newell, Bryce Clayton, and Joseph T. Tennis. "Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs." Rochester, NY, October 2013. <http://papers.ssrn.com/abstract=2345468>.
- Newman, Lily Hay. "MuslimCrypt Steganography App Helps Jihadists Send Secret Messages." *Wired*, 2018. <https://www.wired.com/story/muslimcrypt-steganography>.
- . "Trump's Cybersecurity Executive Order Gets Off To a Slow Start." *Wired*, 2017. <https://www.wired.com/story/trump-cybersecurity-executive-order/>.
- Nguyen, Reese. "Navigating Jus Ad Bellum in the Age of Cyber Warfare." *California Law Review*, 2013.
- Nickel, James W. "Rethinking Rawls's Theory of Liberty and Rights." *Chi.-Kent L. Rev.* 69 (1993): 763.
- Nimmo, Ben. "Question That: RT's Military Mission – DFRLab – Medium." *DFRLab / Medium*, 2018. <https://medium.com/dfrlab/question-that-rts-military-mission-4c4bd9f72c88>.
- Nissen, Thomas E. *The Weaponization of Social Media: Characteristics of Contemporary Conflicts*. Copenhagen, Denmark: Royal Danish Defence College, 2015.
- Nissen, Thomas Elkjer. "Interview, May 31." Copenhagen, Denmark, 2017.
- Nissenbaum, H. "Privacy as Contextual Integrity." *Washington Law Review*, n.d.
- Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU

Press, 2018.

Nora, Simon, and Alain Minc. *L'informatisation de La Société: Rapport à Monsieur Le Président de La République*. Vol. 3. La Documentation française, 1978.

Novak, Matt. "US Homeland Security Will Start Collecting Social Media Info on All Immigrants October 18th [Updated]." Gizmodo, 2017. <https://gizmodo.com/us-homeland-security-will-start-collecting-social-media-1818777094>.

Nozick, Robert. *Anarchy, State, and Utopia*. Vol. 5038. New York: Basic Books, 1974.

Nylan, Michael. *The Five "Confucian" Classics*. Yale University Press, 2008.

Office of the Director of National Intelligence. "Assessing Russian Activities and Intentions in Recent US Elections," 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Ogunseitan, O. A. "Framing Environmental Change in Africa: Cross-Scale Institutional Constraints on Progressing from Rhetoric to Action against Vulnerability." *Global Environmental Change* 13, no. 2 (2003): 101–11. [https://doi.org/10.1016/S0959-3780\(03\)00004-9](https://doi.org/10.1016/S0959-3780(03)00004-9).

Olga, Olikier. "Unpacking Russia's New National Security Strategy." Center for Strategic and International Studies, 2016. <https://www.csis.org/analysis/unpacking-russias-new-national-security-strategy>.

OSCE. "Intimidation of Observers at Odds with OSCE Commitments to Ensure Transparent Elections, ODIHR Director Says." Organization for Security and Co-operation in Europe. Accessed February 4, 2018. <http://www.osce.org/odihr/elections/171726>.

Osnos, Evan, David Remnick, and Joshua Yaffa. "Trump, Putin, and the New Cold War." *The New Yorker*, 2016. <https://www.newyorker.com/magazine/2017/03/06/trump-putin-and->

the-new-cold-war.

Oxford English Dictionary. "Neo-Liberal, Adj. and N." *Oxford English Dictionary*. Accessed

March 10, 2018. <http://www.oed.com/view/Entry/245592?redirectedFrom=neo-liberal#eid>.

Oyeshile, Olatunji A. "A Critique of the Maximin Principle in Rawls' Theory of Justice."

Humanity & Social Sciences Journal 3, no. 1 (2008): 65–69.

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.607.5171&rep=rep1&type=pdf>.

Pacepa, Ion. *Disinformation : Former Spy Chief Reveals Secret Strategies for Undermining*

Freedom, Attacking Religion, and Promoting Terrorism. WND Books, 2013.

Palm, Elin. "Securing Privacy at Work: The Importance of Contextualized Consent." *Ethics and*

Information Technology 11, no. 4 (2009): 233–41. [https://doi.org/10.1007/s10676-009-](https://doi.org/10.1007/s10676-009-9208-8)

9208-8.

Pan, Yiling. "China Shuts Down Harper's Bazaar and 24 Others on WeChat." *Jing Daily*, 2017.

<https://jingdaily.com/china-shut-down-accounts-on-wechat/>.

Panchenko, A.M. "'Potemkin Villages' as Cultural Myth." In *Russian History and Culture:*

Works of Different Years., 462–75. St. Petersburg: Yuna, 1999.

Panda, Ankit. "Xi Jinping: China Should Become a 'Cyber Power.'" 2014. Accessed February

22, 2018. <https://thediplomat.com/2014/03/xi-jinping-china-should-become-a-cyber-power/>.

Paradise, J.F. "CHINA AND INTERNATIONAL The Role of Confucius Institutes" 49, no. 4

(2009): 647–69.

Pariser, Eli. *The Filter Bubble: How the New Personalized Web Is Changing What We Read and*

How We Think. The Penguin Press, 2011.

