Wicked Crypto

Alan Z. Rozenshtein*

INTRODUCTION

More than thirty years ago, historian of technology Melvin Kranzberg put forward his famous "First Law": "Technology is neither good nor bad; nor is it

* Associate Professor of Law, University of Minnesota Law School. For helpful comments, I thank Steven Bellovin, Susan Landau, Mayank Varia, my colleagues at the University of Minnesota Law School, and participants at the Arizona State University Sandra Day O'Connor College of Law's Sixth Annual Conference on Governance of Emerging Technologies & Science: Law, Policy and Ethics conference and the Eleventh Annual Privacy Law Scholars Conference. For excellent research assistance, I thank Paul Dimic and Ronald Waclawski.

neutral."[1] By this he meant to combat technological determinism, by which a particular technology has a "good" or "bad" essence that dictated its adoption by and effect on society. But Kranzberg's law also cautioned against technological utopianism, the illusion that society can maintain full instrumental control of technology.

A stark illustration of Kranzberg's first law is modern information and communications technology. The Internet and its ecosystem of connected devices have profoundly altered individual and social life, including those aspects that are the topic of this symposium: the intersection of gender, law, and technology. Technology has enabled new forms of gender- and sexual-based crime and has frequently made it harder to prosecute those who commit sexual assault. Yet in many cases technology has also served as a shield for victims, getting them help and protecting their privacy. These effects, both negative and positive, have been of the unintended variety, as society grapples to adapt to technological change it does not fully understand. The Internet and its outgrowths have been neither good nor bad; but neither have they been neutral.

Of particular importance has been ubiquitous strong encryption, one of the core technologies underpinning digital life. Since its adoption by business and the public in the late 1980s and early 1990s, the issue of law-enforcement access to encrypted data has been hotly debated in the legal, policy, and technology communities.[2] After a decade and a half of relative peace, the "crypto wars" have started up again.[3] The issue has seen a revival in legal scholarship,[4] and it is also

[1] Melvin Kranzberg, *Technology and History: "Kranzberg's Laws,"* 27 TECH. & CULTURE 544, 545 (1986).

[2] *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

[3] The "crypto wars" is the common name for an intense period of policy debate in the 1990s between the government, Silicon Valley, and civil society over whether there should be any limits on the availability of strong encryption and, in particular, whether encryption systems should be designed to permit court-authorized government access to encrypted data. *See* Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 433–41 (2012).

[4] *See, e.g.*, ASHLEY DEEKS, HOOVER INSTITUTION, THE INTERNATIONAL LEGAL DYNAMICS OF ENCRYPTION, Aegis Series Paper No. 1609 (2016), https://www.hoover.org/research/international-legal-dynamics-encryption [https://perma.cc/SMY2-GK4F]; Justin (Gus) Hurwitz, *Encryption*^{Congress} *mod (Apple + CALEA)*, 30 HARV. J.L. & TECH. 355 (2017); Geoffrey S. Corn, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data*, 72 WASH. & LEE L. REV. 1433 (2015) [hereinafter *Averting the Inherent Dangers*]; Geoffrey S. Corn, *Encryption, Asymmetric Warfare, and the Need for Lawful Access*, 26 WM. & MARY BILL RTS. J. 337 (2017); Jamil N. Jaffer & Daniel J. Rosenthal, *Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge*, 24 CATH. U. J.L. & TECH. 273 (2016); Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989 (2018); Eric Manpearl, *Preventing Going Dark: A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate*, 28 U. FLA. J.L. & PUB. POL'Y 65 (2017); David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 CONN. L. REV. 1657 (2017); Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599 (2016); Swire & Ahmad, *supra* note 3.

salient in the policy arena, prompting high-profile reports from law-enforcement organizations,[5] information security researchers,[6] policy analysts,[7] and multiple branches of government,[8] including proposed legislation on all sides of the issue,[9] at both the federal and state levels.[10]

This Article seeks to advance the debate around government access to encrypted data. Part I explains how encryption secures communications and data; how it helps protect victims of crime; and how it impedes law enforcement, particularly at the state and local levels. Part II, the analytical core of the Article, introduces the public-policy literature on "wicked problems" to explain why the encryption issue is such a difficult one. Part III suggests some changes to policy and institutional design.

This Article aims at several audiences. The first is those—whether in the legal academy, government, industry, civil society, or the information-security community—who are working on the issue of law-enforcement access to encrypted data. We are in a critical period for this issue: public opinion is split on whether

[5] *See, e.g.*, Int'l Ass'n of Chiefs of Police, Data, Privacy and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence (2015); Manhattan Dist. Attorney's Office, Third Report of the Manhattan District Attorney's Office on Smartphone Encryption (2017) [hereinafter Manhattan DA Report].

[6] Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. Cybersecurity 69 (2015).

[7] Berkman Ctr. for Internet & Society at Harvard Univ., Don't Panic: Making Progress on the "Going Dark" Debate (2016) [hereinafter Don't Panic]; The Chertoff Grp., The Ground Truth About Encryption and the Consequences of Extraordinary Access (2016); Charles Duan et al., Policy Approaches to the Encryption Debate (R. Street Policy Study No. 133, 2018); EastWest Inst., Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions (2018); James A. Lewis et al., Center for Strategic & International Studies, The Effect of Encryption on Lawful Access to Communications and Data (2017).

[8] Nat'l Acads. of Sci., Eng'g & Med., Decrypting the Encryption Debate: A Framework for Decision Makers (2018) [hereinafter NASEM Encryption Report]; House Comm. on Homeland Sec., Going Dark, Going Forward: A Primer on the Encryption Debate (2016); Analytic Exchange Program, Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation (2017).

[9] *Compare* Cody M. Poplin, *Burr-Feinstein Encryption Legislation Officially Released*, Lawfare (Apr. 13, 2016, 6:12 PM), https://www.lawfareblog.com/burr-feinstein-encryption-legislation-officially-released [https://perma.cc/F7JV-A2MR] (describing legislation that would effectively ban encryption that did not provide exceptional access), *with* David Ruiz, *The Secure Data Act Would Stop Backdoors*, Electronic Frontier Found. (May 10, 2018), https://www.eff.org/deeplinks/2018/05/secure-data-act-would-stop-backdoors [https://perma.cc/3BGD-AF82], *and* Dustin Volz, *U.S. Lawmakers Seek to Bar States from Mandating Encryption Weaknesses*, Reuters (Feb. 10, 2016, 2:05 AM), https://www.reuters.com/article/us-usa-cyber-encryption/u-s-lawmakers-seek-to-bar-states-from-mandating-encryption-weaknesses-idUSKCN0VJ0VI [https://perma.cc/7VCL-RGKV].

[10] *See* Andy Greenberg, *Proposed State Bans on Phone Encryption Make Zero Sense*, Wired (Jan. 26, 2016, 7:00 AM), https://www.wired.com/2016/01/proposed-state-bans-on-phone-encryption-make-zero-sense [https://perma.cc/7K88-776U] (describing proposed California and New York legislation that would restrict encryption).

companies should design their systems to permit law-enforcement access;[11] technology companies can no longer assume a hands-off, deregulatory environment;[12] and the looming specter of foreign regulation from liberal and autocratic regimes alike gives the government and Silicon Valley an incentive to resolve the encryption issue one way or the other, thereby setting a global precedent.[13] My hope is that this article will nudge the discussion away from oppositional, all-or-nothing analyses of short-term proposals and toward a higher-level, longer-term approach that can find common ground among the various sides.

Another audience this Article addresses is scholars who study the intersection of gender, equality, and technology. For these scholars, I hope my account will usefully inform them of an important technological dimension to how the internet and other communications and computing technology can both undergird and undermine attempts to end gender and sexual crime.

Finally, this Article speaks to scholars of administrative law and regulatory theory. In particular, I hope my discussion of wicked problems provides a novel and useful lens through which administrative-law scholars think about how to grapple with today's biggest regulatory challenges.[14]

I. ENCRYPTION AND PUBLIC SAFETY

Much has been written about how encryption can both support and undermine public safety,[15] so I will keep my discussion of this issue short. I first give a brief definition of encryption and the associated issue of *exceptional access*, third-party access to decrypted data or communications. I then discuss how encryption can improve public safety, focusing (given the topic of this symposium) on how encryption can help victims of sexual and gender violence. I conclude by

[11] *See* Aaron Smith, *Americans and Cybersecurity: 3. Attitudes About Cybersecurity Policy*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/3-attitudes-about-cybersecurity-policy [https://perma.cc/BR6Q-2Z3U] ("Americans remain divided over whether government should be able to access encrypted communications.").

[12] *See* Alan Z. Rozenshtein, *Silicon Valley's Regulatory Exceptionalism Comes to an End*, LAWFARE (Mar. 23, 2018, 7:00 AM), https://www.lawfareblog.com/silicon-valleys-regulatory-exceptionalism-comes-end [https://perma.cc/YV79-QW4Q].

[13] *See* DEEKS, *supra* note 4, at 18 ("There is likely a modest first-mover advantage to be gained by deciding the US position [encryption] quickly and promoting that position . . . ."); Hurwitz, *supra* note 4, at 417 ("If the United States engages in a serious discussion about possible approaches to regulating encryption today, the discussions we have will have some ability to set standards and moderate approaches set elsewhere . . . .").

[14] I am not the first to use the "wicked problems" framework in a legal setting. *See, e.g.*, Richard J. Lazarus, *Super Wicked Problems and Climate Change: Restraining the Present to Liberate the Future*, 94 CORNELL L. REV. 1153 (2009); Sharon Lewis, *The Tissue Issue: A Wicked Problem*, 48 JURIMETRICS J. 193 (2008). Nevertheless, its use is sporadic in the literature, and my hope is that this Article will contribute to its adoption as part of the legal analyst's toolkit. *Cf.* WARD FARNSWORTH, THE LEGAL ANALYST: A TOOLKIT FOR THINKING ABOUT THE LAW (2007).

[15] For a balanced overview, see NASEM ENCRYPTION REPORT, *supra* note 8, at 27–39.

describing how encryption can pose challenges for public safety, in particular by thwarting law-enforcement investigations at the federal, state, and local levels.

A. Encryption and Exceptional Access

In order to cryptographically secure data, both the sender and recipient of the communication (or, in the case of stored data, the user at the time they encrypt the data and when they later seek to decrypt it) must jointly know some shared piece of secret information, referred to as the *key*.[16] The process of generating and sharing the key, known as the problem of secure key exchange, is a complex one. To make their devices and services user-friendly, companies that build encryption into their products also handle secure key exchange behind the scenes. For example, when you set up a passcode or fingerprint on an iPhone, you are providing information that the iPhone uses to generate the key that will encrypt the device when you lock it and then decrypt the device when you unlock it. Similarly, when you register for a WhatsApp account, WhatsApp generates a key, known only to you (specifically, to the WhatsApp program on your various devices) that allows you to communicate securely with others.

When companies design their cryptographic systems—specifically the details of how they handle secure key exchange—they have to decide whether or not to keep a copy of the key or some other means, independent of the user, to decrypt the information. If they don't keep a copy, then only the user (and their intended recipient) can decrypt the resulting encrypted data. If, by contrast, the company keeps a copy of the key—or builds the system with a "backdoor" so that any device or application can be accessed, under certain circumstances, by the company—then the data can be decrypted by the company, for its own purposes or on behalf of the government or some other third party. This capability is known as *exceptional access*.[17]

There are good reasons for companies to build exceptional access into their systems; it allows them to provide their users with useful features like malware scanning, password recovery, and text prediction. But for law enforcement the key benefit is that the companies can decrypt data or provide access to locked devices in response to government orders.

