Hacked and Leaked:
Legal Issues Arising From the Use of Unlawfully Obtained Digital Evidence in International Criminal Cases

Lindsay Freeman*

Abstract

Digital open source investigations—the use of publicly available information on the internet for intelligence, leads, or evidence—are becoming an increasingly critical part of international criminal investigations. While the definition of open source information is simple, there are several categories of information that fall into a gray area between private and public—in particular, the growing amount of illegally hacked and leaked information on the web. Online leaks, whether the result of hacking or whistleblowing, fit the definition of open source information. Yet, there is something inherently different about information in the public domain that was not *intended* to be public. The dissemination of incriminating information unlawfully obtained by a third party creates a complex situation in which, on one hand, the illegal method of acquisition should not be rewarded, while at the same time, the illegal acts that are exposed in the documents should not go unpunished. The public interest can cut both ways. What are the rules and practical implications of using this information in criminal investigations or, more importantly, criminal trials? By examining specific hacks and leaks, describing their relevance to international criminal cases, and identifying the applicable evidentiary rules, this Article explores the challenges to admitting hacked and leaked digital documents into evidence.

* Lindsay Freeman is the Law and Policy Director of the Human Rights Center at UC Berkeley School of Law and a consultant for the Office of the Prosecutor of the International Criminal Court. The views expressed in this Article are her own. The author thanks Alexa Koenig and Rebecca Wexler for their valuable insights and feedback, as well as the UCLA *JILFA* team for their enthusiasm, professionalism, and editorial support.

Table of Contents

Introduction

The definition of open source information is simple. It is information that is publicly available: information that can be legally accessed by any member of the public through observation, request, or purchase.[1] Closed source information, in contrast, is information that is proprietary. But what happens when private information acquired through illegal or prohibited means is placed in the public domain? what are the rules and practical implications of using this information in criminal investigations or, more importantly, criminal trials? Going further, how might such evidence be evaluated in international criminal cases in which government and military documents often play a critical role in establishing linkage and criminal responsibility for high-level perpetrators?

1. Off. of the U.N. High Comm'r for Hum. Rts. [OHCHR] & Hum. Rts. Ctr, Berkeley Protocol on Digital Open Source Investigations 3 (2020), https://www.ohchr.org/Documents/Publications/OHCHR_BerkeleyProtocol.pdf [https://perma.cc/N4S5-F5WV] [hereinafter Berkeley Protocol].

The open and anonymous nature of the internet makes it the perfect conduit for distributing large numbers of documents to a public audience without attribution. Far from late-night rendezvous in underground parking lots, the internet provides a considerably easier platform for anonymously leaking information than was available to Daniel Ellsberg, who leaked the Pentagon Papers, or Mark Felt, the source known as Deep Throat who leaked information on the Watergate scandal.[2] The internet also provides a lower-risk alternative for stealing documents. The web is a platform through which hackers can break into computer networks from the comfort of their own homes rather than assume the risk of breaking into buildings like the burglars who were caught breaking into the Watergate complex.

For clarity, hacked information is information acquired by an outsider who gains unauthorized access to it, whereas leaked information is information obtained by an insider who has authorized access to it, but shares it in an unauthorized manner.[3] Most forms of hacking are illegal,[4] but there are a few exceptions, such as penetration testing, which are not.[5] Similarly, most leaking is illegal,[6] but exceptions do exist for whistleblowers in a number of jurisdictions.[7] The term "online leak" is used more generally in this Article to refer to any public dissemination

2. Daniel Ellsberg is the whistleblower who released the Pentagon Papers. *Daniel Ellsberg Biography*, Biography (Sept. 30, 2019), https://www.biography.com/activist/daniel-ellsberg [https://perma.cc/42YJ-ZH7S]. Mark Felt was the source known as "Deep Throat" in the Watergate scandal. Bob Woodward, The Secret Man: The Story of Watergate's Deep Throat (2005); John O'Connor & Mark Felt, Mark Felt: The Man Who Brought Down the White House (2006).

3. Elad Ben-Meir, *The Very Fine Line Between Hacking and Whistleblowing*, Cyberint (Sept. 18, 2016), https://blog.cyberint.com/the-very-fine-line-between-hacking-and-whistleblowing [https://perma.cc/4ZTH-DZEA].

4. *See* Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030; *Hacking Laws and Punishments*, FindLaw (May 2, 2019), https://criminal.findlaw.com/criminal-charges/hacking-laws-and-punishments.html [https://perma.cc/587D-ZTGK].

5. Scott Nicholson, *When Is Hacking Illegal and Legal?*, Bridewell Consulting Blog (Feb. 12, 2019), https://www.bridewellconsulting.com/when-is-hacking-illegal-and-legal [https://perma.cc/CT9D-7TBX].

6. Conor Friedersdorf, *All Leaks Are Illegal, but Some Leaks Are More Illegal Than Others*, The Atl. (June 13, 2013), https://www.theatlantic.com/politics/archive/2013/06/all-leaks-are-illegal-but-some-leaks-are-more-illegal-than-others/276828 [https://perma.cc/YB3G-FX8T].

7. *See* Whistleblower Protection Act of 1989, 5 U.S.C. § 1201; *Whistleblower Protections*, U.S. Consumer Prod. Safety Comm'n, https://www.cpsc.gov/About-CPSC/Inspector-General/Whistleblower-Protection-Act-WPA [https://perma.cc/Y75Z-9GB6]. In Canada, the Public Service Disclosure Protection Act shelters government employees, who generally receive far greater protection against retaliation for whistleblowing, compared to those in the private sector. *See Whistleblower Protection Laws in Canada*, Leckler & Assocs. Blog (Nov. 7, 2019), https://leckerslaw.com/whistleblower [https://perma.cc/ZN5Q-W8W6].

of private information on the internet, no matter the source or method of acquisition.

With the rise of professional intermediaries to facilitate leak dissemination,[8] websites dedicated to leak publication,[9] and openness advocates defending the practice of leaking,[10] the Digital Age has ushered in new possibilities for hackers and whistleblowers alike. With greater opportunity, the number and size of online leaks has grown considerably over time, with many now described in terabytes.[11] Several of these leaks are infamous—from the Sony Pictures,[12] Democratic National Committee,[13] Ashley Madison,[14] and Equifax[15] hacks to the

8. For example, journalists and lawyers can play an important role acting as intermediaries to protect leakers.

9. For example, WikiLeaks, GlobaLeaks, PubLeaks, Distributed Denial of Secrets, and The Intercept.

10. *See, e.g.*, Rainey Reitman & Kurt Opsahl, *Wikileaks-Hosted "Most Wanted Leaks" Reflects the Transparency Priorities of Public Contributors*, Elec. Frontier Found. (July 1, 2020), https://www.eff.org/deeplinks/2020/07/wikileaks-hosted-most-wanted-leaks-reflects-transparency-priorities-public [https://perma.cc/73Y3-S6KA]; *see also* Sarah Oh, *Advocating for Openness: Nine Ways Civil Society Groups Have Mobilized to Defend Internet Freedom*, CIMA Digit. Rep. (Nov. 15, 2017), https://www.cima.ned.org/publication/advocating-openness-nine-ways-civil-society-groups-mobilized-defend-internet-freedom [https://perma.cc/67MP-YCE6]; *Sign-On: Advocates Seek Stronger Protections and Confidentiality for Intel Community Whistleblowers*, GAO (Nov. 12, 2019), https://whistleblower.org/letter/sign-on-advocates-seek-stronger-protections-and-confidentality-for-intel-community-whistleblowers [https://perma.cc/4UHE-DTYF].

11. The Panama Papers leak is said to be 2.6 terabytes, which is over double the roughly 1 terabyte of data leaked by Edward Snowden. Tom Metcalfe, *Panama Papers: Just How Big Is the World's Biggest Data Leak?*, LiveScience (Apr. 8, 2016), https://www.livescience.com/54348-how-big-is-panama-papers-leak.html [https://perma.cc/5NF4-5SRY]. Similarly, the scale of a Chinese hack of a U.S. military defense company similar was described as "many terabytes." Sasha Goldstein, *Chinese Hackers Stole F-35 Fighter Jet Blueprints in Pentagon Hack, Edward Snowden Documents Claim*, N.Y. Daily News (Jan. 20, 2015, 9:22 AM), https://www.nydailynews.com/news/national/snowden-chinese-hackers-stole-f-35-fighter-jet-blueprints-article-1.2084888 [https://perma.cc/KPZ8-STEY]. This website shows a visualization of growth of online leaks over the last decade: *World's Biggest Data Breaches & Hacks*, Info. Is Beautiful (Jan. 2021), https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks [https://perma.cc/38X6-FR38].