Parry, Robert. *Lost History: Contras, Cocaine, the Press & "Project Truth"*. Media Consortium,

1999.

Paul, Christopher, and Miriam Matthews. "The Russian Firehose of Falsehood Propaganda Model: Why It Might Work and Options to Counter It." *RAND Corporation*, 2016, 16. <https://doi.org/10.7249/PE198>.

Pekelis, Alexander Haim. "Law and Social Action; Selected Essays. Edited by Milton R. Konwitz." Ithaca, Cornell University Press, 1950.

People's Daily Staff. "在人民日报社考察工作时的讲话--时政--人民网." *People's Daily*, 2008. <https://politics.people.com.cn/GB/1024/7408514.html>.

Pew Research Center. "Demographics of Internet and Home Broadband Usage in the United States." *Pew Internet*, 2018. <http://www.pewinternet.org/fact-sheet/internet-broadband/>.

Pham, Sherisse, and Charles Riley. "Banned! 11 Things You Won't Find in China." *Cnn.com*, 2017. <http://money.cnn.com/gallery/technology/2016/05/23/banned-china-10/7.html>.

Philips, Tom, and Wang Zhen. "Xi Jinping Becomes Most Powerful Leader since Mao with China's Change to Constitution." *The Guardian*, 2017. <https://www.theguardian.com/world/2017/oct/24/xi-jinping-mao-thought-on-socialism-china-constitution>.

Piketty, Thomas. "Capital in the Twenty-First Century: A Multidimensional Approach to the History of Capital and Social Classes." *British Journal of Sociology* 65, no. 4 (2014): 736–47. <https://doi.org/10.1111/1468-4446.12115>.

Piodi, Franco, and Iolanda Mombelli. "The ECHELON Affair - European Parliament History Series," 2014. http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf.

- Plato, and Benjamin (trans.) Jowett. "The Republic by Plato." The Internet Classics Archive |, 2008. <http://classics.mit.edu/Plato/republic.html>.
- Ponzanesi, Sandra. *Gender, Globalization, and Violence: Postcolonial Conflict Zones*. Routledge, 2014.
- Posner, Richard A. "The Right of Privacy." *L. Rev* 2, no. 393 (n.d.): 1977–78. <https://www.copyright.com/cc/basicSearch.do?>
- Poulsen, Kevin. "Teen Bomb Hoaxer 'Tyrone' Sentenced to 22 Months Time-Served." *Wired*, 2011. <https://www.wired.com/2011/01/tyrone/>.
- Prins, Esther. "Framing a Conflict in a Community-University Partnership." *Journal of Planning Education and Research*, 2005. <https://doi.org/10.1177/0739456X04270370>.
- Pryor, William. "United States v. Vergara, 2018 WL 1324589 (11th Cir. 2018)," 2018. <http://media.ca11.uscourts.gov/opinions/pub/files/201615059.pdf>.
- Qiu, Jack Linchuan. "Virtual Censorship in Chin: Keeping the Gate Between the Cyberspaces." *International Journal of Communications Law and Policy Issue* 4 (1999). www.ijclp.org.
- Radcliffe, Susan (Ed.). "Amara, Roy." *Oxford Essential Quotations*, 2016.
- Radunović, Božidar, and Jean Yves Le Boudec. "A Unified Framework for Max-Min and Min-Max Fairness with Applications." *IEEE/ACM Transactions on Networking* 15, no. 5 (2007): 1073–83. <https://doi.org/10.1109/TNET.2007.896231>.
- Rainie, Lee, and Mary Madden. "Americans' Privacy Strategies Post-Snowden." [Pewinternet.org](http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/), 2015. <http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>.
- Ramirez, Anthony. "NEW YORK ON LINE; One Site, 14 Ethnic Groups." *The New York*

- Times, 1998. <http://www.nytimes.com/1998/04/12/nyregion/neighborhood-report-new-york-on-line-one-site-14-ethnic-groups.html>.
- Rawls, John. "A Theory of Justice." Cambridge Mass.: Harvard University Press, 1971.
- . *A Theory of Justice - Revised Edition*. Belknap Press, 1999.
- . *Collected Papers*. Edited by Samuel Freeman. Cambridge Mass.: Harvard University Press, 1999.
- . *Justice as Fairness: A Restatement*. Harvard University Press, 2001.
- . *Political Liberalism*. Columbia University Press, 2005.
- . *The Law of Peoples: With "The Idea of Public Reason Revisited"*. Harvard University Press, 2001.
- Rein, Martin, and Donald Schön. "Frame-Critical Policy Analysis and Frame-Reflective Policy Practice." *Knowledge and Policy* 9, no. 1 (1996): 85–104.
- <https://doi.org/10.1007/BF02832235>.
- Rezunkov, Viktor. "«Кремлівські Тролі» Розповіли Про Себе: Де Сидять і Чим Займаються." Radio Svoboda, 2015. <https://www.radiosvoboda.org/a/26903778.html>.
- Richards, Neil M. "The Dangers of Surveillance." *Harvard Law Review* 126, no. 7 (2013): 1934–65. <https://doi.org/10.1093/wbro/10.2.201>.
- Richardson, Henry S. "John Rawls." Internet Encyclopedia of Philosophy. Internet Encyclopedia of Philosophy Pub. Accessed April 4, 2018. <http://www.iep.utm.edu/rawls/>.
- Richey, Jeff. "Confucius." The internet encyclopedia of philosophy. Internet Encyclopedia of Philosophy Pub. Accessed April 16, 2018. <http://www.iep.utm.edu/confuciu/#H4>.
- Rid, Thomas. "Cyberwar and Peace: Hacking Can Reduce Real-World Violence." *Foreign*

Affairs 92 (2013): 77–87.