As discussed in more detail below,[18] the problem is that, all else being equal, a system without exceptional access is more secure than the same system that allows exceptional access (whether by the government, the company that designed the system, or someone else). This tradeoff between government access and

[16] Public-key cryptography (for example, RSA) allows for encrypted communications without a shared secret. However, public-key cryptography requires substantially more computation than does symmetric cryptography (which requires both parties to have access to the same key), and so bulk data is normally encrypted using symmetric encryption. *See* KEITH M. MARTIN, EVERYDAY CRYPTOGRAPHY 21–24, 178–80 (2d ed. 2017).

[17] *See* NASEM ENCRYPTION REPORT, *supra* note 8, at 15.

[18] *See infra* Part III.A.1.

information security is at the core of the roiling public debate over encryption policy.

B. Encryption as a Tool for Victims of Crime

Encryption is an important tool for individuals seeking to protect themselves from a variety of threats to their finances, privacy, or safety. In keeping with the theme of this symposium, I offer several examples of how encryption can help protect individuals from sexual and gender crime, but it's important to emphasize that these same benefits apply to other use cases.

By keeping data inaccessible to third parties, encryption can thwart would-be abusers. As the National Network to End Domestic Violence notes:

> [An abuse victim's] smartphone is often one of the first things an abuser will target simply because of the amount of information on there. If they can compromise the victim's smartphone, they have access to all phone calls, messages, social media, email, location information, and much more. For these reasons, smartphone security and encryption is essential to safeguarding the privacy of victims' personal information.[19]

Similarly, domestic-abuse victims can use encrypted messaging applications like WhatsApp to securely talk to supportive family or friends, without their abuser knowing.

Encryption can also help prevent violations of a broad range of what Danielle Keats Citron has called "sexual privacy": "access to . . . information about . . . our bodies, sexual and gender identities, and intimate activities."[20] For example, encryption can help secure devices that store intimate pictures and videos, thus helping prevent "revenge porn." In the future, "deep fakes"—"hyper-realistic digital falsification of images, video, and audio,"[21] often used to create non-consensual pornography—might be countered with "immutable life logs," which would use encryption to "make it possible for a victim of a deep fake to produce a certified alibi credibly proving that he or she did not do or say the thing depicted."[22]

C. Encryption as a Tool for Criminals

At the same time that encryption can act as a shield against sexual and gender crime, it can also help facilitate such crime, both by helping abusers remain

[19] *Smartphone Encryption: Protecting Victim Privacy While Holding Offenders Accountable*, TECHNOLOGY SAFETY (Apr. 12, 2016), https://www.techsafety.org/blog/2016/4/12/smartphone-encryption-protecting-victim-privacy-while-holding-offenders-accountable [https://perma.cc/HC87-JWMU].

[20] Danielle Keats Citron, *Sexual Privacy*, 128 YALE L.J. 1870 (2019).

[21] Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. (forthcoming 2019) (manuscript at 4), https://papers.ssrn.com/abstract_id=3213954 [https://perma.cc/3FXE-TEZ2].

[22] *Id.* at 54.

anonymous and by making it harder for law enforcement to investigate them. Investigations into sexual and general crimes are only a subtype of those that can be stymied by encryption, but they are well represented. For example, in the burgeoning caselaw on whether the Fifth Amendment's privilege against self-incrimination applies to a defendant's disclosure of phone or computer passcodes, investigations into child pornography and sex trafficking present a common fact pattern.[23] Encryption can frustrate investigations into violent crimes, including sexual assault[24] and sex trafficking.[25] And it can even affect the government's highest-priority activities: end-to-end encryption on popular communications services like WhatsApp and FaceTime may have hindered Special Counsel Robert Mueller's investigation into Russian interference in the 2016 presidential election.[26]

It is impossible to know the precise extent to which encryption frustrates law-enforcement investigations, both because law-enforcement agencies are only beginning to collect accurate statistics, and because one can never be sure of how an investigation would have proceeded in the absence of encryption. But the top-line conclusion is clear: as a report by the National Academies notes, "widespread encryption is having a serious and growing negative impact on the ability of law enforcement to collect relevant plaintext [i.e., unencrypted data]."[27] For example, the FBI estimates that it has over a thousand encrypted smartphones in evidence that it cannot access due to encryption.[28] From 2014 to 2017 the Manhattan District

[23] *See, e.g.*, United States v. Spencer, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018); United States v. Apple MacPro Computer, 851 F.3d 238, 242 (3d Cir. 2017); United States v. Doe (*In re* Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011), 670 F.3d 1335, 1339 (11th Cir. 2012); Commonwealth v. Jones, 481 Mass. 540, 541 (2019). The issue has recently generated substantial scholarly attention. *See, e.g.*, Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. 169 (2018); Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203 (2018); Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019).

[24] MANHATTAN DA REPORT, *supra* note 5, at 8.

[25] Ellen Wulfhorst, *Technology Use by Sex Traffickers Fuels Debate Between Privacy and Security*, REUTERS (Apr. 25, 2017, 2:14 PM), https://www.reuters.com/article/us-trafficking-conference-technology-idUSKBN17R2UI [https://perma.cc/2XX9-SHLC].

[26] *See* Craig Timberg & Drew Harwell, *How WhatsApp, FaceTime and Other Encryption Apps Shaped the Outcome of the Mueller Report*, WASH. POST (Apr. 19, 2019), https://www.washingtonpost.com/technology/2019/04/19/how-whatsapp-facetime-other-encryption-apps-shaped-outcome-mueller-report/ [https://perma.cc/S7BB-27S7].

[27] NASEM ENCRYPTION REPORT, *supra* note 8, at 42.

[28] The FBI initially estimated that it had nearly eight thousand such devices, but later realized that this figure was inflated more than fivefold due to errors. *See* Devil Barrett, *FBI Repeatedly Overstated Encryption Threat Figures to Congress, Public*, WASH. POST (May 22, 2018), https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress-public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html [https://perma.cc/KWW6-MXJS]; Henry Farrell, *The FBI Blunder on Phone Encryption, Explained*, WASH. POST (May 30, 2018), https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/30/the-fbi-blunder-on-phone-encryption-explained [https://perma.cc/U5ZH-5C77].

Attorney's Office seized over two thousand encrypted smartphones.[29] And state and local law-enforcement agencies across the country have experienced similar problems accessing encrypted data.[30] Nor is the problem limited to the United States. Governments around the world have struggled to access encrypted data, to the point that some countries have proposed laws that would mandate provider assistance with decryption.[31]

The impact of encryption on ordinary law-enforcement investigations has often been overshadowed by its hypothetical effects on foreign intelligence and national security. For example, the controversy over the government's attempt to force Apple to help it unlock the iPhone of one of the San Bernardino terrorists involved a federal agency (the FBI) investigating a high-profile national-security incident (the San Bernardino terrorist attacks).[32] Government officials continue to highlight the use of encrypted communications by terrorists. For example, when FBI Director Christopher Wray testified before Congress in late 2017, the first encryption-related example he gave was of FBI "agents and analysts . . . increasingly finding that communications and contacts between groups like ISIS and potential recruits occur in encrypted private messaging platforms."[33]

Encryption can certainly make it harder for national-security and foreign-intelligence agencies to do their jobs, but its effect in those contexts is likely to be limited. The universe of national-security and foreign-intelligence targets is small relative to the resources and expertise of the federal government. With enough effort, the government's "three-letter agencies" (like the FBI, the NSA, or the CIA) can likely hack their way into even the most sophisticated adversary's systems (or, as occurred in the San Bernardino case, purchase third-party tools that do the same).

Instead, encryption poses the largest danger to investigations into "ordinary" crime, especially that which falls under the jurisdiction of state or local law enforcement, which may lack the resources or expertise to get around sophisticated encryption. As the Manhattan DA's Office has argued, "[b]ecause obtaining [encrypted] evidence is extremely costly in the expanding 'lawful hacking'

[29] MANHATTAN DA REPORT, *supra* note 5, at 5.

[30] MANHATTAN DIST. ATTORNEY'S OFFICE, REPORT OF THE MANHATTAN DISTRICT ATTORNEY'S OFFICE ON SMARTPHONE ENCRYPTION AND PUBLIC SAFETY: AN UPDATE TO THE NOVEMBER 2015 REPORT 10–11 (2016).

[31] For example, a recent Australian law allows the government to issue compulsory "technical capability notices" that would obligate providers to redesign their systems so as to help the government decrypt information, although such notices would not cover design changes to "remov[e] one or more forms of electronic protection that are or were applied by, or on behalf of, the provider." *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Austl.), https://www.legislation.gov.au/Details/C2018A00148 [https://perma.cc/LJ94-MQDU].

[32] *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 102–03 (2018).

[33] Christopher Wray, Dir., Fed. Bureau of Investigation, Statement Before the House Homeland Security Committee: Keeping America Secure in the New Age of Terror (Nov. 30, 2017), https://www.fbi.gov/news/testimony/keeping-america-secure-in-the-new-age-of-terror [https://perma.cc/65W3-U6H9].

marketplace, . . . it is available only in cases handled by a small minority of well-funded agencies. Crime victims thus have unequal access to justice, depending on the resources of the city or county in which they live."[34] Conversely, the majority of criminals are likely to stick with commercially available software rather than deploy their own sophisticated encryption systems.[35] Thus, were the government able to convince the major technology companies to build exceptional access into their systems, such access might provide a large return in the form of increased law-enforcement effectiveness.

II. ENCRYPTION AS A WICKED PROBLEM

As this section will demonstrate, the issue of encrypted-data access is best conceptualized as a "wicked" problem that requires a special approach, and a special set of institutions, to solve.

A. Introduction to Wicked Problems

Although wicked problems are as old as social organization itself, their unique characteristics were first formalized in the 1960s and '70s.[36] There are many competing definitions of "wicked" problems, but the definition that first appeared in the planning and public-policy literatures remains a good starting place: that "class of social system problems which are ill-formulated, where the information is confusing, where there are many clients and decision makers with conflicting values, and where the ramifications in the whole system are thoroughly confusing."[37]

One way of understanding the nature of wicked problems is to compare them to their opposite, "tame" problems.[38] Although tame problems may be difficult to solve and require complex analysis, they are in principle solvable. For example, imagine the problem of building a bridge over a river. Physically constructing the bridge is a tame problem. Once the design specifications are set, the builder can use a set of well-developed construction processes to build the bridge. The problems of pouring concrete and placing girders are well-understood; the goals are clear; insights gained in one project can be translated to the next; there is a clear end-point (the bridge is built); there are clear success criteria (the bridge doesn't fall down); and the problem is relatively self-contained (you don't need to solve environmental, transportation, or distributional public-policy problems to build the bridge).

Now compare the process of building the bridge with that of designing it: determining where it should be located, what transportation options it should provide (cars, busses, trains, pedestrians, cyclists), whether to charge fees for its use,

[34] MANHATTAN DA REPORT, *supra* note 5, at 9.

[35] *See* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 14–15 (2014).