12. *See generally* Clare Sullivan, *The 2014 Sony Hack and the Role of International Law*, 8 J. Nat'l Sec. L. & Pol'y 437 (2016).

13. David E. Sanger & Eric Schmitt, *Spy Agency Consensus Grows That Russia Hacked D.N.C.*, N.Y. Times (July 26, 2016), https://www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html [https://perma.cc/JTM6-9RMG].

14. Steve Mansfield-Devine (ed.), *The Ashley Madison Affair*, 2015 Network Sec. 8 (2015).

15. McKay Smith & Garrett Mulrain, *Equi-Failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. Nat'l Sec. L. & Pol'y 549 (2018).

Iraq War Logs,[16] Guantanamo files,[17] NSA files,[18] and Panama Papers.[19] In many cases, the information contained in leaked documents has been used in various fact-finding processes.[20] In particular, leaked information from government insiders has played a central role in establishing the truth and holding individuals accountable for abuses of power and violations of the law that would otherwise have gone unpunished.

While international criminal prosecutions rely on a diverse body of evidence, some types of evidence prove more valuable than others. Traditionally, government and military documents have played a key role in establishing difficult-to-prove elements of crimes such as the perpetrator's knowledge or intent.[21] For example, when it comes to proving the link between a high-level military commander and the actions of his troops on the ground, private military communications play a crucial role.[22] Similarly, internal communiqués are often the only direct evidence of an organizational "plan or policy," a contextual

16. *Baghdad War Diaries*, WikiLeaks, https://wikileaks.org/irq.

17. *WikiLeaks Reveals Secret Files on All Guantánamo Prisoners*, WikiLeaks, https://wikileaks.org/gitmo [https://perma.cc/2A45-KPMA].

18. Ewen Macaskill & Gabriel Dance, *NSA Files Decoded: What the Revelations Mean for You*, The Guardian (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [https://perma.cc/HZE4-F5L3].

19. The Int'l Consortium of Investigative Journalists, Offshore Leaks Database, https://offshoreleaks.icij.org/about:blank [https://perma.cc/N4ZW-KS5F] [hereinafter ICIJ Database].

20. Various factfinding processes include international and national criminal investigations; United Nations factfinding missions and commissions in inquiry; human rights investigations by nongovernmental organizations and civil society; investigative journalism; and transitional justice, peace, and reconciliation processes.

21. In Justice Robert H. Jackson's opening statement before the International Military Tribunal at Nuremberg, he explained that the counts in the Indictment could all be proved with books and records, since the Germans were meticulous record keepers. *See* Robert H. Jackson, *Opening Statement Before the Military Tribunal*, Robert H. Jackson Ctr. (Nov. 21, 1945), https://www.roberthjackson.org/speech-and-writing/opening-statement-before-the-international-military-tribunal/about:blank [https://perma.cc/H7NL-N76E].

22. As scholars Gabriele Chlevickaite and Barbora Hola explain, "[Insiders] are often able to bring to light aspects of the crimes that otherwise would be difficult, if not impossible, to establish, such as the internal structure of an organisation the accused was part of or his/her role in the planning of the crimes." Gabriele Chlevickaite & Barbora Hola, *Empirical Study of Insider Witnesses' Assessments at the International Criminal Court*, 16 Int'l Crim. L. Rev. 673, 674 (2016). In the Katanga and Ngudjolo judgments, the Trial Chamber noted that "it would . . . have been desirable to hear the testimonies of some of the commanders who played a key role before the attack, during combat and thereafter." Prosecutor v. Katanga, ICC-01/04-01/07-3436tENG, Judgment Pursuant to Article 74 of the Statute, ¶ 63 (Mar. 7, 2014); Prosecutor v. Ngudjolo, ICC-01/04-02/12-3-tENG, Judgment Pursuant to Article 74 of the Statute, ¶ 119 (Dec. 18, 2012) [hereinafter Ngudjolo Judgment].

element of crimes against humanity that can be challenging to prove beyond reasonable doubt based on circumstantial evidence alone.[23]

While a few academics have written about the admissibility of illicitly obtained evidence in international courts,[24] existing scholarship has only scratched the surface of the legal challenges ahead. This Article explores the legal issues raised by the use of hacked and leaked digital evidence in international criminal investigations and prosecutions. Parts I and II present case studies of past hacks and leaks to establish the variety of possible scenarios, and to illustrate the potential evidentiary value of such material. Part III describes the applicable rules governing relevance and admissibility of evidence in international criminal cases, with a particular focus on the rules of the International Criminal Court (ICC or Court). Part IV applies the law to factual scenarios stemming from the case studies discussed earlier and assesses how the rules might impact the admissibility of hacked or leaked documents at trial. Finally, this Article concludes with some recommendations to international criminal justice practitioners on how to handle hacked and leaked digital evidence based on current rules. Due to the newness of the issue and the notable lack of jurisprudence, this Article does not provide concrete answers to all of the questions posed. Rather, it provides a framework for thinking through relevant legal challenges that are bound to arise in many of the forthcoming cases before the ICC and other international criminal law (ICL) courts and tribunals.

23. ICC, Elements of Crimes, art. 7 (2011). In the reasoning for the acquittal of Gbagbo and Blé Goudé, the judges explained that the prosecution had not demonstrated a "common plan" to keep Gbagbo in power, the prosecution did not substantiate the alleged existence of a policy aimed at attacking civilians, and the prosecution did not show that the crimes as alleged in the charges were committed in accordance with or pursuant to the policy of a state of organization. Prosecutor v. Gbagbo, ICC-02/11-01/15-1263, Reasons for Oral Decision of 15 January 2019, ¶ 28 (July 16, 2019); *see also* Abraham Kouassi, *Judges Issue Written Reasons for Acquittal in Gbagbo Case; What Bensouda Can Do Now*, Int'l Just. Monitor (July 16, 2019), https://www.ijmonitor.org/2019/07/icc-judges-issue-written-reasons-for-acquittal-in-the-gbagbo-case-what-bensouda-can-do-now [https://perma.cc/ZM29-7VCJ].

24. *See, e.g.*, Petra Viebig, Illicitly Obtained Evidence at the International Criminal Court (2016); Cherie Blair & Ema Vidak Gojković, *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence*, 33 ICSID Rev.–Foreign Inv. L.J. 235 (2018); Lejla Zilić & Semir Mujezinović, *Admissibility of Illegally Obtained Evidence Before the International Criminal Court—Hypothetical Case*, 24 Annals Fac. L.U. Zenica 191 (2019); Shayan Ahmed Khan, *The Issues of Admissibility Pertaining to Circumstantial, Contested, Classified, & Illicitly Obtained Evidence in the International Court of Justice*, 1 Rsch. Soc'y Int'l L. Rev. 105 (2017); Isabella Bogunovich, *I Object! The Use of WikiLeaks Evidence in International Courts and Tribunals*, Perth Int'l L.J. (Aug. 21, 2016), https://www.perthilj.com/blog/2019/2/19/i-object-the-use-of-wikileaks-evidence-in-international-courts-and-tribunals [https://perma.cc/P33C-MEDJ].

I. Super Leaks and Their Consequences

A hooded man in a torn garment stands atop a cardboard box, his hands outstretched. Electrical wire is tied to his fingers and wrapped around his neck like a noose.[25] This haunting image, recognizable to many, is titled *The Hooded Man.* The photo was taken by Sergeant Ivan Frederick in Iraq's Abu Ghraib prison in 2003 and leaked to journalists by Joe Darby in 2004 along with other photographs depicting Iraqi detainees tortured at the hands of United States soldiers.[26] The leak led to legal action against some of those involved. TIME Magazine reported that "eleven low-ranking soldiers of the 372nd Military Police Company, a unit of reservists that guarded the prison, were convicted on criminal charges for the abuses at Abu Ghraib."[27] In addition, "the prison commander in Iraq at the time, Janis Karpinski, faced administrative action and was demoted from the rank of general," while "others were discharged from duty and convicted in court martials."[28] This leak also fundamentally altered public perception of the U.S. military and the war in Iraq.[29] It took the American Civil Liberties Union twelve years of litigation to get a court to require that the Pentagon release additional photographic documentation of the Abu Ghraib detention center,[30] revealing how extremely difficult it can be to acquire this type of information through traditional legal channels.