Rider, Sharon, and Michael A. Peters. “Post-Truth, Fake News: Viral Modernity and Higher Education.” In *Post-Truth, Fake News*, 3–12. Singapore: Springer Singapore, 2018.

https://doi.org/10.1007/978-981-10-8013-5_1.

Roberts, Margaret E. “Interview 4/18/2018,” 2018.

Roberts, Sarah. “Commercial Content Moderation: Digital Laborers’ Dirty Work.” In *Intersectional Internet: Race, Sex, Class and Culture Online*, edited by Safiya Noble and Brandesha Tynes. Peter Lang, 2016. <http://ir.lib.uwo.ca/commpub/12>.

Rosbalt Agency. “Russia’s Trial against ‘Anonymous International’ Hacktivist Leader Will Be Closed to the Public.” Meduza, 2017. <https://meduza.io/en/news/2017/06/12/russia-s-trial-against-anonymous-international-hacktivist-leader-will-be-closed-to-the-public>.

Rosenblat, Alex, and Luke Stark. “Uber’s Drivers: Information Asymmetries and Control in Dynamic Work.” *SSRN Electronic Journal*, July 30, 2015.

<https://doi.org/10.2139/ssrn.2686227>.

Roth, Kenneth. “The Law of War in the War on Terror: Washington’s Abuse of ‘Enemy Combatants.’” *Foreign Affairs* 83, no. 1 (2004): 2–7. <https://doi.org/10.2307/20033823>.

Rovner, Joshua. “‘Exclusive’ on NSA Surveillance Reveals Almost Nothing New.” War on the Rocks, 2014. <https://warontherocks.com/2014/07/exclusive-on-nsa-surveillance-reveals-almost-nothing-new/>.

RT. “RT - Fact vs Fiction.” RT.com. Accessed February 4, 2018. <https://www.rt.com/facts-vs-fiction/>.

Rushkoff, Dougless. “Social Currency.” *The Digital Divide*, 2011, 127–29.

Russian Federation. “Doctrine of Information Security of the Russian Federation.” *The Ministry of Foreign Affairs of the Russian Federation*, 2016.

http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICk6BZ29/content/id/2563163.

———. “Government of the Russian Federation | Embassy of the Russian Federation to the United States of America.” Embassy of the Russian Federation . Accessed February 4, 2018. <http://www.russianembassy.org/page/government-of-the-russian-federation>.

Rydgren, Jens. “Explaining the Emergence of Radical Right-Wing Populist Parties: The Case of Denmark.” *West European Politics* 27, no. 3 (May 2004): 474–502.

<https://doi.org/10.1080/0140238042000228103>.

Sánchez Abril, Patricia, Avner Levin, and Alissa Del Riego. “Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee.” *American Business Law Journal* 49, no. 1 (March 1, 2012): 63–124. <https://doi.org/10.1111/j.1744-1714.2011.01127.x>.

Sandel, M. “JUSTICE: What’s the Right Thing to Do?” *Hong Kong Journal of Social Work*, 2009.

<http://www.worldscinet.com/abstract?id=pii:S0219246209000175%5Cnpapers2://publication/uuid/CA695EF0-7B53-47CB-B253-730E4095DA2E>.

Scanlon, Thomas M. “Rawls’ Theory of Justice.” Accessed April 4, 2018.

http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=5241&context=penn_law_review.

Scannell, Kara, David Shortell, and Veronica Stracqualursi. “Mueller Indicts 13 Russian Nationals over 2016 Election Interference.” CNN, 2018.

<https://www.cnn.com/2018/02/16/politics/mueller-russia-indictments-election-interference/index.html>.

Schaefer, Richard T. *Encyclopedia of Race, Ethnicity, and Society*. Vol. 1. Sage, 2008.

Schauer, Frederick. "Fear, Risk and the First Amendment: Unraveling the 'Chilling Effect.'" *Faculty Publications, College of William and Mary*, 1978.

<http://scholarship.law.wm.edu/facpubs>.

Schiff, Adam. "Interview, May 11." Burbank, CA, 2017.

Schiff, Adam B. "State Discriminatory Actions against Nonresidents: Using the Original Position Theory as a Framework for Analysis." *Harvard Journal on Legislation* 22 (1985): 583.

Schlanger, Margo. "Interview, March 15 2018," 2018.

Schon, Donald A, and Martin Rein. *Frame Reflection: Toward the Resolution of Intractable Policy Controversies*. Basic Books, 1995.