[36] *See* C. West Churchman, *Wicked Problems*, 14 MGMT. SCI. B141 (1967); Horst W.J. Rittel & Melvin M. Webber, *Dilemmas in a General Theory of Planning*, 4 POL'Y SCI. 155 (1973).

[37] Churchman, *supra* note 36, at B141.

[38] *See* Rittel & Webber, *supra* note 36, at 160.

and so on. This has all the hallmarks of a wicked problem. The goals are often unclear and contested. Different groups may demand different things: homeowners near the bridge may prioritize that it not block their view of the river; car and mass-transit advocates may fight over whether the bridge should have dedicated bus lanes; and environmentalists may be concerned with the bridge's impact on the river's ecology and pollution levels. There's no clear end-point to the problem, since once the bridge is built, it will cause second-order effects on traffic, residential patterns, and the environment that will have to be dealt with (and these second-order effects will interact with each other, causing complicated interdependencies). Because of the many and conflicting goals, there are no clear success criteria. And because the context in which each bridge is built is unique, involving a different constellation of interest groups and facts on the ground, it's hard to apply lessons learned from a "successful" bridge project in a context different from the current one.

Wickedness is neither rare nor even particularly uncommon in today's policy landscape. Indeed, one could argue that any long-run policy problem that hasn't yet been solved is, at least among some dimensions, wicked.[39] But the ubiquity of wicked problems does not render the concept of wickedness superfluous; rather, it underscores the importance, when confronting a policy problem, of clearly and forthrightly recognizing those aspects that make it so difficult to solve. Thus, the wicked-problem framework provides a sort of conceptual checklist by which proposed solutions can be evaluated, and proposals—whether quick fixes or comprehensive solutions—can be quickly weeded out if they overpromise or otherwise ignore the inherent intractability of wicked problems.[40] In other words, a diagnosis of wickedness can bring about policy humility, which has two additional useful consequences. It may lead us to take seriously proposals that might otherwise be discarded as imperfect, second best, or non-ideal, so that the unobtainable perfect does not crowd out the attainable good (or even middling).[41] And this sense of humility may lead parties on various sides of the issue to view each other's proposals and perspectives more charitably, and to better appreciate the value of compromise.

B. Dimensions of Wickedness

The argument of this section is that the problem of government access to encrypted data is a quintessential wicked problem. Here, I draw from various theoretical discussions of wicked problems to identify their most salient features.

[39] *See* B. Guy Peters, *What Is So Wicked About Wicked Problems? A Conceptual Analysis and a Research Program*, 36 POL'Y & SOC'Y 385, 388 (2017).

[40] *See infra* Part III.A.

[41] *See infra* Part III.B.

1. There Is No Agreement on Goals

Conflicts over goals and values lie at the heart of many wicked problems. A fundamental difficulty in solving the problem of law-enforcement access to data is that there is no consensus as to what problem needs to be solved. Is the issue that law enforcement is "going dark" in a way that threatens public safety, or is the issue that law enforcement is enjoying a "golden age of surveillance" that threatens privacy and civil liberties?[42] As a result of this indeterminacy, traditional policy analysis—such as attempts to require technology companies to internalize the social costs of encryption—is similarly indeterminate.[43]

As fundamental as this problem uncertainty is, it's only the most visible of a number of framing conflicts. At the same time that the government wants access to encrypted data, the companies that are making those devices are desperately trying to protect them from hackers and criminals. Thus, what might appear from the government's perspective as an ecosystem whose cybersecurity is too robust (at least when it comes to preventing lawful government access) is, from the perspective of technology companies, a cat-and-mouse game between hackers and technology companies that the companies are barely staying on top of. Indeed, this tension runs so deep that the government can sometimes sound contradictory, as when officials urge companies to build exceptional-access capabilities and widely deploy "strong encryption" all at the same time. This does not mean that exceptional access systems are, from an information-security perspective, worthless, but it does mean that the two goals present difficult tradeoffs.

Part of the problem is that the very definition of the term "secure" (as in "secure encryption" or "secure system") depends on contested value judgments. In the real world, security is never an all-or-nothing proposition. Security always comes at a cost; for example, it takes more time and money to design more secure systems, and security often requires trading off user features like password or data recovery. The real question is whether a particular system is "secure enough." This in turn requires tallying up the benefits of the system to information security and

[42] *Compare* James B. Comey, Dir., Fed. Bureau of Investigation, Remarks Before the Brookings Institution: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? 2 (Oct. 16, 2014), https://www.brookings.edu/wp-content/uploads/2014/10/10-16-14-Directors-Remarks-for-Brookings-Institution-AS-GIVEN.pdf [https://perma.cc/6G5Y-5TWJ] ("Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it 'Going Dark,' and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."), ***with*** Swire & Ahmad, *supra* note 3, at 420 ("Notably, law enforcement and national security agencies fear they are 'going dark' as criminals and terrorists increasingly use a bewildering variety of new communications tools. On more careful examination, however . . . this mix of new technology is actually enabling a 'golden age of surveillance.'").

[43] *Cf.* Claire A. Hill, *The Rhetoric of Negative Externalities*, 39 SEATTLE U. L. REV. 517, 525 (2016).

comparing those to the costs of that system to, for example, public safety in the form of relevant data that is unavailable to law enforcement. This is not just an empirical question; it is also a tradeoff between two security *values*: how much (public-safety) security are we willing to give up for (information) security?[44]

Not only is cybersecurity a rival to public safety but so is business competitiveness (a factor that encryption advocates are understandably reluctant to emphasize publicly). Companies may resist demands by the government to provide access to data because complying with such demands might be technologically costly, or because it might cost companies business with civil liberties-minded users, especially abroad.[45]

A final conflict is between the public safety of Americans versus the civil rights of foreigners, particularly those living in repressive regimes. One argument commonly raised against lawful access mandates is that their presence in the United States will make it easier for other countries—particularly authoritarian ones—to demand the same access. But unlike the United States, those countries may not use this access in lawful or rights-respecting ways.[46] As one technology-company employee told me, "The government only has to worry about the safety of its citizens. We don't have that luxury. We have to worry about the safety of our users everywhere, including from their own governments."

2. Information Is Uncertain and Diffuse

A key challenge in solving wicked problems is that the information that is necessary to solve them is usually unavailable, either because it is distributed among numerous stakeholders, because it is hard to discover, or because it is fundamentally unknowable. The problem of government access to encrypted data exhibits all these informational difficulties.

First, we don't know whether it is possible to build reasonably secure encryption systems that provide exceptional access. Security researchers have convincingly argued that building any such systems would require overcoming several serious technical challenges—challenges to which there are no known solutions.[47] The question is how we ought to view the consensus position: as a call for further research, or instead as a convincing-enough demonstration of impossibility that settles the matter?

Several reasons suggest the former: the consensus position is best viewed as a hypothesis that, while strong, should not yet be taken as conclusive. First, serious researchers continue to work on the problem, and their work may yet lead to a breakthrough.[48] Second, widespread antipathy toward government in the

[44] *See* Rozenshtein, *supra* note 32, at 137.

[45] *See id.* at 117–18.

[46] *See, e.g.*, Abelson et al., *supra* note 6, at 71.

[47] *See generally id.*

[48] *See* NASEM ENCRYPTION REPORT, *supra* note 8, at 46–47 (describing several

technology industry and security-research community[49] may be scaring away some researchers from tackling the problem. For example, in his keynote speech at a European information-security conference, Bart Preneel, a renowned Belgian cryptographer whose research in encryption has made him both a hero to the information-security and privacy communities and a thorn to law enforcement, encouraged cryptographers to research secure exceptional-access systems (in addition to generally improving the state of information security). After noting that encryption "may sometimes damage what police do," Preneel explained the need for further research:

> [I]t seems to be also a kind of a taboo to work on law-enforcement access, and I think we should actually break this taboo. We should not say it's impossible. I think we should think about it at least. Write papers: how can we do this better? . . . [I] don't think it should be a forbidden question to think about. Imagine we had perfect channels, perfectly secure devices—there [are] some cases where government may need access. How would we do this? In an auditable way, in a controllable way, in a limited way. We have actually no answers either.[50]

The dangers of groupthink in retarding scientific research by disfavoring certain research agendas is well-known[51] and reflects a more general facet of motivated cognition. As Claire Hill has observed, "[I]t is difficult to get a person to understand something when her (individual and[,] more importantly, social) identity depends on her not understanding it."[52] The presence of groupthink and taboo-

recent proposals); *see also* Steven Levy, *Cracking the Crypto War*, WIRED (Apr. 25, 2018), https://www.wired.com/story/crypto-war-clear-encryption/ [https://perma.cc/X5MC-LEQV] (describing one of these proposals in greater depth). Many proposals are variations on the "key escrow" model made (in)famous by the failed Clipper Chip, and, as such, they have been criticized on similar grounds. *See, e.g.*, Matthew Green, *A Few Thoughts on Ray Ozzie's "Clear" Proposal*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (Apr. 26, 2018), https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/ [https://perma.cc/MU38-LD45]; *see also* STEFAN SAVAGE, LAWFUL DEVICE ACCESS WITHOUT MASS SURVEILLANCE RISK: A TECHNICAL DESIGN DISCUSSION (2018). Other proposals do not rely on key escrow. *See, e.g.*, CHARLES V. WRIGHT & MAYANK VARIA, CRYPTO CRUMPLE ZONES: ENABLING LIMITED ACCESS WITHOUT MASS SURVEILLANCE (2018), https://web.cecs.pdx.edu/~cvwright/papers/crumplezones.pdf [https://perma.cc/3Q7G-E4DH].

[49] Rozenshtein, *supra* note 32, at 118–19.

[50] Bart Preneel, *The Future of Cryptography*, EUROCRYPT (June 5, 2016), https://www.youtube.com/watch?v=GWXIxBd3m0Y [https://perma.cc/5SK9-MCZV] at 56:58–57:34; *see also* Kieran McCarthy, *Crypto-Gurus: Which Idiots Told the FBI That Feds-only Backdoors in Encryption Are Possible?*, REGISTER (Feb. 14, 2018, 8:06 PM), https://www.theregister.co.uk/2018/02/14/cryptography_experts_fbi/ [https://perma.cc/NB3Y-RDYE] ("The FBI is also unlikely to release the names of those it has been consulting over fears that they would be ridiculed and come under pressure from their peers not to work on such an approach.").

[51] The recognition that scientific research can be shaped by psychological, sociological, and other non-scientific considerations is at the heart of modern sociological studies of science. *See generally* THOMAS S. KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (4th ed. 2012).

[52] Claire A. Hill, *An Identity Theory of the Short- and Long-Term Investor Debate*, 41 SEATTLE U. L. REV. 475, 482 (2018).

driven reasoning does not by itself undermine the current consensus that secure exceptional access is impossible. But it does suggest that more research is in order.