Among the many online leaks in recent history, three in particular have garnered significant public attention because of their size, import, and consequence. Referred to by some as "super leaks,"[31] this Part examines (1) the Iraq and Afghan war logs leaked by Chelsea Manning through Julian Assange's WikiLeaks Platform in October 2010;[32] (2)

25. Ivan Frederick, *The Hooded Man*, TIME: 100 Photos, http://100photos.time.com/photos/sergeant-ivan-frederick-hooded-man [https://perma.cc/NF44-HUH3].

26. Anjani Trivedi, *The Abu Ghraib Prison Pictures—Joe Darby (2004)*, TIME (June 10, 2013), https://world.time.com/2013/06/10/10-notorious-leakers-and-how-they-fared/slide/abu-ghraib-photo-leak [https://perma.cc/27FY-32FG].

27. *Id.*

28. *Id.*

29. Paul Gronke, Darius Rejali & Peter Miller, *No, Americans Aren't 'Fine With Torture.' They Strongly Reject It.*, Wash. Post (Dec. 11, 2014), https://www.washingtonpost.com/posteverything/wp/2014/12/11/no-americans-arent-fine-with-torture-they-strongly-reject-it [https://perma.cc/6MEG-4C6B].

30. Eliza Relman, *Pentagon Releases 198 Abuse Photos in Long-Running Lawsuit. What They Don't Show Is a Bigger Story*, ACLU Blog (Feb. 5, 2016), https://www.aclu.org/blog/national-security/torture/pentagon-releases-198-abuse-photos-long-running-lawsuit-what-they [https://perma.cc/S3GE-YRBU].

31. The Panama Papers (Bungalow Media + Entertainment 2018).

32. *See generally* David Leigh & Luke Harding, WikiLeaks: Inside Julian Assange's War on Secrecy (2011); WikiLeaks, The WikiLeaks Files: The World According

the NSA files leaked by Edward Snowden through Guardian journalist Glenn Greenwald and documentarian Lara Poitras in June 2013;[33] and (3) the Panama Papers leaked by "John Doe" through German journalists Frederik Obermaier and Bastian Obermayer in partnership with an international consortium of journalists in April 2016.[34] Each of these super leaks led to radical, real-world results—from the launch of national and international inquiries, to the resignations of CEOs and Heads of State, to lawsuits and criminal convictions.

While super leaks often lead to criminal charges against the leakers themselves,[35] as was the case with Manning and Snowden, this type of legal action is not the focus of this Article. Rather, this Article examines how the content of these leaked documents can be—and in some cases already has been—used as evidence against the original document-owners or third parties for other types of violations of international and national laws.

A. Iraq and Afghan War Logs

According to its website, WikiLeaks released the largest classified military leak in history on February 22, 2010.[36] The 391,832 reports, referred to as the "Iraq War Logs," cover U.S. military activities during the war in Iraq over a five-year period. In July of that same year, WikiLeaks released another set of documents, now known as the "Afghan War Diaries" or "Afghan War Logs," which contained 91,000 reports documenting the war in Afghanistan.[37] The source of these

---

to US Empire (2016); Daniel Domscheit-Berg & Tina Klopp, Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website (Jefferson Chase trans., 2011); The N.Y. Times, Open Secrets: WikiLeaks, War, and American Diplomacy (2011); Chelsea Manning, Untitled Chelsea Manning Memoir (forthcoming 2021).

33. *See generally* Edward Snowden, Permanent Record (2019); Glenn Greenwald, No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State (2014); Barton Gellman, Dark Mirror: Edward Snowden and the American Surveillance State (2020); Citizenfour (HBO Films 2014).

34. *See generally* Frederik Obermaier & Bastian Obermayer, The Panama Papers: Breaking the Story of How the Rich & Powerful Hide Their Money (2016); Jake Bernstein, Secrecy World: Inside the Panama Papers Investigation of Illicit Money Networks and the Global Elite (2017); The Panama Papers (Bungalow Media + Entertainment 2018).

35. For example, the U.S. government brought criminal charges against Daniel Ellsberg, Chelsea Manning, and Edward Snowden, to name a few. *See* Stephen P. Mulligan & Jennifer K. Elsea, Congressional Research Service, Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information 17–18, 21–22, 24 (Mar. 7, 2017).

36. *Baghdad War Diaries*, *supra* note 16.

37. *Afghan War Diary, 2004–2010*, WikiLeaks (July 25, 2010), https://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010 [https://perma.cc/44VJ-43PN].

reports was a former U.S. soldier, Chelsea Manning, who was convicted by court-martial for disclosing a total of nearly 750,000 classified or sensitive military documents in violation of the Espionage Act.[38] Interestingly, the Manning court-martial was one of the earliest criminal trials to test the admissibility of digital open source evidence, such as social media posts from Twitter as well as the WikiLeaks archives themselves.[39] By bringing criminal charges against Manning and using the leaked documents as evidence, the U.S. government implicitly validated the authenticity of the documents, creating a foundation for their use in subsequent legal proceedings.

In addition to the case against Manning, the Iraq and Afghan war logs have been used in numerous investigations into the conduct of elected government officials and politicians, members of the military at all ranks, and private military contractors. For example, the U.S. Senate investigation of Central Intelligence Agency (CIA) tactics used in the "War on Terror" resulted in a scathing report detailing many cases of torture that cite to leaked reports.[40] The logs contained details of hundreds of incidents of U.S. troops directly causing civilian casualties.[41] This information has been particularly valuable for investigators because, prior to 2008, there was a lack of reliable data on civilian conflict-related deaths.[42] The leaked documents not only exposed violations of the law, such as the unjustified killing of civilians by members of the military, but also revealed that those at the top of the chain of command knew about these abuses.[43] They comprised evidence of the crimes and evidence of the cover up.

38. Chelsea E. Manning, *The Years Since I Was Jailed for Releasing the 'War Diaries' Have Been a Rollercoaster*, The Guardian (May 27, 2015), https://www.theguardian.com/commentisfree/2015/may/27/anniversary-chelsea-manning-arrest-war-diaries [https://perma.cc/NE7X-KJQS].

39. *See* Ian Simpson, *WikiLeaks Soldier's Court-Martial Wrestles Online Evidence Rules*, Reuters (June 25, 2013), https://www.reuters.com/article/us-usa-wikileaks-manning-evidence/wikileaks-soldiers-court-martial-wrestles-online-evidence-rules-idUSBRE95O1J920130625 [https://perma.cc/2Y8L-K8BX].

40. Greg Miller, Adam Goldman, & Julie Tate, S*enate Report on CIA Program Details Brutality, Dishonesty*, Wash. Post (Dec. 9, 2014), https://www.washingtonpost.com/world/national-security/senate-report-on-cia-program-details-brutality-dishonesty/2014/12/09/1075c726-7f0e-11e4-9f38-95a187e4c1f7_story.html [https://perma.cc/YDV2-2EB5].

41. Beth Goldberg, *Wikileaks Releases 'Afghan War Diary'*, Inst. for Pol'y Stud. (July 26, 2010), https://ips-dc.org/wikileaks_releases_kabul_war_diary [https://perma.cc/78C7-KJS6].

42. Situation in the Islamic Republic of Afg., ICC-02/17-7-Red, Public Redacted Version of "Request for Authorisation of an Investigation Pursuant to Article 15", 20 November 2017, ICC-02/17-7-Conf-Exp, ¶ 32 (Nov. 20, 2017).

43. *WikiLeaks: Iraq War Logs 'Reveal Truth About Conflict'*, BBC (Oct. 23, 2010),

These leaked documents also serve as evidence of international crimes, including violations of the United Nations Convention Against Torture and violations of international humanitarian law, including grave breaches of the Geneva Conventions of 1949. Under the principle of universal jurisdiction, Spanish judge Baltasar Garzón filed criminal charges against six former officials of the U.S. government in the George W. Bush administration.[44] This is one of several universal jurisdiction cases filed in Europe based on investigations conducted by national war crimes prosecutors and initiated in large part because of the WikiLeaks disclosures.[45] In addition, litigants have been successful in filing related cases at the European Court of Human Rights against countries—such as Lithuania and Romania—that were complicit in the CIA's illegal torture and rendition programs.[46]

As of publication, the Office of the Prosecutor (OTP) at the ICC has an open investigation into the "situation in Afghanistan"[47] and has previously conducted a preliminary examination into the "situation in Iraq."[48] Both situations[49] are defined within the temporal scope covered by the WikiLeaks logs, with the Afghanistan investigation specifically looking into the CIA's conduct. While the prosecution's request to open an investigation into Afghanistan does not mention WikiLeaks explicitly, it does explain that it "examined US Government documents, memoranda, decisions, internal reports, detainee profiles, combatant status review tribunal summaries, letters and e-mails and used such material as important documentary sources" in its determination as to whether there was a reasonable basis to believe that crimes within the jurisdiction of the ICC had occurred.[50] The immense amount of data in

https://www.bbc.com/news/world-middle-east-11612731 [https://perma.cc/AZ22-UQC9].