Schradie, Jen. "The Trend of Class, Race and Ethnicity on Social Media Inequality."

Information, Communication & Society 15, no. 4 (May 2012): 555–71.

<https://doi.org/10.1080/1369118X.2012.665939>.

Seddon, Max. "Documents Show How Russia's Troll Army Hit America." BuzzFeed. Accessed February 3, 2018. https://www.buzzfeed.com/maxseddon/documents-show-how-russias-troll-army-hit-america?utm_term=.ffYN0XM3B#.wbKbZYMQq.

Seelye, Katherine Q. "Microsoft to Provide and Sell Ads on Facebook, the Web Site." *The New York Times*, 2006. <http://www.nytimes.com/2006/08/23/technology/23soft.html>.

Selznick, Philip. "Foundations of Communitarian Liberalism." *Responsive Community* 4, no. 4

(1994): 16–28.

Sen, Amartya. “Economic Development and Capability Expansion in Historical Perspective.”

Pacific Economic Review 6, no. 2 (2001): 179–91. <https://doi.org/10.1111/1468-0106.00126>.

———. “The Idea of Justice: A Response.” *Philosophy and Social Criticism* 41, no. 1 (2015): 77–88. <https://doi.org/10.1177/0191453714553501>.

Senate Homeland Security and Governmental Affairs. “Committee Hearing on Border Security and Public Safety.” U.S. Senate, 2017.

https://www.thisweekinimmigration.com/uploads/6/9/2/2/69228175/hearingtranscript_senate_homelandsecurityandgovernmentalaffairsheaingwithsecretarykelly_2017-04-05.pdf.

Shadish, William R., Thomas D. Cook, and Donald T. Campbell. *Experimental and Quasi-Experimental Designs for Generalized Causal Inference*. Boston: Houghton Mifflin, 2002.

Shain, Barry Alan. *The Myth of American Individualism: The Protestant Origins of American Political Thought*. Princeton University Press, 1996.

Shaltai Boltai. “Анонимный Интернационал.” Shaltai Boltai, 2014.

<https://boltai.wordpress.com/2014/05/>.

Shearer, Elisa, and Jeffrey Gottfried. “News Use Across Social Media Platforms 2017.” Pew Research Center - Journalism & Media, 2017. <http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/>.

Shifman, Limor. *Memes in Digital Culture*. Mit Press, 2014.

Shipler, David K. *The Rights of the People: How Our Search for Safety Invades Our Liberties*. New York: Alfred E. Knopf, n.d.

<http://pearl.stkate.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=llf&AN=58150779&site=ehost-live>.

- Shu, Catherine. "China Doubles down on Real-Name Registration Laws, Forbidding Anonymous Online Posts." TechCrunch, 2017. <https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/>.
- Sima, Qian, and Burton Watson. *Records of the Grand Historian of China*. New York: Columbia University Press., 1961.
- Simonyan, Margarita. "Putin Talks NSA, Syria, Iran, Drones in RT Interview." RT.com, 2013. <https://www.rt.com/news/putin-rt-interview-full-577/>.
- Sinnott-Armstrong, Walter. "Consequentialism." Stanford Encyclopedia of Philosophy. Stanford University, 2015.
- Slayton, Rebecca. "Interview, August 24." Ithaca, NY, 2017.
- Smith, Hedrick. "The Russians. New York: Quadrangle." *New York Times Book Co*, 1976.
- Snow, Jackie. "Algorithms Are Making American Inequality Worse - MIT Technology Review." MIT Technology Review, 2018. <https://www.technologyreview.com/s/610026/algorithms-are-making-american-inequality-worse/>.
- Sobaih, Abu Elnasr E., Mohamed A. Moustafa, Parvis Ghandforoush, and Mahmood Khan. "To Use or Not to Use? Social Media in Higher Education in Developing Countries." *Computers in Human Behavior* 58 (May 1, 2016): 296–305. <https://doi.org/10.1016/J.CHB.2016.01.002>.
- Solove, Daniel J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." *San Diego Law Review* 44, no. May (2007): 1–23. <https://doi.org/10.2139/ssrn.998565>.

- . “Nothing to Hide. The False Tradeoff between Privacy and Security.” *Yale* 8, no. 6 (2011): 1–255. <https://doi.org/10.1038/ncb0606-541b>.
- Søraker, Johnny Hartz. “The Role of Pragmatic Arguments in Computer Ethics.” *Ethics and Information Technology* 8, no. 3 (2006): 121–30. <https://doi.org/10.1007/s10676-006-9119-x>.
- Specter, Michael. “Russia’s Purveyor of ‘Truth’, Pravda, Dies After 84 Years.” *The New York Times*. Accessed February 3, 2018. <http://www.nytimes.com/1996/07/31/world/russia-s-purveyor-of-truth-pravda-dies-after-84-years.html>.
- Sputnik. “About Us - Sputnik International.” *Sputniknews.com*. Accessed February 4, 2018. <https://sputniknews.com/docs/about/index.html>.
- Srinivasan, Ramesh. *Whose Global Village?: Rethinking How Technology Shapes Our World*. NYU Press, 2017.
- Staff. “Engine Failure.” *Logic*, 2017. <https://logicmag.io/03-engine-failure/>.
- . “‘Great Wall’ May Crumble, But More China-U.S. Films Are Coming.” *Bloomberg News*, 2017. <https://www.bloomberg.com/news/articles/2017-02-17/-great-wall-may-crumble-but-more-china-u-s-films-are-coming>.
- . “May 1997: Six Degrees - Then and Now: A History of Social Networking Sites.” *CBS News*, 2011. <https://www.cbsnews.com/pictures/then-and-now-a-history-of-social-networking-sites/2/>.
- . “Mom Says Patriot Act Stripped Son of Due Process.” *WRAL.Com*, 2009. <http://www.wral.com/news/local/story/5049867/>.
- . “Russia’s Media Watchdog Boasts It ‘Convinced’ China to Lift Vkontakte Ban.” *The*