A second informational difficulty with the problem of access to encrypted data is that it exhibits many complex interdependencies and second-order effects. The obvious examples are technological. On the one hand, exceptional access may create systemic, hard-to-predict security risks that harm overall information security. On the other hand, a regime of widespread lawful hacking (the only plausible alternative to third-party access) could have its own negative effects on information security.[53]

Second-order effects go beyond technical issues. On the legal front, the increasing prevalence of encryption could lead courts to restrict Fourth Amendment rights in a variety of ways. For example, they could expand the exigent circumstances doctrine to allow police to warrantlessly search unlocked cell phones that are recovered incident to arrest if the police credibly believe the phones are about to auto-lock or become otherwise inaccessible.[54] And if metadata becomes comparatively more important to law-enforcement investigations[55]—since metadata, unlike content, is likely to remain unencrypted[56]—courts may think twice about further limiting the reach of the third-party doctrine.[57]

A third problem is that the encryption issue has several distinct sub-issues, each with its own unique challenges. The problem of "data in motion" (data that is encrypted as it travels across the Internet) is distinct from the problem of "data at rest" (data that is encrypted when it is stored). Data-at-rest problems can be further subdivided: Is the data stored on the user's device or in the cloud? Would exceptional access only apply to a company's own products or would it require the company to block non-complying third-party application; for example, would it be enough for Apple to provide exceptional access for iOS devices and its iMessage service, or would it also have to prohibit third-party secure-messaging apps like Telegram or Signal? Would the exceptional-access procedure require that the government have physical access to the device or would it permit remote access (which would increase the risk of unauthorized access)?

[53] *See infra* Part III.B.

[54] *See* Rozenshtein, *supra* note 32, at 169–70. In the summer of 2018, Apple released a software update that would make it impossible for third parties, including law enforcement, to access a locked iOS device's data and charging port an hour after the device is locked. Jack Nicas, *Apple to Close iPhone Security Hole That Law Enforcement Uses to Crack Devices*, N.Y. TIMES (June 13, 2018), https://www.nytimes.com/2018/06/13/technology/apple-iphone-police.html [https://perma.cc/VT53-D6LP]; *see also* Riana Pfefferkorn, *Exigent Circumstances: iOS 12's USB Restricted Mode and Warrantless iPhone Access,* JUST SECURITY (June 22, 2018), https://www.justsecurity.org/58345/exigent-circumstances-ios-12s-usb-restricted-mode-warrantless-iphone-access [https://perma.cc/NZB5-YTNP].

[55] Pell, *supra* note 4, at 619–20.

[56] DON'T PANIC, *supra* note 7, at 3.

[57] *See* Carpenter v. United States, 138 S. Ct. 2206 (2018). *See generally* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943 (2019).

A fourth issue is that there is no way to test whether a particular exceptional-access solution works—whether from a technological, legal, or policy perspective—except to try it. But attempts to solve wicked problems are not free—they leave "'traces' that cannot be undone."[58] Because decision-makers are not free to experiment, the decisions they ultimately make will be hampered by suboptimal information. This makes it that much more important to do as much pre-implementation analysis, and to collect as much information from as broad an array of sources, as is possible.

A fifth informational difficulty is that the past can only offer limited lessons.[59] It is tempting to think of the current debate as a repeat of the crypto wars of the 1990s. But some commentators have gone further, arguing that the issue of government access to encrypted data was definitively resolved with the failure of the Clipper Chip, government-designed hardware that would be incorporated into consumer devices and that would simultaneously provide encryption and exceptional access.[60] For example, Steven Levy, author of the leading history of the crypto wars,[61] has asked, "Why are we fighting the crypto wars again?" and has complained that the U.S. government is "welching on [the] deal" that resolved the first crypto wars—that cryptography would be left largely unregulated.[62]

But stare decisis doesn't apply to public policy, especially when the technological, policy, and legal debates at issue are over twenty years old. First, there's no guarantee that the issue of government access to encrypted devices was properly decided in the 1990s. Although specific flaws were indeed discovered in the Clipper Chip's design, those flaws were not in the level of protection afforded to the user (the sort of flaw that would be of greatest concern in a mandatory-access regime); rather, the flaws could allow individuals to bypass the key escrow process, thereby rendering their communications confidential as against the government.[63] It is possible that additional research could have solved these problems.

Second, and more importantly, even if the first crypto war was properly resolved (for example, because the sort of key-escrow system the government proposed was simply too vulnerable[64]), that doesn't mean that the current policy dispute should be precluded by the previous one. Too many variables are different

[58] Rittel & Webber, *supra* note 36, at 163.

[59] *Id.* at 164–65.

[60] *See* Froomkin, *supra* note 2, at 752–79.

[61] *See* STEVEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT—SAVING PRIVACY IN THE DIGITAL AGE (2001).

[62] Steven Levy, *Why Are We Fighting the Crypto Wars Again?*, WIRED (Mar. 11, 2016, 12:00 AM), https://www.wired.com/2016/03/why-are-we-fighting-the-crypto-wars-again [https://perma.cc/5ZHQ-N9FA].

[63] *See* Matt Blaze*, Protocol Failure in the Escrowed Encryption Standard*, 2 PROC. ACM CONF. ON COMPUTER & COMM. SECURITY 59 (1994).

[64] *See* Hal Abelson et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, 2 WORLD WIDE WEB J. 241 (1997).

today than they were twenty years ago. From the government's perspective, encryption has spread enormously in the past twenty years, from a few niche applications to being omnipresent, especially on consumer devices like phones, tablets, and computers. Thus, why shouldn't the U.S. government "welch" on a "deal" that really amounted to a temporary truce, especially if the cost-benefit analysis may have changed? As Levy himself admits, the reason crypto wars have restarted is because "[f]or the first time, [the government is] really struggling with the results of the first war, as more information is now encrypted, increasingly in a manner the government finds really hard (or impossible) to decode."[65]

Alternatively, from the perspective of industry and information-security advocates, the very spread of encryption means that any risk that a government-access mandate could be compromised makes it that much more important to resist them. For both sides, then, the current environment is sufficiently different as to render any "lessons" from the first crypto wars at best provisional.

3. The Problem Cannot Be Fully or Permanently Solved

There can and will be no permanent resolution to the problem of law-enforcement access to encrypted data, for several reasons. First, as just mentioned, the resolution of a particular problem is always contingent and up for renegotiation, since the underlying parameters of the negotiation—for example, the technological realities and the costs and benefits to various social values like privacy and security—can change over time. Again, it's a fallacy to ascribe precedential force to a public-policy status quo.

Second, the nature of the problem keeps changing as technology advances. In the 1990s, law enforcement's chief concern was encryption. In the interbellum period of the 2000s—after the first crypto war ended and before the second broke out—law enforcement's focus switched to ensuring that voice-over-IP (VoIP) telephone and other communications providers maintained intercept capabilities.[66] Today, encryption is back in the spotlight, but it is far from the only part of the "going dark" problem. Equally important is law-enforcement access to data stored by U.S. companies outside the United States.[67] No doubt the future will subject lawful surveillance to technical impediments as yet unimagined.

Third, any solution to the problem of government access to encrypted data will involve costly tradeoffs. On the one hand, any solution will likely decrease, at

[65] Levy*, supra* note 62.

[66] *See* Am. Council on Educ. v. F.C.C., 451 F.3d 226, 227 (D.C. Cir. 2006) (upholding the FCC's classification of broadband and VoIP providers as "telecommunications carriers" under CALEA); Valerie Caproni, Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security (Feb. 17, 2011), https://archives.fbi.gov/archives/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies [https://perma.cc/TT77-8BAJ].

[67] *See* Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. § 2523 (2018).

least marginally (and perhaps substantially more), the overall security of encrypted systems. Security researchers will thus—as they should—constantly advocate for changes to the system so as to minimize those risks.

On the other hand, no solution will fully prevent criminals from using encryption that law enforcement cannot defeat, because there are hundreds of encrypted hardware and software services, both in the United States and abroad, that an individual seeking encrypted communications or storage could use.[68] Even the most extreme government-access proposals would not be able to reach every encrypted product in the United States, not to mention foreign products. This does not mean that attempts to regulate encryption are fruitless. The vast majority of criminals are unsophisticated and will stick to the most popular consumer products (which could be more easily regulated).[69] And the resources freed up by easier access to those criminals' data could be used on the expensive, one-off techniques—such as lawful hacking[70]—necessary to access the encrypted data of more sophisticated criminals. But law enforcement will still frequently be stymied in its quest for data and so will continuously push for farther-reaching regulation of encryption.

As the political scientist Charles E. Lindblom explained in a seminal article on public administration: "Policy is not made once and for all; it is made and re-made endlessly. Policy-making is a process of successive approximation to some desired objectives in which what is desired itself continues to change under reconsideration."[71] The problem of law-enforcement access to encrypted data typifies this chronic aspect of the most difficult policy problems.

****

The above discussion may strike some as discouraging, but it need not. Recognizing that something is a wicked problem is not an admission of its insolubility; rather, it's just a realistic appreciation of its challenges. Progress on difficult social problems reflects, almost by definition, progress on wicked problems, whether economic inequality, environmental degradation, or government access to data. Progress can be made, but it first requires a clear-eyed appreciation of the nature of the problem and the nature of its challenges.

III. LESSONS

A. Beware Easy Answers

If nothing else, recognizing that law-enforcement access to encrypted data is a wicked problem should make us skeptical of proposals that attempt to fully solve (or dissolve) the problem. A particularly common mistake in this regard is to

[68] *See* BRUCE SCHNEIER, KATHLEEN SEIDEL & SARANYA VITAYAKUMAR, A WORLDWIDE SURVEY OF ENCRYPTION PRODUCTS 2 (2016), https://www.schneier.com/cryptography/paperfiles/worldwide-survey-of-encryption-products.pdf [https://perma.cc/E7EV-N2QN].

[69] *See* Bellovin et al., *supra* note 35.

[70] *See infra* Part III.B.

[71] Charles E. Lindblom, *The Science of "Muddling Through"*, 19 PUB. AD. REV. 79, 86 (1959).

propose a solution that either ignores or denies the existence of the complexities and tradeoffs that categorize wicked problems. This section gives two such examples—one advanced by the government, the other by its critics—and illustrates how the theory of wicked problems can vividly highlight each argument's flaws.

1. *Exceptional-Access Mandates*

As noted above, the decision to design an encrypted system that doesn't permit exceptional access is not preordained. Rather, it is a design choice that each provider makes depending on its values and business interests, as well as what it believes its users demand. For this reason, when the government is faced with an encrypted system that it cannot access, even with a warrant or other judicial process, it can try to demand that the provider redesign its system or take some other action to help the government access the needed data. Collectively, we can call all such requests *exceptional-access mandates*.

The problem is that systems that permit exceptional access are generally less secure than systems that don't. There are several reasons for this. First, the more entities there are that can decrypt data, the more opportunities there are for a bad actor to access that data, including by hacking or getting help from insiders. Second, a system that allows for exceptional access is more complicated than a system without such access and thus "run[s] afoul of the information security axiom that 'complexity is the enemy of security.'"[72] This is especially true for systems that give law enforcement access, since they would have to cater to many different law-enforcement entities, both in the United States and around the world. A system that gave the FBI access might not work the same way for the tens of thousands of state and local law-enforcement agencies. And it would be even harder to design a system that would simultaneously give United States and French (let alone Russian or Chinese) law-enforcement officials access without opening one country's citizens up to the risk of surveillance by another country's government.[73]

For various reasons, the government has so far declined to offer any proposals for how a law-enforcement exceptional-access system would actually work.[74]

[72] *See* Rozenshtein, *supra* note 32, at 138 (2018) (citing Ronald L. Rivest, *On the Notion of "Software Independence" in Voting Systems*, 366 PHIL. TRANSACTIONS ROYAL SOC'Y A 3759, 3760 (2008) ("It is a common maxim that complexity is the enemy of security and accuracy, thus it is very difficult to evaluate a complex system.")).