44. *Torture in Guantanamo: Spain Closes Investigations into "Bush Six"*, ECCHR, https://www.ecchr.eu/en/case/torture-in-guantanamo-spain-closes-investigations-into-bush-six [https://perma.cc/6ZNU-3Y9X].

45. *Universal Jurisdiction: Accountability for U.S. Torture*, Ctr. for Const. Rts. (Oct. 26, 2007), https://ccrjustice.org/universal-jurisdiction-accountability-us-torture [https://perma.cc/EX5M-FDT3].

46. *ACLU Statement on CIA Torture Program Rulings From European Court of Human Rights*, ACLU (May 31, 2018), https://www.aclu.org/press-releases/aclu-statement-cia-torture-program-rulings-european-court-human-rights [https://perma.cc/2WKL-Y8MC].

47. *Situation in the Islamic Republic of Afghanistan*, ICC, https://www.icc-cpi.int/afghanistan [https://perma.cc/5TCG-SUGH].

48. *Preliminary Examination: Iraq/UK*, ICC, https://www.icc-cpi.int/iraq [https://perma.cc/6CLT-KVGF].

49. "Situation" is the term used by the ICC to refer to incidents occurring within a specific geographic and temporal period.

50. Situation in the Islamic Republic of Afghanistan, ICC-02-17-7-Red, Public Redacted Version of "Request for Authorisation of an Investigation Pursuant to Article 15", 20

the Iraq and Afghan war logs are still available on WikiLeaks and will certainly be relevant to these ICC cases.[51] However, with increasing hostility from the United States against the ICC since the Prosecutor's request to open the Afghanistan investigation,[52] it is expected that, if a case gets to trial, the admissibility of WikiLeaks evidence will be vigorously challenged in this forum.

B. NSA Files

In the summer of June 2013, the world learned the name of Edward Snowden, a National Security Agency (NSA) contractor and source behind the largest leak in history at that time. The Iraq and Afghan war logs pale in comparison to the 1.7 million classified documents disclosed by Snowden, which exposed U.S. surveillance programs like PRISM, XKEYSCORE, and STELLARWIND.[53] The U.S. government

November 2017, ICC-02/17-7-Conf-Exp, ¶ 36 (Nov. 20, 2017).

51. Even WikiLeaks has noted its relevance to the ICC investigation with this Tweet: WikiLeaks (@wikileaks), Twitter (Mar. 5, 2020, 4:59 AM), https://twitter.com/wikileaks/status/1235550531495645184?lang=en [https://perma.cc/8ELM-UR6R]; *see also US Faces War-Crimes Investigations Following an International Criminal Court Ruling*, Morning Star, https://morningstaronline.co.uk/article/w/us-faces-war-crimes-investigations-following-an-international-criminal-court-ruling [https://perma.cc/6XKQ-UEKS]; *International Criminal Court Rules U.S. To Be Investigated for Afghanistan War Crimes*, People's World, https://www.peoplesworld.org/article/international-criminal-court-rules-u-s-to-be-investigated-for-afghanistan-war-crimes [https://perma.cc/U45U-Y3J5]; Linda Pearson, *WikiLeaks Shows How US, Britain Rigged the ICC to Avoid Justice for Iraq*, Green Left (July 8, 2016), https://www.greenleft.org.au/content/wikileaks-shows-how-us-britain-rigged-icc-avoid-justice-iraq [https://perma.cc/Y8BG-WRZE].

52. Afua Hirsch, *WikiLeaks Cables Lay Bare US Hostility to the International Criminal Court*, The Guardian (Dec. 17, 2010), https://www.theguardian.com/law/2010/dec/17/wikileaks-us-international-criminal-court [https://perma.cc/G8SH-RJGA]. On June 11, 2020, the Trump Administration issued an Executive Order authorizing sanctions against persons associated with the International Criminal Court (ICC). *See* Exec. Order No. 13,928, 85 Fed. Reg. 36,139 (June 11, 2020). On September 2, 2020, the Administration announced sanctions against two officials of the ICC: Prosecutor Fatou Bensouda and Phakoso Mochochoko, Head of the Jurisdiction, Complementarity and Cooperation (JCCD) in the Office of the Prosecutor (OTP). *Blocking Property of Certain Persons Associated With the International Criminal Court Designations*, U.S. Dep't of Treasury (Sept. 2, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200902 [https://perma.cc/92MQ-JS5U]. Bensouda and Mochochoko are now on the Treasury's specially designated nationals list. *See Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. Dep't of Treasury (Jan. 8, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists [https://perma.cc/8GJW-4TLJ].

53. *See* Morgan Marquis-Boire, Glenn Greenwald & Micah Lee, *XKEYSCORE: NSA's Google for the World's Private Communications*, The Intercept (July 1, 2015), https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications [https://perma.cc/5TZ4-69MX]; Timothy B. Lee, *Here's Everything We Know About PRISM to Date*, Wash. Post (June 12, 2013), https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date [https://perma.cc/5DCS-J3Z4]; Robert

continued its pattern of pursuing the leaker, characterizing Snowden as a traitor and bringing charges against him under the Espionage Act.[54] Furthermore, the Obama Administration asserted that Snowden was not a whistleblower, for which there are well-established processes and protections, but a traitor who put American national security at risk.[55] In bringing these charges, the U.S. government once again implicitly recognized the authenticity of the documents, even without acknowledging their validity directly.

In addition to what the documents revealed about the NSA's mass surveillance programs, the leaked files also exposed participation by partners like the United Kingdom's Government Communications Headquarters (GCHQ). The involvement of the NSA's British counterpart established jurisdiction of the European Court of Human Rights and allowed dozens of human rights organizations to bring a lawsuit against GCHQ for illegal mass surveillance—violating the rights to privacy and freedom of expression under international human rights law.[56] *Big Brother Watch and Others v. the United Kingdom* was lodged as a result of Snowden's revelations about the extent of the U.S. surveillance programs and intelligence sharing between the United States and the United Kingdom. Specifically, the case concerned "complaints by journalists, individuals and rights organisations about three different surveillance regimes: (1) the bulk interception of communications; (2) intelligence sharing with foreign governments; and (3) the obtaining of communications data from communications service providers."[57] In 2018, the European Court of Human Rights issued a

O'Harrow Jr. & Ellen Nakashima, *President's Surveillance Program Worked With Private Sector to Collect Data After Sept. 11, 2001*, Wash. Post (June 27, 2013), https://www.washingtonpost.com/investigations/presidents-surveillance-program-worked-with-private-sector-to-collect-data-after-sept-11-2001/2013/06/27/2c7a7e74-df57-11e2-b2d4-ea6d8f477a01_story.html [https://perma.cc/MP3A-7WP8].

54. *See* Whistleblower Protection Act, *supra* note 7; *The Whistleblower Protection Program*, U.S. Dep't of Labor, https://www.whistleblowers.gov [https://perma.cc/3D22-YTQD].

55. Nick Gass, *White House: Snowden 'Is Not a Whistleblower'*, Politico (Sept. 14, 2016), https://www.politico.com/story/2016/09/edward-snowden-not-whistleblower-earnest-228163 [https://perma.cc/E5VN-923K].

56. *Mass Surveillance Challenge Proceeds to Europe's Highest Human Rights Court*, Amnesty Int'l (Feb. 5, 2016), https://www.amnesty.org/en/latest/news/2019/02/mass-surveillance-challenge-proceeds-to-europes-highest-human-rights-court [https://perma.cc/7VS4-TVVY]; *see also* Scarlet Kim & Patrick Toomey, *What a European Court Ruling Means for Mass Spying Around the World*, ACLU (Sept. 24, 2018), https://www.aclu.org/blog/national-security/privacy-and-surveillance/what-european-court-ruling-means-mass-spying-around [https://perma.cc/66DT-CCUL].