- Moscow Times, 2018. <https://themoscowtimes.com/news/russia-media-watchdog-boasts-it-convinced-china-to-lift-vkontakte-ban-60523>.
- . “RÜSTUNGS-AUFTRÄGE: Kalifornische Preise.” *Der Spiegel*, 1959.
<http://www.spiegel.de/spiegel/print/d-42624035.html>.
- . “SCANDALS: Lockheed’s Defiance: A Right to Bribe?” *Time Magazine*, 1975.
<http://content.time.com/time/subscriber/article/0,33009,917751-1,00.html>.
- . “The FSB Has Caught the Alleged Head of ‘Humpty Dumpty’: What Does This Have to Do with Treason?” *Meduza*, 2017. <https://meduza.io/en/feature/2017/01/31/the-fsb-caught-humpty-dumpty>.
- . “The Long March to Privacy | *The Economist*.” *The Economist*, 2006.
<https://www.economist.com/node/5389362>.
- . “Twitter User Numbers Overtaken by China’s Sina Weibo.” *BBC News*, 2017.
<http://www.bbc.com/news/technology-39947442>.
- . “What You Need to Know about Echelon.” *BBC.co.uk*, 2001.
<http://news.bbc.co.uk/2/hi/sci/tech/1357513.stm>.
- . “Xi Jinping Is No Longer Any Old Leader - Core Upgrade.” *The Economist*, 2018.
<https://www.economist.com/news/china/21737068-mao-would-be-proud-xi-jinping-no-longer-any-old-leader>.
- Standing Committee of the National People’s Congress. “People’s Republic of China Network Security Law.” *China Law Translate*, 2016.
<http://www.chinalawtranslate.com/cybersecuritylaw/?lang=en>.
- Stark, Luke, and Kate Crawford. “The Conservatism of Emoji: Work, Affect, and

Communication.” *Social Media + Society* 1, no. 2 (September 22, 2015):
205630511560485. <https://doi.org/10.1177/2056305115604853>.

State Internet Information Office. “Provisions on the Management of Internet Forum Community
Services.” China Law Translate, 2017. [https://www.chinalawtranslate.com/互联网论坛社
区服务管理规定/?lang=en](https://www.chinalawtranslate.com/互联网论坛社区服务管理规定/?lang=en).

———. “Provisions on the Management of Internet Post Comments Services.” China Law
Translate, 2017. [https://www.chinalawtranslate.com/互联网跟帖评论服务管理规定
/?lang=en](https://www.chinalawtranslate.com/互联网跟帖评论服务管理规定/?lang=en).

Statista. “Global Social Media Ranking 2018 | Statistic.” Statista.com, 2018.
[https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-
users/](https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/).

Suarez, Sergio. “Is America Safer? The USA FREEDOM Act of 2015 and What the FBI and
NSA Have, Can, and Should Be Doing,” 2017.
http://scholarship.shu.edu/student_scholarship.

Sunstein, Cass R. “Nudging: A Very Short Guide.” *Journal of Consumer Policy*, 2014.
<https://doi.org/10.1007/s10603-014-9273-1>.

Sunstein, Cass R. # *Republic: Divided Democracy in the Age of Social Media*. Princeton
University Press, 2018.

Swanton, Christine. *Virtue Ethics, Role Ethics, and Business Ethics*. Oxford: Oxford University
Press, 2007.

Swire, Briony, Adam J Berinsky, Stephan Lewandowsky, and Ullrich K H Ecker. “Processing