[73] *See* Abelson, *supra* note 6, at 18.

[74] Reasons include that the government recognizes that industry has greater technical expertise than the government does (at least outside the foreign-intelligence context), performance standards are generally more popular than are design mandates in contemporary regulatory practice, and the government was badly burned when, in the 1990s, its Clipper Chip proposal was found to be technically flawed. *See* Sean Gallagher, *What the Government Should've Learned About Backdoors from the Clipper Chip*, ARS TECHNICA (Dec. 14, 2015, 3:05 PM), https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip [https://perma.cc/Q6X5-CQT5].

Instead, government officials insist that the problem—designing a lawful-access system that is scalable and secure—is solvable and that, with their impressive record of technological innovation, Silicon Valley's engineers simply need to try harder. For example, as FBI Director Wray has argued:

> We have the brightest minds doing and creating fantastic things. If we can develop driverless cars . . . if we can establish entire computer-generated virtual worlds . . . surely we should be able to design devices that both provide data security and permit lawful access with a court order.[75]

Scholars supporting the government's position have similarly insisted that technology companies solve the technical challenges inherent in third-party solutions, without explaining beyond bare outlines how companies are to go about doing so.[76] But the difficulty in building third-party access is not in the high-level approaches to "splitting keys" or putting keys in "escrow," but instead in the actual implementations that have to be used in the field and at scale. If there is to be a "Manhattan-like project" to create secure exceptional-access systems (as Hillary Clinton called for during the 2016 campaign),[77] it will have to focus on these tricky implementation issues.

Ultimately there's no guarantee that scalable and secure exceptional access is possible. It's no use arguing that, because Silicon Valley has done a bunch of amazing things, it should just "nerd harder" to do this other amazing thing;[78] the problems are fundamentally different. As critics of the government's position have acidly noted, the government's argument is akin to telling NASA, "Well, if we can put a man on the moon, well, surely we can put a man on the sun."[79]

Of course, that the problem is difficult doesn't mean (unlike landing on the sun) that it's impossible. The point is that any solution will require a massive amount

[75] Christopher Wray, Remarks at the Fordham University - FBI International Conference on Cyber Security (Jan. 9, 2018), https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation [https://perma.cc/HEG6-GXL8].

[76] *See, e.g.*, *Averting the Inherent Dangers*, *supra* note 4, at 1445 (describing, at a high level of generality, a "'split key' approach" by which manufacturers would create keys that could access encrypted devices and that the "keys would be 'split' and retained by two (or more) distinct entities: the manufacturer and a privacy rights organization"); Jaffer & Rosenthal, *supra* note 4, at 310–11 (similarly advocating for a "splitting keys" approach); Opderbeck, *supra* note 4, at 737 ("For encrypted data at rest, a reasonable approach could include a requirement that the service provider render technological assistance in retrieving plaintext pursuant to a valid court order. This could be accomplished by the provider through the use of public key encryption with a key escrow retained by the provider, or by any other reasonable means.").

[77] *See* Keith Wagstaff, *Could Hillary Clinton's Encryption "Manhattan Project" Work?*, NBC NEWS (Dec. 22, 2015, 12:21 PM), https://www.nbcnews.com/tech/security/could-hillary-clinton-s-encryption-manhattan-project-work-n484086 [https://perma.cc/D79X-6YYA].

[78] *See* Julian Sanchez (@normative), TWITTER (Jan. 29, 2016, 7:34 AM), https://twitter.com/normative/status/693049694457569281 [https://perma.cc/5UBX-U7BY] ("We all know their answer, right? Some variant on: Nerd harder! Love will find a way!").

[79] *See* Matt Blaze, *Last Week Tonight with John Oliver*, YOUTUBE (March 13, 2016), https://www.youtube.com/watch?v=zsjZ2r9Ygzw [https://perma.cc/B8MF-6TP3].

of research and development to which the government has so far not publicly contributed. Until the government develops the institutions that will incentivize and help Silicon Valley and the broader information-security community tackle this monumental technical challenge, its demands for exceptional access will remain the first step, not the last, to solving this problem.

2. "Going Dark" vs. "A Golden Age of Surveillance"

The government's argument that it is "going dark"—in the face of encryption and other technical impediments to surveillance—has not gone unchallenged. Peter Swire and Kenesa Ahmad have argued that, far from going dark, the government is enjoying "a golden age of surveillance."[80] Conceding that encryption may hamper government access to data in some circumstances, Swire and Ahmad argue that the net effect of new technology is to greatly facilitate government surveillance. They cite the many technologies that have in a few short decades created massive new troves of data for the government to access, from cell-phone location-tracking data to the masses of information held as emails, messages, and social-media logs.[81] In the years since Swire and Ahmad made their "golden age" argument, potential sources of surveillance data have only increased. The "Internet of Things" will create even more targets for government surveillance,[82] as has already occurred with always-on, always-listening "smart speakers" like the Amazon Echo.[83] And as virtual and augmented reality become more prominent, they will generate huge collections of data that may be useful to government investigators.[84] And no matter the source, a large proportion of data will always remain unencrypted, either because encryption would be technologically infeasible (as with the case of the metadata that routes internet traffic) or because the technology companies that hold that data would find it in their business interests to maintain access to that data (for example, to more effectively sell advertisements).[85]

[80] Swire & Ahmad, *supra* note 3, at 463.

[81] *Id.* at 466–70.

[82] DON'T PANIC, *supra* note 7, at 12–15; Pell, *supra* note 4.

[83] *See* Amy B. Wang, *Can Amazon Echo Help Solve a Murder? Police Will Soon Find Out.*, WASH. POST (Mar. 9, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/09/can-amazon-echo-help-solve-a-murder-police-will-soon-find-out/ [https://perma.cc/8QVH-LNAS]; *see also* Sarah Knapton, *Fridges and Washington Mahines Could Be Vital Witnesses in Murder Plots*, TELEGRAPH (Jan. 2, 2017), https://www.telegraph.co.uk/science/2017/01/02/fridges-washing-machines-could-vital-witnesses-murder-plots [https://perma.cc/4BRS-M9DM] (quoting a London police official who argued that "[w]ireless cameras within a device such as [the] fridge may record the movement of owners and suspects," that "[d]oorbells that connect directly to apps on a user's phone can show who has rung the door and the owner or others may then remotely, if they choose, to give controlled access to the premises while away from the property," and that "[a]ll these [activities] leave a log and a trace of activity").

[84] *See generally* Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051 (2018); Gilad Yadin, *Virtual Reality Surveillance*, 35 CARDOZO ARTS & ENT. L.J. 707 (2017).

[85] DON'T PANIC, *supra* note 7, at 3.

The "golden age" argument has drawn sharp critiques from the government. For example, law enforcement has argued that metadata will never replace the investigative or evidentiary value of actual content; metadata may be enough to place a suspect at the scene of the crime, but it's not enough to establish that the person actually pulled the trigger.[86] Law enforcement can also point to increased juror expectations for digital evidence: the "tech effect" by which jurors "significantly expect that prosecutors will use the advantages of modern science and technology to help meet their burden of proving guilt beyond a reasonable doubt."[87] The concern is that, as jurors come to recognize how much data is (theoretically) available to law enforcement, they will view prosecutorial cases more skeptically if they're not presented with all that data. This is a particular problem for state and local police departments, which may not have access to the same sophisticated techniques yet will be held to the same high standards by local jurors. For example, a study of jurors in a Michigan county found that nearly half "believe[d] the police should use DNA analysis in every case."[88] It's easy to imagine similar attitudes with respect to digital forensics.

But let's assume that the empirical premise of the golden-age argument is correct, and that the government has, on net, greater surveillance capabilities, and thus crime-fighting power, today than it did before the digital age, even taking encryption into account. What does that actually mean for the larger debate over whether the government *should* be able to access encrypted (or otherwise technologically inaccessible) data? The short answer is: very little. Indeed, whether the government is "going dark" or instead is enjoying a "golden age of surveillance" is, despite its centrality in both academic and popular discussion of the issue, largely orthogonal to the issues at stake.

Debates about whether the government is "going dark" or instead is enjoying a "golden age of surveillance" are, in the first instance, competing *descriptive* accounts over how much surveillance power the government currently enjoys. But the reason we spend so much time on this question is because it serves as a proxy for the fight people actually care about: whether the government, as a *normative* matter, has too much or not enough access to data. The reason for the proxy is that this normative question is hard to answer. In order to tally up the costs and benefits

[86] *See* NASEM ENCRYPTION REPORT, *supra* note 8, at 44 (noting that "information is not fungible" and that the "law enforcement community thus argues that it is much harder to convince a jury of criminal intent using metadata evidence than with content evidence"). The intelligence community has similarly stressed the importance of metadata. *See* Letter from the Office of the Director of National Intelligence, to Senator Ron Wyden 2 (May 5, 2016), *available at* https://www.wyden.senate.gov/imo/media/doc/ODNI%20Legal%20Review%20of%20Dont%20Panic%20Article.pdf [https://perma.cc/AM8J-35ZK].

[87] Donald E. Shelton et al., *A Study of Juror Expectations and Demands Concerning Scientific Evidence: Does the "CSI Effect" Exist?*, 9 VAND. J. ENT. & TECH. L. 331, 364 (2006).

[88] Donald E. Shelton et al., *An Indirect-Effects Model of Mediated Adjudication: The CSI Myth, the Tech Effect, and Metropolitan Jurors' Expectations for Scientific Evidence*, 12 VAND. J. ENT. & TECH. L. 1, 28–29 (2009).

of government surveillance, one would have to answer a number of difficult questions: To what extent does any particular technical impediment to government surveillance—encryption, offshoring, and so on—impede government investigations? When a government investigation is thwarted, how much does that harm society? And, conversely, what are the harms to society from increased government surveillance?

A common way to avoid these difficult questions is to rely on heuristics—rules of thumb—that simplify the analysis. An approach frequently used by even sophisticated commentators on both sides of the "going dark" debate is the status quo heuristic. This heuristic first picks some historical baseline of law-enforcement surveillance capabilities (or the mirror image, law-enforcement infringements on privacy) and criticizes the current state of affairs as diverging from that baseline. Both the government and its critics have operated from the status-quo baseline, though from opposite directions. For the government, the relevant baseline is recent history—specifically, right before companies like Apple and WhatsApp encrypted their products. From this baseline, the government's ability to surveil has diminished. For critics of government surveillance, the relevant baseline is the pre-digital age, before smartphones and social media vastly expanded the government's surveillance capabilities. From this baseline, the technological changes underlying the "going dark" problem are mere blips on the otherwise rocketing growth of the surveillance state.

But baseline arguments like these have two serious flaws. The first is the problem, which afflicts baseline arguments generally, that there may be no non-arbitrary way of picking the "right" baseline.[89] Yet the choice of baseline is crucial, often determining the outcome of the analysis. Here, the critical choice is between a pre-encryption baseline and a pre-digital-age baseline, and there's no reason why one is less of a legitimate status quo than is the other.