57. *Factsheet—Mass Surveillance*, Eur. Ct. H.R. (Oct. 2020), https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf [https://perma.cc/6QRZ-H9AP].

landmark decision determining that the surveillance programs revealed by Snowden's leaked documents violated the rights to privacy and freedom of expression.[58]

While the European Court of Human Rights does not oversee criminal cases and, therefore, applies a lower evidentiary threshold, *Big Brother* provides a prime example of the use of leaked documents as evidence against an entity implicated in them rather than against the leaker. While nonbinding, the case law of the European Court of Human Rights can be relied on in ICC judgments pursuant to Article 21(1)(b) of the Rome Statute.[59]

The content of the Snowden documents can be used by the ICC as intelligence or lead information. The documents reveal U.S. military intelligence tactics, which may help inform the operational security strategy and witness protection measures instituted by the OTP during investigations. This information is particularly relevant for any investigations challenged by the United States.[60] Additionally, the documents provide insight into the type of information that the NSA and GCHQ have collected and stored on their citizens, the citizens of other countries, and the officials of other countries. For example, the documents revealed that the NSA had tapped the phone of German chancellor Angela Merkel.[61] The information collected as part of these mass surveillance programs may also be relevant to ongoing ICC investigations, and the NSA files could provide guidance on what to request from State Parties like the UK.

C. Panama Papers

In April 2016, the International Consortium of Investigative Journalists (ICIJ) released the Panama Papers in an open and searchable

58. Kim & Toomey, *supra* note 56.

59. Article 21(1)(b) of the Rome Statute states that, in addition to the Court's founding documents, judges should apply, where appropriate, rules of international law. In the only two ICC cases to date addressing the internationally recognized human right to privacy in the in the context Article 69(7), the Court relied on jurisprudence of the European Court of Human Rights to determine what qualifies as such a right. *See* Prosecutor v. Bemba, ICC-01/05-01/13-1854, Decision on Requests to Exclude Western Union Documents and Other Evidence Pursuant to Article 69(7), ¶¶ 28–30 (Apr. 29, 2016); Prosecutor v. Bemba, ICC-01/05-01/13-1855, Decision on Requests to Exclude Dutch Intercepts and Call Data Records, ¶¶ 9–11 (Apr. 29, 2016).

60. *See* Elizabeth Evenson, *US Official Threatens International Criminal Court—Again*, Hum. Rts. Watch (May 22, 2020), https://www.hrw.org/news/2020/05/22/us-official-threatens-international-criminal-court-again [https://perma.cc/JJ9F-M92Z].

61. *Snowden NSA: Germany to Investigate Merkel 'Phone Tap'*, BBC (June 4, 2014), https://www.bbc.com/news/world-europe-27695634 [https://perma.cc/ZG9J-HRZE].

internet database.[62] Over double the size of the NSA files, the 2.6 terabytes of data make the Panama Papers the largest leak in history as of this writing.[63] The leak contained a trove of internal communications, business records, and contracts from the Panamanian law firm Mossack Fonseca, a company that specialized in offshore accounts and tax havens with a high-profile list of clients. Going by the computer screenname "John Doe,"[64] an anonymous individual reached out to journalists Obermaier and Obermayer who had been covering stories related to offshore banking. Doe asked if they were interested in information on global corruption and, after some back and forth, the two parties opened a channel for data sharing.[65] Once Obermaier and Obermayer began receiving the data, they quickly realized the newsworthiness of the material and the public interest in publishing it. As the data continued to flow, they also recognized that a two-man team did not have the capacity to review all the documents. Thus, they reached out to the ICIJ, which brought together journalists from all over the world to review the documents and pull out the stories of greatest interest to their home countries. At a time when news outlets were struggling financially due to increasing digitization and information access, the ICIJ created a new and innovative model of collaboration for handling large amounts of data. By pooling resources, these journalists were able to structure the leaked documents in a database that has since become open and accessible to the public. Further, uniting an international group of journalists provided the requisite language skills and country-specific knowledge to properly interpret the data.

The Panama Papers are distinguishable from the Iraq and Afghan war logs and NSA files for a few reasons. First, the documents were taken from a private commercial entity rather than a government entity. In addition, the documents were authenticated, not through the implied admission of the custodian, but through the comparison of the leaked documents with verified documents from the same firm. Finally, the source of the documents and means by which they were obtained remain unknown, at least to the general public. Thus, it is unclear whether Doe

62. ICIJ Database, *supra* note 19.

63. Victor L. Hou et al., *U.S. Criminal Prosecution Based on Panama Papers Hack Raises Novel Legal Issues*, Cleary Cybersecurity & Priv. Watch (June 26, 2020), https://www.clearyenforcementwatch.com/2019/01/u-s-criminal-prosecution-based-on-panama-papers-hack-raises-novel-legal-issues [https://perma.cc/25NL-SUBS].

64. *See John Doe's Manifesto, Panama Papers: The Secrets of Dirty Money*, Süddeutsche Zeitung, https://panamapapers.sueddeutsche.de/articles/572c897a5632a39742ed34ef [https://perma.cc/RG8N-H7HG].

65. Obermaier & Obermayer, *supra* note 34, at 16–27.

is an insider who worked for Mossack Fonseca and blew the whistle or an outsider who hacked into Mossack Fonseca's private network.

The Panama Papers' exposure of global crime and corruption led to varying levels of accountability for high profile individuals, such as close associates of Russian President Vladimir Putin.[66] Stories derived from the leaked documents and ensuing public pressure led to the resignation of the prime minister of Iceland,[67] a $10 million fine and a ten-year prison sentence for the prime minister of Pakistan,[68] calls for resignation of UK prime minister David Cameron and establishment of new transparency measures in British parliament,[69] the impeachment of the president of Brazil and corruption charges against the opposition party,[70] resignations from Spain's Minister of Tourism, Industry, and Energy,[71] Chile's head of Transparency International,[72] FIFA's

66. *Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption*, ICIJ (Apr. 3, 2016), https://www.icij.org/investigations/panama-papers/20160403-panama-papers-global-overview [https://perma.cc/X3VN-TTYP]; Stella Roque, *Panama Papers: The World Reacts*, OCCRP, https://www.occrp.org/en/panamapapers/reactions [https://perma.cc/G65S-Y5FA].

67. *See* Steven Erlanger, Stephen Castle, & Rick Gladstone, *Iceland's Prime Minister Steps Down Amid Panama Papers Scandal*, N.Y. Times (Apr. 5, 2016), https://www.nytimes.com/2016/04/06/world/europe/panama-papers-iceland.html [https://perma.cc/HZ3L-XPML]; Ryan Chittum, *Iceland Prime Minister Tenders Resignation Following Panama Papers Revelations*, ICIJ (Apr. 5, 2016), https://www.icij.org/investigations/panama-papers/20160405-iceland-pm-resignation [https://perma.cc/NHB5-FGYX].

68. Scilla Alecci, *Former Pakistan PM Sharif Sentenced to 10 Years Over Panama Papers*, ICIJ (July 6, 2018), https://www.icij.org/investigations/panama-papers/former-pakistan-pm-sharif-sentenced-to-10-years-over-panama-papers [https://perma.cc/SY86-PX5V]; Fergus Shiel, *Former Pakistan Prime Minister Sentenced to Imprisonment Again on Corruption Charges*, ICIJ (Dec. 26, 2018), https://www.icij.org/investigations/panama-papers/former-pakistan-prime-minister-sentenced-to-imprisonment-again-on-corruption-charges [https://perma.cc/P2EN-DX6B].

69. *See* Martha M. Hamilton, *British PM Announces New Transparency Measures Following Panama Papers Revelations*, ICIJ (Apr. 11, 2016), https://www.icij.org/investigations/panama-papers/20160411-cameron-parliament-reform [https://perma.cc/JN59-9W8T]; Rowena Mason, *David Cameron's Terrible Week Ends With Calls for Resignation Over Panama Papers*, The Guardian (Apr. 8, 2016), https://www.theguardian.com/news/2016/apr/08/david-cameron-panama-papers-offshore-fund-resignation-calls [https://perma.cc/7CDQ-ML6J].

70. *See* Clarice Silber, *Panama Papers Lob 'Atomic Bomb' on Brazil's Political Class*, McClatchy DC Bureau (Apr. 13, 2016), https://www.mcclatchydc.com/news/nation-world/national/economy/article71594327.html [https://perma.cc/7UKM-7ZCC].

71. *See* Raphael Minder, *Spain's Industry Minister Steps Down Over Panama Papers Revelations*, N.Y. Times (Apr. 15, 2016), https://www.nytimes.com/2016/04/16/world/europe/panama-papers-spain.html [https://perma.cc/EEJ4-Q4AM].