- Political Misinformation—Comprehending the Trump Phenomenon.” *Royal Society Open Science*, 2017. <https://doi.org/10.1098/rsos.160802>.
- Szczerba, Robert J. “15 Worst Tech Predictions Of All Time.” *Forbes.com*, 2015. <https://www.forbes.com/sites/robertszczerba/2015/01/05/15-worst-tech-predictions-of-all-time/#6915ac041299>.
- Tabeta, Shunsuke. “Xi’s Iron Grip on China’s Internet Extends to Social Media- Nikkei Asian Review.” *Nikkei*, 2017. <https://asia.nikkei.com/Politics-Economy/Policy-Politics/Xi-s-iron-grip-on-China-s-internet-extends-to-social-media>.
- Tang, Chao. “In - Depth Analysis of the Great Firewall of China,” 2016. <https://www.cs.tufts.edu/comp/116/archive/fall2016/ctang.pdf>.
- Tatlow, Didi Kirsten. “China Approves Security Law Emphasizing Counterespionage.” *New York Times*, 2014. <https://www.nytimes.com/2014/11/03/world/asia/china-approves-security-law-emphasizing-counterespionage.html>.
- Taylor, Charles. “Atomism.” In *Philosophy and the Human Sciences: Philosophical Papers 2*, 187–210, 1985.
- Tencent. “TENCENT ANNOUNCES 2017 THIRD QUARTER RESULTS 3Q2017 Financial Review.” *Hong Kong*, 2017. <https://www.tencent.com/en-us/articles/8003451510737482.pdf>.
- Thaler, Richard H. “Behavioral Economics: Past, Present, and Future.” *American Economic Review*, 2016. <https://doi.org/10.1257/aer.106.7.1577>.
- The White House. “FACT SHEET: Cybersecurity National Action Plan | Whitehouse.Gov.” *Obamawhitehouse.archives.org*, 2016. <https://obamawhitehouse.archives.gov/the-press->

office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

———. “National Security Strategy of the United States of America,” 2017.

<https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

Thomas, Timothy L. “Russia’s Reflexive Control Theory and the Military.” *The Journal of Slavic Military Studies* 17, no. 17 (2004): 237–56.

<https://doi.org/10.1080/13518040490450529>.

Thompson, Kirill O. “The Archery of ‘Wisdom’ in the Stream of Life: ‘Wisdom’ in the Four Books with Zhu Xi’s Reflections.” *Philosophy East and West* 57, no. 3 (2007): 330–44.

<https://doi.org/10.1353/pew.2007.0040>.

Thomson, Judith Jarvis. “The Right to Privacy.” In *Philosophical Dimensions of Privacy: An Anthology*, 272–89, 1984. <https://doi.org/10.1017/CBO9780511625138.012>.

Tiezzi, Shannon. “Is This the Year China Gets Serious About Ending Rural Poverty?” *The Diplomat*, 2018. <https://thediplomat.com/2018/02/is-this-the-year-china-gets-serious-about-ending-rural-poverty/>.

———. “Xi Jinping Leads China’s New Internet Security Group.” *The Diplomat*, 2014.

<https://thediplomat.com/2014/02/xi-jinping-leads-chinas-new-internet-security-group/>.

TimeWarner. “ICQ Celebrates 100 Million Registered Users | Time Warner Inc.” Press Release, 2001. <http://www.timewarner.com/newsroom/press-releases/2001/05/09/icq-celebrates-100-million-registered-users>.

Ting, Carol, and Famin Yi. “ICT Policy for the ‘Socialist New Countryside’—A Case Study of Rural Informatization in Guangdong, China.” *Telecommunications Policy* 37, no. 8

(September 1, 2013): 626–38. <https://doi.org/10.1016/J.TELPOL.2012.03.007>.

- Tocqueville, Alexis De. *Democracy in America (1835)*. Vol. 10. Regnery Publishing, 2003.
- Treisman, Daniel. "Why Putin Took Crimea." *Foreign Affairs*, April 18, 2016.
<https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea>.
- Trottier, Daniel, and Christian Fuchs. *Social Media, Politics and the State: Protests, Revolutions, Riots, Crime and Policing in the Age of Facebook, Twitter and Youtube*. Vol. 16. Routledge, 2014.
- Tu, Wei-Ming. "Confucius and Confucianism." In *Confucianism and the Family*, 3–22. New York: SUNY Press, 1998.
- Tufekci, Zeynep. "'Not This One' Social Movements, the Attention Economy, and Microcelebrity Networked Activism." *American Behavioral Scientist* 57, no. 7 (2013): 848–70.
- Turkle, Sherry. "Alone Together." New York: Basic Books, 2011.
- . "Life on the Screen: Identity in the Age of the Internet." *NY Etc.: Cop*, 1995.
- Twitter Public Policy. "Update on Twitter's Review of the 2016 U.S. Election." Twitter Blog, 2018. https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html.
- U.S. Customs and Border Protection. Border Search of Electronic Devices, Pub. L. No. CBP Directive No. 3340-049A (2018).
<https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf>.
- . "CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics | U.S. Customs and Border Protection." CBP.gov, 2017.

<https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and>.

U.S. Department of Justice. “DOJ, DHS Report: Three Out of Four Individuals Convicted of International Terrorism and Terrorism-Related Offenses Were Foreign-Born.” Justice.gov. Accessed April 2, 2018. <https://www.justice.gov/opa/pr/doj-dhs-report-three-out-four-individuals-convicted-international-terrorism-and-terrorism>.

U.S. Dept. of State - Office of the Historian. “Milestones: 1945–1952.” History.state.gov. Accessed February 22, 2018. <https://history.state.gov/milestones/1945-1952/chinese-rev>.

U.S. Strategic Command. “U.S. Cyber Command (USCYBERCOM) Factsheet.” Stratcom.mil, 2016. <http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscycybercom/>.