The second and more serious problem is that, even if one could non-arbitrarily pick a government-surveillance baseline, it's not clear why sticking to it would be normatively desirable. Just calling something a baseline doesn't by itself provide a reason to abide by it. One needs some other reason. Frequently this other reason is legal: for example, if the Fourth Amendment prohibits general warrants, or if the Wiretap Act imposes "super-warrant" requirements for wiretaps, the rule of law provides a normative reason to not deviate from the legal baseline—that is, what the law says. But *policy* baselines lack this sort of independent normative force; by assumption, the government has the legal ability to engage in some sort of surveillance, and the question is whether or not that surveillance is normatively desirable on the basis of social welfare.

Defenders of the status quo sometimes appeal to "balance," as in the balance between security and public safety on the one side and privacy and civil liberties on the other. The problem with the balance argument is that it is unsupportable and so

[89] *See generally* FARNSWORTH, *supra* note 14.

frequently begs the question. If by "balance" defenders of the status quo simply mean the state of affairs they want to preserve, then appeals to balance are circular: "we should stick to the status quo because it represents a balance between security and privacy" ends up meaning "we should stick to the status quo because it's the status quo." Alternatively, if balance is given some additional content, the arguments for why it has that content and why that content should matter are typically begged. For example, the word "balance" is often used to evoke stability. But this stability is more often assumed than demonstrated. The government's surveillance capabilities are always in flux and the stability that attends the description of those capabilities at a particular moment is often the result of taking a snapshot of a dynamic, rather than static, system.

More fundamentally, even if the current state of affairs represents some ongoing equilibrium, this fact only weakly supports the claim that the status quo is optimal or even just better than the alternative that is being argued against. At most it (weakly) suggests that, in light of the background conditions in effect at the time—the government's technological capabilities, the societal values placed on security and privacy, and so on—the status quo represented a local maximum (and even this requires the contestable assumption that social policy gets better over time). But change those conditions and all bets are off. For example, a critic of DNA testing could not convincingly argue that, simply because there was no DNA testing before the technology had been developed, the long-run "balance" should continue into the post-DNA-testing age.

Nor are the only background changes technological. Background changes in social values can also render the status quo inappropriate. Consider a situation in which society has to make a tradeoff between security and privacy. The optimal tradeoff will depend on the relative value society ascribes to these goods, and these values may change over time. The psychologist Steven Pinker has described how western society, including in the United States, has experienced "a rising abhorrence of violence, and of even the slightest trace of a mindset that might lead to it."[90] This has led to an increasing categorization of many once-common practices as morally reprehensible, from the overdue (sexual harassment and assault) to the silly (schoolyard dodgeball[91]). The more intolerant society becomes to violence and crime, and the more it categorizes certain activities that were once merely frowned upon as legitimate targets for state intervention (domestic violence is perhaps the most striking example over the past fifty years), the more society will demand

[90] STEVEN PINKER, THE BETTER ANGELS OF OUR NATURE: WHY VIOLENCE HAS DECLINED 388 (2011).

[91] *See, e.g.*, *Increasingly, Schools Move to Restrict Dodgeball*, N.Y. TIMES (May 6, 2001), http://www.nytimes.com/2001/05/06/us/increasingly-schools-move-to-restrict-dodgeball.html [https://perma.cc/ZZ2G-L7K8] (quoting a "curriculum specialist" who argues against dodgeball on the grounds that, "[w]ith Columbine and all the violence that we are having, we have to be very careful with how we teach our children").

increased security, even at the cost of privacy and other competing values. And once the government moves to satisfy these increased public safety expectations, the increased size and expense of the public-safety bureaucracy in turn drive greater public expectations of public safety, leading to a feedback loop of growing expectations.[92]

By the same token, changes in attitudes toward privacy could also require a recalibration in one direction or the other. Perhaps Facebook CEO Mark Zuckerberg was right when, in 2010, he questioned whether privacy was still a relevant "social norm."[93] Echoing this observation, Bernard Harcourt has powerfully written how we are often the greatest threat to our own privacy, as we "give ourselves up in a mad frenzy of disclosure."[94] Changed norms may explain why Congress reauthorized, even in a post-Snowden environment, a far-reaching national-security surveillance program that warrantlessly collects information (albeit incidentally) on potentially millions of Americans. On the other hand, perhaps we are due for a correction in the direction of less surveillance and more privacy, especially in the wake of Russian interference in the 2016 election and increasing concerns that too much of our data is available for manipulation.

Nothing I've said should be interpreted as an argument against *incrementalism*, the position that policy change should happen gradually, especially under conditions of complexity, disagreement over goals, and incomplete information.[95] Incrementalism can even justify a decision strategy that gives some of the same results as one dependent on the status quo fallacy. Imagine that law enforcement has a surveillance capacity *s*, that it has had this capacity for some time, and that this capacity is generally regarded as acceptable (even if suboptimal) from an overall social-welfare perspective. Now imagine some exogenous shock—for example, technological and social change—that dramatically and rapidly increases the amount of data individuals produce and that enhances law enforcement surveillance capabilities such that the new *s'* is far greater than *s*.

The problem confronting society is to decide whether society is better off at *s'* versus *s*. Incrementalism tells us the status quo is the best source of information for evaluating alternatives.[96] But if the alternative is radically different than the status

[92] *See* FRANK P. HARVEY, THE HOMELAND SECURITY DILEMMA 1, 16–17 (2008).

[93] Bobbie Johnson, *Privacy Is No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [https://perma.cc/L3A3-GEZL].

[94] BERNARD HARCOURT, EXPOSED 18 (2015).

[95] For classic statements of incrementalism and its benefits, see, for example, JAMES C. SCOTT, SEEING LIKE A STATE 345 (1998); ROBERT A. DAHL & CHARLES E. LINDBLOM, POLITICS, ECONOMICS, AND WELFARE 82–85 (1953); Charles E. Lindblom, *Still Muddling, Not Yet Through*, 39 PUB. AD. REV. 517 (1979); Lindblom, *supra* note 71, at 84–88, 88 n.9 (1959). For applications of incrementalism in the legal literature, see, for example, CASS R. SUNSTEIN, ONE CASE AT A TIME (1999); Colin S. Diver, *Policymaking Paradigms in Administrative Law*, 95 HARV. L. REV. 393 (1981); Ozan O. Varol, *Temporary Constitutions*, 102 CAL. L. REV. 409, 421–27 (2014).

[96] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 535–37 (2011).

quo, this comparison may not be available. Thus, from a decision-strategy standpoint, incrementalism may counsel for a correction, by which society brings *s'* back to *s* (or close to) and then applies incremental analysis to see if a move toward the full *s'* is justified on welfarist grounds. But note the role of the status quo in this analysis; there's no assumption that it's superior or encodes a beneficial "balance." Rather, the status quo is simply the best source of information we have and so any deviations from it should be gradual, not disruptive.

If the status-quo heuristic won't work as a guide for policymaking, what should take its place? The problem with the status-quo approach is that it's an insufficient proxy for what we actually care about: not whether the government has more or less surveillance powers than it did in the past, but rather whether the government, right now, has *too much* or *too little* such powers. As difficult as this inquiry might be, there is no substitute for a substantive inquiry into the optimal level of government surveillance.

One way to answer the question is to adopt a precautionary approach: pick some value and reject any policies that harm that value, no matter how marginally. In the context of government surveillance, Cass Sunstein has identified two applications of this approach: "Cheneyism" and "Snowdenism". Cheneyism focuses on security threats and argues that almost any policy is justified if it lowers the risk of those security threats. Snowdenism, by contrast, focuses on the threats of government surveillance and argues that no surveillance should be conducted if it even marginally increases the risk of government surveillance abuses.[97] Although Cheneyism and Snowdenism are theoretical positions—in practice, no one (probably not even Dick Cheney nor Edward Snowden themselves) actually subscribe to them in their strongest forms—they are useful labels because they identify the two main poles of precautionary thinking about government surveillance.

There are two problems with positions like Cheneyism and Snowdenism. First, they are not just based on different empirical judgments about the world—for example, judgments about the likelihood of terrorist attacks or of government surveillance abuses—but also about different *values*. Cheneyists might simply value physical safety more than do Snowdenists, and vice versa for privacy. It's not clear whether there are any "neutral principles" available for choosing between such incommensurable values.

Second, Cheneyism and Snowdenism, like all applications of the precautionary principle, ignore the fact that optimizing for one value might impose large costs on competing values. It's not like Cheneyists don't care at all about preventing government abuse or Snowdenists completely discount the role government surveillance plays in ensuring public safety and national security. The problem with

[97] Cass R. Sunstein, *Beyond Cheneyism and Snowdenism*, 83 U. CHI. L. REV. 271, 271–73 (2016).

each approach is that, by focusing on a single value, each uses excessively "narrow viewscreens, focusing on a subset of the risks at stake rather than the whole."[98]

Instead of Cheneyism or Snowdenism, what is required is *risk management*: recognizing that "risks of many kinds are on both sides of the ledger, and the task is to manage the full set, not to focus on one or a few."[99] As Sunstein recognizes, however, traditional risk management—in the form of some sort of cost-benefit analysis—is difficult to deploy where the costs and benefits of the policy are difficult to quantify, either because they are uncertain or because they require monetizing seemingly unmonetizable values (how do you put a price on privacy or a human life?).[100]

These are indeed difficult challenges, but, as the rest of the Article argues, we can make progress on them. We have no choice.

B. Focus on Imperfect Solutions: The Case of Lawful Hacking

Although wicked problems cannot be solved, they can be managed. But to do so, we must focus our attention on imperfect solutions, while at the same time being sensitive to their drawbacks.

The most important such proposal, advocated for by an increasing proportion of the information-security community, is for the government to expand its "lawful hacking" of devices.[101] As is apparent to anyone whose computer has ever been infected by a virus or whose smartphone incessantly pesters about "critical security" system updates, electronic devices are shot through with software vulnerabilities. These vulnerabilities allow unauthorized third parties,[102] whether criminal hackers or government investigators, to overcome whatever security measures are in place and access user data. Lawful hacking proposals differ in their details; some envision the government purchasing hacking tools from third parties (as the FBI did when it accessed the iPhone of one of the San Bernardino terrorists),[103]

[98] *Id.* at 277.

[99] *Id.* at 283.

[100] *Id.* at 284–85.

[101] The most comprehensive proposal for lawful hacking is Bellovin et al., *supra* note 35; see also Susan Hennessey, *Lawful Hacking and the Case for a Strategic Approach to Going Dark*, *in* BROOKINGS BIG IDEAS FOR AMERICA 241 (Michael E. O'Hanlon ed., 2017); Kerr & Schneier, *supra* note 4, at 1009–12. For a more critical perspective, especially in the context of extra-territorial searches, see Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1095–99 (2017).

[102] Frequently, the term "attacker" is used to describe any third party who accesses a device or system without authorization. I avoid that term here because I don't want to want to imply that unauthorized access is ipso facto normatively problematic. Thus, the FBI investigator who exploits a vulnerability on a criminal's phone is an "attacker" from the perspective of the criminal's interest in information security, though the FBI agent may be doing precisely what we want them to do.