72. *See* Gram Slattery, *Chile's Head of Transparency International Resigns After 'Panama Papers'*, Reuters (Apr. 4, 2016), https://www.reuters.com/article/panama-tax-chile-idUSL2N1771Z1 [https://perma.cc/9SPL-JAH8].

ethics judges,[73] and the resignation of the CEO of Hypobank in Australia,[74] whose banks were subsequently raided. In the United States, the New York Department of Financial Services asked financial institutions named in the documents to produce communications between their branches and Mossack Fonseca and later fined Mega International Commercial Bank of Taiwan $180 million for violating anti–money laundering laws.[75] On December 4, 2018, the U.S. Attorney's Office for the Southern District of New York unsealed an indictment against four individuals for tax fraud and money laundering based on the Panama Papers.[76]

As the OTP builds its financial investigation capacity,[77] it is probable that leaked corporate documents and bank records in general—and the Panama Papers in particular—will prove useful in their investigative work, both for building cases and tracing assets.[78] Although whether these leaked business records can then be used as evidence in a trial remains an open question, international criminal investigators would be remiss not to explore this trove of potentially relevant data to generate leads and support operations.

73. *See* Graham Dunbar, *FIFA's Ethics Judge Just Resigned After Being Named in the Panama Papers*, Associated Press (Apr. 6, 2016), https://www.businessinsider.com/ap-fifa-ethics-judge-damiani-resigns-while-under-suspicion-2016-4 [https://perma.cc/7WH8-XBLK].

74. *See Austrian Bank's CEO Quits After Panama Papers Reports*, Reuters (Apr. 6, 2016), https://www.reuters.com/article/us-panama-tax-austria/austrian-banks-ceo-quits-after-panama-papers-reports-idUSKCN0X40DY [https://perma.cc/V54Z-ZYB2].

75. Hou et al., *supra* note 63.

76. Press Release, Department of Justice, Four Defendants Charged in Panama Papers Investigation (Dec. 4, 2018), https://www.justice.gov/usao-sdny/pr/four-defendants-charged-panama-papers-investigation [https://perma.cc/858H-WHMP]; Sealed Indictment, United States v. Owens, No. 18-cr-693 (S.D.N.Y. Sept. 27, 2018), https://www.justice.gov/usao-sdny/press-release/file/1117201/download [https://perma.cc/H893-CGR3].

77. The Off. of the Prosecutor [OTP], ICC, Strategic Plan 2019–2021 ¶ 16 (2019), https://www.icc-cpi.int/itemsDocuments/20190726-strategic-plan-eng.pdf [https://perma.cc/9KDC-TRHQ].

78. While the ICC would not have jurisdiction over financial crimes, the Panama Papers could be used for asset tracing of defendants or to establish contextual information about the funding and beneficiaries of armed conflicts. *See* OTP, ICC, Financial Investigations and Recovery of Assets 5, 15–16 (Nov. 2017), https://www.icc-cpi.int/iccdocs/other/Freezing_Assets_Eng_Web.pdf [https://perma.cc/6WZY-UG3P]; *see also Global: Assistance with Asset Tracing*, Glob. Diligence (May 26, 2020), https://www.globaldiligence.com/projects-and-news/2020/5/26/global-assistance-with-asset-tracing [https://perma.cc/4GQ3-LVM9].

II. From Cybercriminals to Hacktivists

"Life is short. Have an affair."[79] That was the slogan of Ashley Madison—a Canadian dating site targeted at married people looking to cheat on their spouses and flaunting a customer-base of 37.6 million members—when it was hacked in 2015.[80] Security analyst Brian Krebs broke the story after being alerted to the millions of real names and credit card numbers stolen from the servers of parent company Avid Media Life and leaked onto the internet by a group calling themselves the Impact Team. Despite Ashley Madison's assurances that they were discreet, secure, and totally anonymous, all of the members of the service—including some well-known celebrities and politicians—were exposed. The publication of personal data from this hack could, and perhaps did, serve as a useful resource for evidence of infidelity in divorce proceedings.

While there is precedent for using leaked documents from a well-intentioned whistleblower as evidence of government wrongdoing, the situation is more complicated when the facts are reversed. What happens when a hacker, possibly one working for or affiliated with a government, leaks the personal data of private citizens? A hacker or leaker may be unknown, unreliable, or motivated by malice. Hacking, which is defined as the act of gaining unauthorized access to information through computer networks, can be done using a variety of techniques,[81] carried out by a number of different types of actors for various reasons. A profit-driven hacker may steal proprietary information for financial gain, a hacktivist (hacker with the goal of social or political activism) may steal and leak private data with the goal of punishment, retribution, or accountability, or a bored hacker may just do it for the lulz.[82]

79. Brian Krebs, *Online Cheating Site Ashley Madison Hacked*, Krebs on Sec. (July 19, 2015), https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked [https://perma.cc/4EQ4-ZPKB].

80. Tom Lamont, *Life After the Ashley Madison Affair*, The Guardian (Feb. 27, 2016), https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked [https://perma.cc/AL5S-7KMJ].

81. *See Hack*, Oxford Eng. Dictionary, https://www.oed.com/view/Entry/83030; *5 Common Hacking Techniques*, Mitnick Sec. (Feb. 22, 2020, 2:04 PM), https://www.mitnicksecurity.com/blog/5-common-hacking-techniques-for-2020 [https://perma.cc/PKJ9-PTTB].

82. The word "lulz" is a slang version of the commonly used internet term "LOL," which stands for laughing out loud. Hacking for the lulz means hacking just for the fun or entertainment of it. *See I Did it for the Lulz*, Urb. Dictionary, https://www.urbandictionary.com/define.php?term=i%20did%20it%20for%20the%20lulz [https://perma.cc/54B2-T9NB].

A hack can range from an individual stumbling across a network vulnerability, to coordinated attacks perpetrated in contravention of international law. This Part examines three common hacking scenarios, using some of the more notorious hacks as case studies, including: (1) state-sponsored hacks in which private entities have their emails and other data stolen and published online—such as the Sony Pictures and the Democratic National Committee (DNC) hacks; (2) data breaches in which personal user data held by a third-party are published online—such as the examples of Equifax, Yahoo, and LinkedIn; and (3) politically or socially motivated hacks that target specific entities and publish their information online—such as those operations carried out by Anonymous aimed at the Westboro Baptist Church, Bashir-al-Assad's regime in Syria, Tunisian government officials, and the Steubenville High School football team.

A. State-Sponsored Hacks

On November 24, 2014, in advance of the release of the comedy film *The Interview*, confidential data—including email correspondence and employee information from Sony—was leaked on the internet.[83] A group calling themselves Guardians of Peace took credit for the hack, demanding that the film—which poked fun at the leader of North Korea, Kim Jong-un—be withdrawn.[84] The group also threatened to attack movie goers if the film was screened in theaters.[85] The hacking method of choice for the Guardians of Peace was malware that erased the company's computer infrastructure.[86] After investigating the incident, the U.S. government attributed the hack to North Korea.[87]

In anticipation of the 2016 presidential election in the United States, the servers of the DNC were illegally accessed by a hacker with the handle Guccifer 2.0, and DNC emails were subsequently and strategically released on WikiLeaks. Before the breach occurred, presidential

83. Alex Campbell, *The Legal Implications of Sony's Cyberhack*, 11 Okla. J.L. & Tech. 1, 1 (2015).

84. Andrea Peterson, *The Sony Pictures Hack, Explained*, Wash. Post (Dec. 18, 2014, 1:15 PM), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained [https://perma.cc/PYS8-LBHZ].

85. *Id.*

86. Kim Zetter, *The Sony Hackers Were Causing Mayhem Years Before They Hit the Company*, Wired (Feb. 24, 2016, 7:00 AM), https://www.wired.com/2016/02/sony-hackers-causing-mayhem-years-hit-company [https://perma.cc/F9KE-P8UC].