United Nations. “Universal Declaration of Human Rights | United Nations.” UN.org, 1948. <http://www.un.org/en/universal-declaration-human-rights/>.

Usadel, Georg Friedrich Hennig. *Zucht Und Ordnung: Grundlagen Einer Nationalsozialistischen Ethik*. Hanseatische Verlagsanstalt, 1935.

USCIS. “A-Files Numbered Below 8 Million.” USCIS.gov, 2018. <https://www.uscis.gov/history-and-genealogy/genealogy/files-numbered-below-8-million>.

Verloo, Mieke. “Mainstreaming Gender Equality in Europe. A Critical Frame Analysis Approach.” *The Greek Review of Social Research* 117, no. B’ (2005): 11–34. <https://doi.org/10.1063/1.3033202>.

Victor, Daniel. “What Are Your Rights If Border Agents Want to Search Your Phone?” *The New York Times*, 2017. <https://www.nytimes.com/2017/02/14/business/border->

enforcement-airport-phones.html.

Vieten, Ulrike M., and Scott Poynting. "Contemporary Far-Right Racist Populism in Europe."

Journal of Intercultural Studies 37, no. 6 (2016): 533–40.

<https://doi.org/10.1080/07256868.2016.1235099>.

Vivek Wadhwa. "Laws and Ethics Can't Keep Pace with Technology." MIT Technology

Review, 2014. <https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/>.

Voreskova, Svetlana. "Yes: 'There Is No Truth in the News and No News in the Truth' Was a

Very Common Saying." Medium, 2017. <https://medium.com/@svetlanavoreskova/yes-there-is-no-truth-in-the-news-and-no-news-in-the-truth-was-a-very-common-saying-9f44f3d678f7>.

Vronskaya, Jeanne. "Obituary: Alexei Adzhubei." *The Independent*, 1993.

<http://www.independent.co.uk/news/people/obituary-alexei-adzhubei-1499406.html>.

Wagner, Jack. "China's Cybersecurity Law: What You Need to Know | The Diplomat." *The*

Diplomat, 2017. <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>.

Wagner, Lauren. "How to Search MySpace." *SEARCH Training Services*, 2007.

<https://www.eff.org/document/2007-article-how-search-myspace>.

———. "MySpace Friend Mapper Article." *SEARCH Training Services*, 2007.

<https://www.eff.org/document/doj-social-network-foia-myspace-friend-mapper-article>.

Wallentine, Ken. "Officer's Warrantless Smartphone Search Permitted by Border Search

Doctrine." Lexipol, 2018. <http://www.lexipol.com/news/officers-warrantless-smartphone->

search-permitted-border-search-doctrine/.

Walton, Greg. “China’s Golden Shield.” *Human Rights in China 中国人权* | HRIC, 2002.

<https://www.hrichina.org/en/content/4598>.

Walzer, Michael. “The Communitarian Critique of Liberalism.” *Political Theory* 18, no. 1 (1990): 6–23. <http://journals.sagepub.com/doi/pdf/10.1177/0090591790018001002>.

Wang, Hao. *Protecting Privacy in China: A Research on China’s Privacy Standards and the Possibility of Establishing the Right to Privacy and the Information Privacy Protection Legislation in Modern China*. Springer Science & Business Media, 2011.

Ward, Alex. “House Approves FISA and Allows Spying on Americans to Continue.” *Vox*, 2018.

<https://www.vox.com/2018/1/11/16878220/house-vote-surveillance-spying-fisa>.

Warren, Samuel, and Louis Brandeis. “The Right to Privacy.” *Harvard Law Review* 4, no. 5 (1890): 193. <https://doi.org/10.2307/1321160>.

Warren, Tom. “Did Microsoft Just Give up on Windows Phone?” *The Verge*, 2015.

<https://www.theverge.com/2015/7/8/8913365/microsoft-lumia-windows-phones-strategy-2015>.

Watson. *The Tso Chuan: Selections from China’s Oldest Narrative History*. New York: Columbia University Press, 1989.

Welde, Morten, and James Odeck. “Do Planners Get It Right? The Accuracy of Travel Demand Forecasting in Norway.” *EJTIR Issue* 11, no. 1 (2011): 80–95. www.ejtir.tbm.tudelft.nl.

Westin, Alan F. “Social and Political Dimensions of Privacy.” *Journal of Social Issues* 59, no. 2 (2003): 431–53. <https://doi.org/10.1111/1540-4560.00072>.

Whitaker, Reg. “A Faustian Bargain? America and the Dream of Total Information Awareness.”