[103] More recently, a company called Grayshift developed "GrayKey," hardware which purportedly can unlock all versions of iPhones. *See* Annie Palmer, *The $15,000 Device That Can Unlock ANY iPhone: US Police Forces Buying "GrayKey" Box to Crack into Encrypted Phones—but Experts Warn It Could Be Exploited by Hackers,* DAILY MAIL (Apr. 17, 2018, 11:32 EDT),

while others would have the government invest in in-house computer hacking expertise[104] (essentially an FBI-housed domestic analogue to the NSA's Tailored Access Operations team, which is responsible for breaking into foreign computer systems[105]).

The biggest argument in favor of lawful hacking is that it takes advantage of pre-existing vulnerabilities in computer and communications systems. Unlike exceptional-access mandates, lawful hacking does not require providers to make changes to their systems that might introduce even more security flaws. Thus, lawful hacking can, at least at a first approximation, improve law enforcement's capabilities without further degrading the public's already precarious information security.

At the same time, lawful hacking has a number of limitations, many of which flow from the wicked nature of the problem of government access to encrypted data.

First, and as its proponents recognize, lawful hacking will only be a partial solution, especially outside the context of high-value national security or foreign intelligence operations. There is no guarantee that a particular device or application has a vulnerability that would allow access. Even if such a vulnerability exists, the government may not be able to discover it. And even if the government knows that a third party has knowledge of a suitable vulnerability (or, better yet, a ready-made tool that would allow government access), the vulnerability may be too expensive for the government to acquire, especially if different investigative targets require different vulnerabilities or the targets upgrade their systems, rendering existing vulnerabilities no longer effective.[106] Moreover, the vulnerability may be so sensitive that the government would only be willing to use it for its highest-value targets,[107] especially if it would have to disclose the technical details of the vulnerability in a follow-on prosecution.[108]

http://www.dailymail.co.uk/sciencetech/article-5613597/Police-claim-unlock-iPhone-using-mysterious-10-000-GrayKey-box.html [https://perma.cc/33G7-5SP9].

[104] *See, e.g.*, Susan Landau, *What Law Enforcement Really Needs for Investigations in the Digital Age*, LAWFARE (Feb. 12, 2018, 11:00 AM), https://www.lawfareblog.com/what-law-enforcement-really-needs-investigations-digital-age [https://perma.cc/43C6-SKUU].

[105] *See* Kim Zetter, *NSA Hacker Chief Explains How to Keep Him out of Your System*, WIRED (Jan. 28, 2016, 9:23 AM), https://www.wired.com/2016/01/nsa-hacker-chief-explains-how-to-keep-him-out-of-your-system [https://perma.cc/TJ7U-SR94].

[106] Jaffer & Rosenthal, *supra* note 4, at 314.

[107] Paul Ohm, *The Investigative Dynamics of the Use of Malware by Law Enforcement*, 26 WM. & MARY BILL RTS. J. 303, 314–15, 331–32 (2017).

[108] Courts have split on whether the government can assert a "law-enforcement privilege" against disclosure of technical details of lawful hacking. *See* Jennifer Granick & Riana Pfefferkorn, *Government Hacking: Evidence and Vulnerability Disclosure in Court*, CTR. FOR INTERNET & SOC'Y AT STAN. L. SCH. (May 23, 2017, 10:48 AM), http://cyberlaw.stanford.edu/blog/2017/05/government-hacking-evidence-and-vulnerability-disclosure-court [https://perma.cc/NH46-NDQZ].

These problems are compounded at the state and local levels.[109] As noted above,[110] the tendency to think about law enforcement policy in terms of the federal government obscures the fact that the vast majority of crime, and the vast majority of law enforcement investigations, occur within the jurisdiction of the nearly 18,000 state, county, and local police departments and law-enforcement agencies across the country.[111] Your local police department—or even your state attorney general's office—is unlikely to have the expertise or resources to hack devices that have been secured by the world's most brilliant computer engineers working for the world's largest companies.[112] Thus, even if lawful hacking satisfies the feds' needs, it might leave the vast bulk of the problem unsolved.[113]

The second problem with widespread lawful hacking is that it could have a serious unintended consequence: it could, in certain cases, *decrease* device security. When the government learns of a vulnerability in software or hardware, it has a choice: it can either disclose that vulnerability to the product vendor in hopes that the vendor will fix the vulnerability, or it can keep the vulnerability secret and use the knowledge for its own purposes—for example, to hack devices that have the vulnerability. The decision whether to disclose vulnerabilities is a complex one, and it has led the government to adopt an interagency process by which vulnerabilities are assessed and disclosure decisions are made.[114] A full analysis of this process is complex,[115] but it's safe to say that increased reliance on lawful hacking would clearly incentivize the government to horde, rather than disclose, vulnerabilities.[116]

[109] *See* Kerr & Schneier, *supra* note 4, at 1015.

[110] *See supra* note 35 and accompanying text.

[111] DUREN BANKS ET AL., U.S. DEP'T OF JUSTICE, NATIONAL SOURCES OF LAW ENFORCEMENT EMPLOYMENT DATA 3 (2016), https://www.bjs.gov/content/pub/pdf/nsleed.pdf [https://perma.cc/BV55-Q8YD].

[112] MANHATTAN DA REPORT, *supra* note 5, at 4–5.

[113] The federal government, through the FBI's National Domestic Communications Assistance Center (NDCAC), provides state and local law-enforcement agencies with technical advice (but not research and development or operational assistance). *See* NAT'L DOMESTIC COMMC'NS ASSISTANCE CTR., https://ndcac.fbi.gov/ [https://perma.cc/9Z5S-G2EV] (last visited June 6, 2019). It is conceivable that NDCAC could expand and play a more direct role in state and local investigations involving encrypted data and devices. However, this would require a dramatic increase in resources and would unlikely address lower-priority investigations, for which the government would be unwilling to use a lawful-hacking technique.

[114] *See* VULNERABILITIES EQUITIES POLICY AND PROCESS FOR THE UNITED STATES GOVERNMENT (Nov. 15, 2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF [https://perma.cc/KJ7N-MMN2].

[115] *See generally* Tristan Caulfield et al., *The U.S. Vulnerabilities Equities Process: An Economic Perspective, Decision and Game Theory for Security*, *in* DECISION AND GAME THEORY FOR SECURITY 131 (Stefan Rass et al. eds., 2017); Stephanie K. Pell & James Finocchiaro, *The Ethical Imperative for a Vulnerability Equities Process and How the Common Vulnerability Scoring System Can Aid That Process*, 49 CONN. L. REV. 1549 (2017).

[116] RIANA PFEFFERKORN, CTR. FOR INTERNET & SOC'Y AT STAN. L. SCH., SECURITY RISKS OF GOVERNMENT HACKING 3–5 (2018).

Thus, advocates of lawful hacking should not to try to eat their cake and have it too. For example, after the FBI gave up trying to force Apple to help unlock the San Bernardino iPhone and instead used a third-party tool to gain access, Apple's lawyers reportedly considered ways to force the FBI to disclose information about how the tool worked,[117] many called on the FBI to voluntarily disclose the information,[118] and several news organizations sued unsuccessfully to find out the name of the vendor.[119] Some lawful-hacking supporters argue that the government should have a "default obligation to report" vulnerabilities, "actively reporting and working to fix even those vulnerabilities that it uses" for surveillance, on the theory that there is always a "lead time" between when vulnerabilities are reported and when they're patched, and that new vulnerabilities will always be found "at a rate that exceeds the rate at which they are repaired."[120] But there is no guarantee that this will be the case, especially if the government makes lawful hacking the centerpiece of its strategy to access otherwise technically inaccessible data.

Finally, lawful hacking will exacerbate the already wide divide between the government on the one side and the technology industry and information-security community on the other side. Lawful hacking incentivizes each side to be suspicious of the other: the technology industry will (rightly) think that the government is secretly trying to undermine the security of its products, and the government will (rightly) think that the technology industry is not a partner but rather a target. Consider how the technology industry responded when in 2017 WikiLeaks released documents purporting to show that the CIA had "acquired an array of cyberweapons that could be used to break into Apple and Android smartphones, Windows computers, automotive computer systems, and even smart televisions to conduct surveillance on unwitting users."[121] The CIA was angrily accused of "stockpiling vulnerabilities" and undermining security for users around the world.[122]

[117] Paresh Dave, *Apple Wants the FBI to Reveal How It Hacked the San Bernardino Killer's iPhone*, L.A. TIMES (Mar. 29, 2016, 8:12 PM), http://www.latimes.com/business/technology/la-fi-tn-apple-next-steps-20160330-story.html [https://perma.cc/28E4-67NK].

[118] Sara Sorcher & Malena Carollo, *Influencers: FBI Should Disclose San Bernardino iPhone Security Hole to Apple*, CHRISTIAN SCI. MONITOR (Mar. 24, 2016), https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0324/Influencers-FBI-should-disclose-San-Bernardino-iPhone-security-hole-to-Apple [https://perma.cc/N88F-6693].

[119] *See* Associated Press v. FBI, 265 F. Supp. 3d 82 (D.D.C. 2017).

[120] *See* Bellovin et al., *supra* note 35, at 55.

[121] Vindu Goel & Nick Wingfield, *WikiLeaks Reignites Tensions Between Silicon Valley and Spy Agencies*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/technology/wikileaks-silicon-valley-spy-agencies.html [https://perma.cc/ZRX5-6NX7]

[122] *Id.* (internal quotation marks omitted); *see also* Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT (May 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack [https://perma.cc/LE5K-CXJX].

Exacerbating the "suit-hoodie"[123] divide between the government and Silicon Valley will only make it harder to solve not just the problem of law-enforcement access to encrypted data but cybersecurity issues more generally.[124]

In pointing out these drawbacks I do not mean to suggest that lawful hacking is an inappropriate answer—at least in some cases—to the problem of law-enforcement access to encrypted data. In particular, lawful hacking will remain indispensable to investigations into criminal activity on the "dark web."[125] It will also be an important tool where suspects use products or services that are outside the scope of any exceptional-access mandates (for example, one of the many internationally produced secure messaging services). Rather, the point is that the best we can often do is to put forward partial proposals and focus on minimizing their flaws, in the hope that, flaws and all, they will nevertheless represent an incremental improvement over where things stand today.

C. Invest in Knowledge Production[126]

At the core of the encryption debate lie several factual questions: To what extent does encryption stymie government investigations? What level of access does the government want technology companies to provide, and across what platforms and systems? Most importantly, to what extent would providing such access degrade information security? These are of course not the only relevant questions, and some important additional questions are about values, not facts: Should we make it easier for the government to engage in surveillance? Assuming that government access will necessarily degrade information security by some amount, how much is too much? But we can't make meaningful progress on the value questions until we get our facts straight.

Congress could do much to help generate the answers we need. It could use a combination of carrots (increased funding) and sticks (legislative mandates) to require federal, state, and local agencies to keep detailed statistics on situations in which encryption impeded government investigations. In the wake of reports that the FBI seriously overestimated the number of encrypted devices it could not access,[127] laws requiring more accurate reporting are in order. Congress could also

[123] Amy Zegart, *Policymakers Are from Mars, Tech Company Engineers Are from Venus*, LAWFARE (June 6, 2016, 9:54 AM), https://www.lawfareblog.com/policymakers-are-mars-tech-company-engineers-are-venus [https://perma.cc/43Y6-VLBN].

[124] *See, e.g.*, Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 522–24 (2017) (describing botnet takedowns as an example of successful public-private cybersecurity cooperation).