87. Ellen Nakashima, *U.S. Attributes Cyberattack on Sony to North Korea*, Wash. Post (Dec. 19, 2014), https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html [https://perma.cc/8PR2-BV68].

candidate Donald Trump made a public speech requesting that Russia hack into the emails of his opponent, presidential candidate Hillary Clinton.[88] Trump claimed that he was only joking with this statement, but after investigating the incident, the U.S. intelligence community attributed the hack to Russia.[89]

In both cases, stolen private emails, employee data, and company data were leaked online and reported on by journalists who highlighted the more salacious, incriminating, and entertaining communications found in their disclosure.[90] Leaked documents from Sony and the DNC contained a variety of information, including communications between attorneys and their clients, as well as attorney work product.[91] In the case of Sony, the company-hired lawyer David Boies tried to put the proverbial cat back in the bag by threatening media organizations against publishing the stolen data. He argued that it contained privileged information and that the privilege was not waived by the disclosure.[92] The implications of documents containing privileged communications, such as those between an attorney and their client, are discussed in Part IV. The Sony and DNC hacks were intentional and targeted, but they nevertheless incidentally exposed data on innocent private citizens in the disclosures. As the desire for corporate accountability in international human rights grows, so too will the evidentiary value of this type of data, which could be used to establish a range of

88. Ashley Parker & David E. Sanger, *Donald Trump Calls on Russia to Find Hillary Clinton's Missing Emails*, N.Y. Times (July 27, 2016), https://www.nytimes.com/2016/07/28/us/politics/donald-trump-russia-clinton-emails.html [https://perma.cc/E88J-QJLB].

89. S. Rep. No. 116-XX, at 48 (2020); Nat'l Intel. Council, Off. of the Dir. Of Nat'l Intel., Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution 3 (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [https://perma.cc/3ZQ3-BQ7D].

90. Beatrice Verhoeven & Matt Donnelly, *Greatest Hits of Leaked Sony Emails: Angelina Jolie, 'Aloha,' David Fincher and More*, The Wrap (Nov. 12, 2015), https://www.thewrap.com/greatest-hits-leaked-sony-emails-angelina-jolie-aloha-david-fincher [https://perma.cc/734G-RAWL].

91. Kelly Sweeny, *Sony Pictures' Hacked Emails Reveal Privileged Communications*, Data Priv. & Sec. Insider (Apr. 22, 2015), https://www.dataprivacyandsecurityinsider.com/2015/04/sony-pictures-hacked-emails-reveal-privileged-communications [https://perma.cc/M568-CXKV]; Michael Cieply, *WikiLeaks Posts Sony Pictures Documents, Angering the Studio*, N.Y. Times (Apr. 16, 2015), https://www.nytimes.com/2015/04/17/business/media/sony-pictures-is-angered-by-wikileaks-posting-of-its-stolen-documents.html [https://perma.cc/5MXK-HM4D].

92. Michael Cieply & Brook Barners, *Sony Pictures Demands that News Agencies Delete 'Stolen' Data*, N.Y. Times (Dec. 14, 2014), https://www.nytimes.com/2014/12/15/business/sony-pictures-demands-that-news-organizations-delete-stolen-data.html [https://perma.cc/CUF8-8LR9]; Cieply, *supra* note 91.

facts from the organizational charts and chains of commands to business relationships and contracts.

B. Corporate Data Breaches

If you search for the biggest hacks in history, the majority are significant corporate data breaches in which a private company's servers are hacked and the data of its customers leaked. Some of the most well-known examples of these hacks include attacks on Equifax, Yahoo, LinkedIn, eBay, Marriot, Under Armor, Adobe, and Domino's Pizza.[93] As the diverse range of targeted companies demonstrates, all types of businesses are susceptible to security breaches, no matter what type of services or products they offer. If they are large and possess user data, they may be targets. User data in corporate breaches usually include names, usernames, email addresses, phone numbers, home addresses, passwords, and credit card numbers. The stolen data may be sold, provided at request, or openly accessible on the surface web (World Wide Web, indexed by search engines) or the dark web (hidden websites only accessible through the use of specific software).[94]

The Equifax data breach revealed the personal data of over 145 million people,[95] including "people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."[96] The hackers also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people. Equifax agreed to a global settlement of up to $425 million with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories.[97] In 2018, the fitness clothing company Under Armor revealed that data from about 150 million MyFitnessPal diet and fitness app accounts were compromised in one of the biggest hacks in history.[98] As a smartphone

93. Megan Leonhardt, *The 10 Biggest Data Hacks of the Decade*, CNBC (Dec. 27, 2019), https://www.cnbc.com/2019/12/23/the-10-biggest-data-hacks-of-the-decade.html [https://perma.cc/7D2K-5JSA].

94. Berkeley Protocol, *supra* note 1, at 6.

95. Hal Berhel, *Equifax and the Latest Round of Identity Theft Roulette*, 50 Computer 72, 72 (2017).

96. Seena Gressin, *The Equifax Data Breach: What to Do*, Knox Cnty. Emps. Credit Union (Sept. 8, 2017), http://www.knoxcountyecu.com/Docs_Pdfs/KCECU/Equifax_Data_Breach-What_To_Do.pdf [https://perma.cc/KNS2-NQHB].

97. *Equifax Data Breach Settlement*, FTC (Jan. 2020), https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement [https://perma.cc/M3ZJ-6KJ9].

98. *Under Armour Says Data Hacked From 150M MyFitnessPal App Accounts*, NBC News (Mar. 30, 2018), https://www.nbcnews.com/tech/security/under-armour-says-data-hacked-150m-myfitnesspal-app-accounts-n861406 [https://perma.cc/WJ5D-EWKT].

application that tracks a person's movement and diet, among other metrics and biometrics, this hack exposed the health and geolocation data of users in addition to the traditional types of leaked data. Other super data breaches include 3 billion compromised Yahoo accounts[99] and credentials for more than 412 million users of dating websites run by California-based FriendFinder.[100] A 2014 attack compromised the data of some 83 million JPMorgan Chase customers, and the email addresses retrieved in this breach were later used to commit fraud.[101]

While these types of commercial hacks may not seem immediately relevant to international criminal investigations, they certainly could turn out to be relevant in some circumstances.[102] War criminals and corrupt government officials use these services too, especially social media platforms.[103] As a result, digital open source investigations are becoming an integral part of investigation strategy at ICL courts and tribunals.[104] Digital open source investigators use a diverse range of publicly available information in their investigative work, including social media, government websites, public records, maps and geospatial platforms, directories, and databases. Some open source investigators consider the use of data from breaches fair game to advance their investigations. For example, the website HaveIBeenPwned.com, created by technology consultant Troy

99. *Yahoo Must Face Litigation by Data Breach Victims Judge Rules*, NBC News (Aug. 31, 2017), https://www.nbcnews.com/tech/tech-news/yahoo-must-face-litigation-data-breach-victims-judge-rules-n797871 [https://perma.cc/97BA-9DSB].

100. *Adult FriendFinder Hack Potentially Exposes Millions*, NBC News (May 22, 2015), https://www.nbcnews.com/tech/security/hack-potentially-exposes-millions-adult-friend-finder-users-n363196 [https://perma.cc/F5PR-ZRX7].

101. '*Hacking as a Business Model': Three Indicted in JPMorgan Hack*, NBC News (Nov. 10, 2015), https://www.nbcnews.com/tech/tech-news/jp-morgan-hack-three-indicted-cyberattacks-major-companies-n460671 [https://perma.cc/6MMA-DWFM].

102. *Cf.* Joseph F. Yenouskas & Levi W. Swank, *Emerging Legal Issues in Data Breach Class Actions*, Bus. L. Today (July 17, 2018), https://www.americanbar.org/groups/business_law/publications/blt/2018/07/data-breach [https://perma.cc/7R5E-QVFQ]; Mark Baker, *Expert Witness: Delivering Evidence from the Dark Web When Data Breaches Go to Court*, UK Tech News (June 24, 2020), https://uktechnews.co.uk/2020/06/24/expert-witness-delivering-evidence-from-the-dark-web-when-data-breaches-go-to-court [https://perma.cc/3TW8-TGPE]; Winston Krone, Kivu Consulting, Legal and Technical Issues Concerning Evidence in Data Breach Cases (2012), https://kivuconsulting.com/wp-content/uploads/2012/08/2012-Legal_and_Technical_Issues_Concerning_Evidence_in_Data_Breach_Cases_WKrone.pdf [https://perma.cc/PY85-NTEX].

103. Prosecutor v. Al-Werfalli, ICC-01/11-01/17-2, Warrant of Arrest (Aug. 15, 2017); *see also Libya 'War Crimes' Video Shared on Social Media*, BBC (Apr. 30, 2019), https://www.bbc.com/news/av/world-africa-48105968 [https://perma.cc/3Q3H-V397].

104. Berkeley Protocol, *supra* note 1, at 4; Alexa Koenig, Hum. Rts. Ctr., The New Forensics: Using Open Source Information to Investigate Grave Crimes (Andrea Lampros & Eric Stover eds., 2018), https://humanrights.berkeley.edu/sites/default/files/publications/bellagio_report_july2018_final.pdf [https://perma.cc/932Q-QRKP]; OTP, ICC, *supra* note 77, ¶¶ 46, 54.