- In *The New Politics of Surveillance and Visibility*, 141–70. Toronto: University of Toronto Press, 2006.
- Williams, Garrath. “Thomas Hobbes: Moral and Political Philosophy.” Internet Encyclopedia of Philosophy. Internet Encyclopedia of Philosophy Pub. Accessed March 10, 2018.
<https://www.iep.utm.edu/hobmoral/#SH4d>.
- Windrem, Robert. “Guess Who Came to Dinner With Flynn and Putin.” NBCNews.com, 2017.
<https://www.nbcnews.com/news/world/guess-who-came-dinner-flynn-putin-n742696>.
- . “Terror in the Family: When Radicalization Begins at Home.” NBC News, 2015.
<https://www.nbcnews.com/news/us-news/terror-family-when-radicalization-begins-home-n481816>.
- Wolf, M J, and F S Grodzinsky. “Good/Fast/Cheap: Contexts, Relationships and Professional Responsibility During Software Development.” In *Proceedings of the 2006 ACM Symposium on Applied Computing*, 261–66, 2006.
<https://doi.org/http://doi.acm.org.library.capella.edu/10.1145/1141277.1141339>.
- Wolfe, Spencer. “The Top 10 Worst Social Media Cyber-Attacks - Infosecurity Magazine.” InfoSecurity, 2017. <https://www.infosecurity-magazine.com/blogs/top-10-worst-social-media-cyber/>.
- Wolfenstein, Martha, and Margaret Mead. *Childhood in Contemporary Cultures*. Edited by Martha Wolfenstein and Margaret Mead. Chicago, IL: University of Chicago Press, 1955.
- Wood, Gordon S. *The Radicalism of the American Revolution*. New York: Alfred E. Knopf, 1992.
- Wright, Marie. “Domestic Terrorism, Cyber-Radicalization, U.S. College Students.” *Forensic*

- Examiner*, 2011, 10–18. <https://issuu.com/acfei.media/docs/fallwinter2011>.
- Wright, Steve. “An Appraisal of the Technology of Political Control.” Luxembourg, 1998. http://www.europarl.europa.eu/pdf/jadis/2013_12/8.PE4_AP_PV!LIBE.1994_LIBE-199801260050EN.pdf.
- Wysocki, Diane Kholos. “Let Your Fingers Do the Talking: Sex on an Adult Chat-Line.” *Sexualities* 1, no. 4 (1998): 425–52. <https://doi.org/10.1177/136346098001004003>.
- “Xi Jinping: How to Read Confucius and Other Chinese Classical Thinkers.” China Daily, 2017. http://www.chinadaily.com.cn/china/xismoments/2017-05/12/content_29324341.htm.
- Xi, Jinping. “Xi Jinping’s Speech in Commemoration of the 2,565th Anniversary of Confucius’ Birth.” Chinausfocus.com, 2014. <http://library.chinausfocus.com/article-1534.html>.
- Xu, Xueyang, Z Morley Mao, and J Alex Halderman. “Internet Censorship in China: Where Does the Filtering Occur?” Accessed February 19, 2018. <http://www.cse.umich.edu>.
- Yuan, Li. “Beijing Pushes for a Direct Hand in China’s Big Tech Firms.” The Wall Street Journal, 2017. <https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-1507758314>.
- Zak, Paul J. “The Neuroscience of Trust Management Behaviors That Foster Employee Engagement.” Level Five Executive, 2017. <https://levelfiveexecutive.com/wp-content/uploads/2017/03/hbr-neuroscience-of-trust.pdf>.
- Zeitiz, Josh. “How Trump Is Recycling Nixon’s ‘Law and Order’ Playbook.” Politico Magazine, 2016. <https://www.politico.com/magazine/story/2016/07/donald-trump-law-and-order-richard-nixon-crime-race-214066>.
- Zelevnikow, John, Emilia Bellucci, Uri J Schild, and Geraldine Mackenzie. “Bargaining in the

- Shadow of the Law-Using Utility Functions to Support Legal Negotiation.” In *Proceedings of the 11th International Conference on Artificial Intelligence and Law*, 237–46, 2007.
- Zeng, Meg Jing. “China’s Social Credit System Puts Its People under Pressure to Be Model Citizens.” *The Conversation*, 2018. <https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963>.
- Zhao, Zhang. “Long Conflict over QQ Continues into Court|Business|chinadaily.Com.Cn.” *China Daily*, 2013. http://usa.chinadaily.com.cn/epaper/2013-07/24/content_16824251.htm.
- Zheping, Huang. “Human Rights Lawyer Wang Yu on Year of Secret Detention in China.” *Quartz*, 2017. <https://qz.com/1129837/human-rights-lawyer-wang-yu-on-year-of-secret-detention-in-china/>.
- Zhong, Raymond, and Sui-Lee Wee. “China Seeks Small Stakes in, and More Sway over, Online Firms.” *The New York Times*, 2017.
- Zhou, Jinghao. *Remaking China’s Public Philosophy for the Twenty-First Century*. ABC-CLIO, 2003.
- Zimmer, Michael. “‘But the Data Is Already Public’: On the Ethics of Research in Facebook.” *Ethics and Information Technology* 12, no. 4 (2010): 313–25.
- Zinnbauer, Markus, and Tobias Honer. “How Brands Can Create Social Currency--A Framework for Managing Brands in a Network Era.” *Marketing Review St. Gallen* 28, no. 5 (2011): 50–55.
- Zurkus, Kacy. “Social Media, the Gateway for Malware.” *CSO*, 2016. <https://www.csoonline.com/article/3106292/social-networking/social-media-the-gateway-for-malware.html>.