[125] *See* Ghappour, *supra* note 101, at 1095–99.

[126] This and portions of the next section are closely adapted from Alan Z. Rozenshtein, Mayank Varia & Charles Wright, *How Congress Can De-Escalate the Second Crypto War: Fund Research and Broker a Crypto Armistice*, LAWFARE (June 5, 2018, 9:00 AM), https://www.lawfareblog.com/how-congress-can-de-escalate-second-crypto-war-fund-research-and-broker-crypto-armistice [https://perma.cc/BV2D-UW7L]. I am grateful to Mayank and Charles for helping me develop these ideas.

[127] *See* Barrett, *supra* note 28.

require agencies to keep data on how the government responded to encryption (for example, by dropping the investigation, using different investigative techniques, or defeating the encryption, whether through its own lawful hacking or the purchase of third-party tools), and it could require agencies to specify and prioritize what capabilities they need.

Congress could also directly fund research into whether secure exceptional-access systems are possible. Perhaps stung by the failure of the government-developed Clipper Chip during the 1990s, the government has studiously avoided putting forward any concrete proposals of its own, instead arguing that only the technology community is capable of the relevant research. But this undersells the government's role. From the beginning of the Internet—which, after all, started as a Defense Department project—to the present day, the government has played a key role in technological innovation, and there's no reason why this situation should be any different. Indeed, to use FBI Director Wray's own reference to autonomous vehicles,[128] the government-sponsored DARPA Grand Challenges during the 2000s stimulated much of the foundational work in this field.

There are several avenues by which Congress could invest in relevant knowledge generation. Agencies that fund basic science research could administer new challenges to develop viable options and to understand fundamental limitations. Exchange programs could send technologists from the private sector and the academy into the government to help think through the technological and policy issues around exceptional access. Eventually, cryptographic standards organizations could hold a competition to evaluate the security of exceptional access systems, just as occurred with the now broadly supported Advanced Encryption Standard[129] and Cryptographic Hash Algorithm.[130]

None of this will result in viable exceptional-access systems overnight. It is important to recognize that, whether with driverless cars or realistic virtual reality (Wray's examples of Silicon Valley innovation), it took years—sometimes decades—to develop the technologies, which even now remain works in progress. Secure exceptional-access systems may similarly be years away from viability. That doesn't mean we should skimp on the necessary research and development, just that we should have a realistic timetable in mind and start as early as possible.

D. Improve Relationships Between the Government and the Technology Community

Underlying many approaches to managing wicked problems is the need to foster a more collaborative, rather than combative, relationship between the various stakeholders. This is important for at least two reasons. First, because information

[128] *See* Wray, *supra* note 75 and accompanying text.

[129] *AES Development*, NIST, https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development [https://perma.cc/8CFV-VBDG] (last visited June 6, 2019).

[130] *SHA-3 Project*, NIST, https://csrc.nist.gov/projects/hash-functions/sha-3-project [https://perma.cc/4LWE-K7FW] (last visited June 6, 2019).

and expertise are diffuse, the best answers rely on cooperation. Second, because wicked problems involve tradeoffs among legitimate values, compromise is necessary.

Unfortunately, the relationship between the government and the technology sector is at a nadir. One of the most pernicious features of debates on government surveillance is the pronounced us-versus-them tribalism. This has a host of unhelpful effects when it comes to collaborative problem solving, but a singularly toxic one is each side's lack of respect for the other's highest values. For example, the government frequently downplays the extent to which the information-security community—in both the private and academic sectors—feels an overriding duty to protect the information of its users. Conversely, when surveillance skeptics dismiss government arguments as based on exaggerations about the "Four Horsemen of the Infopocalypse" (terrorists, drug dealers, pedophiles, and organized criminals), they ignore law enforcement's strongly felt duty to protect society against these threats. As the psychologist Philip Tetlock has explained, blindness to the other side's values can lead to "taboo trade-offs," in which one side trivializes the other side's values, leading to failed negotiation, even worsened inter-group relationships, and a corresponding digging in by each side into its positions.

Fortunately, such conflicts can be repaired. Tetlock's research suggests that where "taboo trade-offs" are reframed as "tragic trade-offs"—ones that forthrightly recognize that legitimate values on all sides have come into conflict—and where the decision-maker "linger[s] over a tragic trade-off . . . emphasiz[ing] the gravity of the issues at stake," the moral outrage that taboo trade-offs spark can be defused.[131] In the best case, the process of working together can help participants forge a new, shared group identity—a "community of interest" that transcends participants' pre-existing group interests and gets them to think in terms of what is good for all members.[132]

When thinking about techniques to improve or repair relationships, it is useful to divide them into two categories: first, those that affirmatively improve relationship, and, second, those that remove existing impediments to healthy relationships.

In the first category, the support for research advocated above would certainly help. If security researchers try to develop secure third-party access systems—even if they ultimately decide that such systems are infeasible—they will naturally develop some appreciation for the government's legitimate need to access encrypted data.

[131] Philip E. Tetlock, *Thinking the Unthinkable: Sacred Values and Taboo Cognitions*, 7 TRENDS IN COGNITIVE SCI. 320, 322 (2003).

[132] *See* Nancy Roberts, *Wicked Problems and Network Approaches to Resolution*, 1 INT'L PUB. MGMT. REV. 1, 14 (2000); *cf.* Hill, *supra* note 43, at 529 ("Consensus is arguably the best guide for what society should encourage firms to do . . . ."). The importance of negotiation "in good faith" and where the parties "remain open to learning" is a key feature of other forms of consensus-based social-policy formation, as in much of contemporary public-law litigation. Charles F. Sabel & William H. Simon, *Destabilization Rights: How Public Law Litigation Succeeds*, 117 HARV. L. REV. 1015, 1068 (2004).

Conversely, if law enforcement feels that the technology community is trying in good faith to solve their problem, they will be more inclined to believe when told that a particular solution won't work. And to the extent that government-funded research brings together individuals from the technology community and the government—whether through research grants, innovation challenges, or exchange programs—the personal relationship will help break down the us-versus-them group identities that make cooperation that much harder. Familiarity breeds friendliness more than contempt.

In the second category, the government should stop trying to force a resolution to the problem—particularly one that favors law enforcement—given the lack of even a partial consensus that a satisfactory technological solution exists. No amount of collaboration will do the trick if the technology community believes that the government is poised to force insecure or unvetted "backdoors" into encrypted products and services.

Of all the ways that government attempts to force the technological community to comply can backfire, the best example is the FBI's 2016 attempt to use a court order to force Apple to modify the operating system of the iPhone of one of the San Bernardino terrorists. There are many reasons why the government's strategy was, at least in hindsight, ill-advised. First, it is not clear whether the law the government relied on, the All Writs Act,[133] actually authorized the court to issue the government's desired order.[134] Second, courts have limited technical expertise and are thus ill-suited to making the technical judgments that are necessary to decide whether a government demand for technical assistance is appropriate. Third, courts, which must decide on the individual government request before them, are ill-placed to consider the system-wide effects of their decisions. While the government emphasized that its request was limited to one phone, Apple and others correctly pointed out that, were Apple to build the capability that the government wanted, it would open the floodgates to similar assistance requests from law-enforcement agencies across the country. In addition, such dynamics would encourage forum shopping by the government, which could go from court to court until it found one willing to impose an assistance order, which would then effectively apply nationwide.

But the biggest drawback of having the courts settle the encryption issue is the effect that litigation has on the participants. The adversarial nature of litigation encourages each side to take maximalist positions and rhetorically demonize the

[133] *See* Judiciary Act of 1789, ch. 20, § 14, 1 Stat. 73, 81–82 (codified as amended at 28 U.S.C. § 1651).

[134] This was the main point of contention between the government and Apple in the litigation before the court. A different court had earlier held that the All Writs Act did not grant it power to issue a far less burdensome iPhone-unlocking assistance order to Apple. *See In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court, 149 F. Supp. 3d 341, 376 (E.D.N.Y. 2016); *see also* Rozenshtein, *supra* note 32, at 125–28.

other, rather than work together. In the iPhone litigation, the government characterized Apple's use of unbreakable encryption as a "marketing decision to engineer its products so that the government cannot search them, even with a warrant,"[135] while Apple accused the government of trying to violate its constitutional rights.[136] And in a high-profile statement that Apple CEO Tim Cook published on the company's home page, he accused the FBI of "undermin[ing] the very freedoms and liberty our government is meant to protect."[137]

Just as importantly, the litigation also polarized the larger technology community. The litigation attracted over a dozen amicus briefs on Apple's side, covering virtually every sector of the technology community: Apple's Silicon Valley competitors; leading civil-society organizations like the American Civil Liberties Union and the Electronic Frontier Foundation; and dozens of technologists, researchers, and cryptographers.[138] This was predictable; group tensions rise—and the possibility for cooperation correspondingly lowers—when one group feels that its core values are under attack. And in Silicon Valley, where encryption has come to symbolize Silicon Valley's commitment to its users' information security and its opposition to government surveillance, few moves by the government would so obviously inflame as a top-down effort to restrict encryption, whether through litigation, legislation, or regulation.

Ultimately, the government will be better served if it recognizes that, until there is an (at minimum partial) consensus among technologists that secure third-party access is possible, no top-down mandate will be possible. Until then, the government may be best off supporting an armistice that takes design mandates off the table.

A 2018 bipartisan bill in the House of Representatives provides one model of what a crypto-armistice might look like. The "Secure Data Act of 2018," would prohibit any regulations or court orders (other than those already permitted under the law) that would require a company "to design or alter the security functions in its product or service to allow the surveillance of any user of such product or service, or to allow the physical search of such product" by the government.[139] By removing the specter of exceptional-access design mandates, the bill might actually make it

[135] Government's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 1, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. 5:16-cm-00010-SP (C.D. Cal. Feb. 25, 2016).

[136] *See* Apple Inc's [sic] Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 32–34, *In re* Search of an Apple iPhone.

[137] *See* Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), https://www.apple.com/customer-letter [https://perma.cc/RD7V-UCNG].

[138] For a full list of the amicus filings and letters supporting Apple, see Press Release, Apple Inc., Amicus Briefs in Support of Apple (Mar. 2, 2016), https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple [https://perma.cc/C2Q8-7F5C].

[139] Secure Data Act of 2018, H.R. 5823, 115th Cong. § 2(b) (2018).

more likely that research on secure exceptional access goes forward (whether or not that was the intention of the bill's sponsors).

To be clear, the bill has serious flaws. It unnecessarily goes far beyond encryption, prohibiting design modifications that may pose no security threats. It is permanent, when instead a time-limited bill (for example with a sunset provision after some number of years) might better ensure that the issue remains on Congress's radar. And it misses an opportunity to fund and otherwise support research. But it is nevertheless a useful thought experiment as to how a pause in hostilities between the government and technology sector may be in everybody's interest—and in particular why the government may want to support such an armistice.

CONCLUSION

The point of this Article is not to advance a particular technological or policy solution to the problem of law-enforcement access to encrypted data. It is possible that no adequate solution exists. Instead, this Article has attempted to explain why the problem is both real and difficult, and to suggest conceptual approaches and institutional designs that, while they may not be able to solve the problem in the near future, can continue the conversation along a constructive path. That is of course well short of a solution, but, when it comes to wicked problems, it is often the best one.