Hunt, is a resource for searching data breaches for names of those who might have personal data in the public sphere. One of the more popular resources for open source investigators is IntelTechniques, which offers instructional manuals and online training that cover "breached data" as its own specific category, citing to numerous other similar resources.[105] This data can be used in a number of creative ways in investigations—from finding a potential witness' contact information, to discovering transactions for user services, to mapping secret army bases.

An illustrative example of the creative use of customer data in international investigations is the use of Strava's global heatmap. As a student in 2018, open source researcher Nathan Ruser identified secret U.S. military sites using public data from Strava, a health tracking mobile application that incorporates social networking.[106] This exercise-tracking application's publicly available data, which represented an aggregated and anonymized view of user activities, revealed frequently used paths in areas of Syria and the Sahara not occupied by civilians.[107] Logically, Ruser concluded that the map showed the workout locations of military personnel. If Strava's private user data was hacked and leaked as well, it could be used to deanonymize this data and identify the names of military personnel. Thus, the conclusions that can be drawn from overlaying leaked private data on top of public data could create serious privacy and security vulnerabilities. Despite concerns over these vulnerabilities, leaked user data could prove incredibly valuable to international criminal investigators who, following Ruser's example, can exploit and extrapolate from user data in new and innovative ways.

C. Anonymous Exploits

Finally, there are hacks that are carried out by vigilantes and hacktivists, often motivated by political activism and social justice. The most well-known of these groups is Anonymous, which has been active for decades and engaged in a number of high-profile exploits over the years, including hacking to acquire private information and

105. IntelTechniques, https://inteltechniques.com/index.html [https://perma.cc/FD4G-8HYU]. These include: Have I Been Pwned, https://haveibeenpwned.com; DeHashed, https://dehashed.com; SpyCloud, https://spycloud.com; Gotcha, https://gotcha.pw; Ghost Project, https://ghostproject.fr; We Leak Info, https://weleakinfo.com; Leaked Source, https://leakedsource.ru; SnusBase, https://www.snusbase.com; Have I Been Compromised, https://haveibeencompromised.com (the last three websites are not recommended for use).

106. Strava, https://www.strava.com/about (not recommended for use).

107. Sara Ashley O'Brien, *How a 20-Year-Old Australian Student Discovered U.S. Military's Secret Sites*, CNN (Jan. 29, 2018), https://money.cnn.com/2018/01/29/technology/strava-nathan-ruser/index.html [https://perma.cc/PJF3-M8DG].

cyberattacks. Anonymous' exploits range from denial-of-service attacks on Visa, MasterCard, and PayPal in retaliation for cutting off services to WikiLeaks,[108] to targeting websites of the Tunisian government due to censorship during the Arab Spring,[109] to the release of the personal data of prominent members of the Westboro Baptist Church after they protested at the funeral of Sandy Hook victims.[110] In 2012, Anonymous allegedly broke into the mail server of the Syrian government, gained access to many of Bashar al-Assad staffers' inboxes, and gave over 2.4 million stolen emails to WikiLeaks.[111]

Later that year, they released incriminating photographs and tweets from the Steubenville High School football team in Steubenville, Ohio, after they were alleged to have gang raped an underage girl.[112] In the Steubenville rape case, Anonymous and another hacktivist group, KnightSec, publicly released a video hacked from the account of one of the football program's leaders, who they alleged had helped cover up the case.[113] They threatened to reveal names of unindicted participants and demanded an apology from school officials who covered it up. The hacked information was leaked on Local Leaks, a website similar to WikiLeaks, and contained an incriminating image of football players carrying the unconscious sixteen-year-old victim.[114] While federal law

108. George Reynolds, Ethics in Information Technology (4th ed. 2012), 120–122, 152.

109. *Anonymous Activists Target Tunisian Government Sites*, BBC (Jan. 4, 2011), https://www.bbc.com/news/technology-12110892 [https://perma.cc/CLG8-MLNT].

110. Wolff Bachner, *Anonymous Hacks The Westboro Baptist Church: Posts All Their Personal Information*, INQUISITR (Dec. 16, 2012), https://www.inquisitr.com/440545/anonymous-hacks-the-westboro-baptist-church-posts-all-their-personal-information [https://perma.cc/4GMB-6P3X].

111. Dan Goodin, *Anonymous Takes Credit for Hack That Exposes 2.4 Million Syrian E-mails*, ARS Technica (July 9, 2012), https://arstechnica.com/information-technology/2012/07/anonymous-takes-credit-for-syrian-emails-hack [https://perma.cc/9M6K-P8FG].

112. Erik Ortiz, *Steubenville High School Students Joke About Alleged Rape in Highly-Charged Case Against Big Red Football Players*, N.Y. Daily News (Jan. 3, 2013), https://www.nydailynews.com/news/crime/steubenville-students-laugh-alleged-rape-article-1.1232113 [https://perma.cc/8UY6-ZSW3].

113. Juliet Macur, *Hackers of Football Team's Web Site Demand Apology in Rape Case*, N.Y. Times (Dec. 24, 2012), https://www.nytimes.com/2012/12/25/sports/hackers-of-steubenville-football-teams-web-site-demand-apology-in-rape-case.html [https://perma.cc/V8JZ-TQEQ]; Katie J.M. Baker, *Anonymous Outs Members of Alleged Steubenville High School 'Rape Crew'*, Jezebel (Dec. 24, 2012), https://jezebel.com/anonymous-outs-members-of-alleged-steubenville-high-sch-5970975 [https://perma.cc/WU5C-35TP].

114. Alexander Abad-Santos, *Inside Anonymous Hacking File on Steubenville 'Rape Crew'*, The Atl. (Jan. 2, 2013), https://www.theatlantic.com/national/archive/2013/01/inside-anonymous-hacking-file-steubenville-rape-crew/317301 [https://perma.cc/X7BQ-NRB8].

enforcement sought an indictment under the Computer Fraud and Abuse Act for the hackers, prosecutors on the Steubenville rape case used the now public material as evidence of the rape.[115]

In the wake of the 2020 police murder of George Floyd, Anonymous hacked law enforcement fusion centers to acquire police data.[116] In total, 269 GB of data were taken from over 200 law enforcement agencies in a file named "Blue Leaks" and published by Distributed Denial of Secrets, a platform for online leaks.[117] The Blue Leaks hack exposed the personal data of 700,000 police officers.[118] The data dump contained emails and associated attachments.[119] Fusion centers are state-owned information gathering and analysis centers that coordinate between different local, state, and federal law enforcement. The Blue Leaks file was conveniently published during national protests demanding accountability for police officers, which created the political will necessary to move civil rights lawsuits against police officers forward.[120] While civil rights lawyers were not involved in the hack of police fusion centers, they are potential beneficiaries whose legal cases could be bolstered by these revelations.

On some occasions, Anonymous has threatened their activities in advance or admitted to wanting to assist journalists and lawyers seeking accountability for wrongdoing, as they perceive it.[121] While perhaps the

115. Richard A. Oppel Jr., *Ohio Teenagers Guilty in Rape That Social Media Brought to Light*, N.Y. Times (Mar. 17, 2013), https://www.nytimes.com/2013/03/18/us/teenagers-found-guilty-in-rape-in-steubenville-ohio.html?pagewanted=all [https://perma.cc/TX7X-8ZWW].

116. Andy Greenberg, *Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents*, Wired (June 22, 2020, 12:48 PM), https://www.wired.com/story/blue-leaks-anonymous-law-enforcement-hack [https://perma.cc/N2HJ-S8PN].

117. Nichole Karlis, *Inside "Blue Leak," a Trove of Hacked Police Documents Released by Anonymous*, Salon (June 22, 2020), https://www.salon.com/2020/06/22/inside-blue-leaks-a-trove-of-hacked-police-documents-released-by-anonymous [https://perma.cc/5EJG-24DD].

118. Micah Lee, *Hack of 251 Law Enforcement Websites Exposes Personal Data of 700,000 Cops*, The Intercept (July 15, 2020, 11:00 AM), https://theintercept.com/2020/07/15/blueleaks-anonymous-ddos-law-enforcement-hack [https://perma.cc/F824-4EMF].

119. The National Fusion Center Association explained: "Our initial analysis revealed that some of these files contain highly sensitive information such as ACH routing numbers, international bank account numbers (IBANs), and other financial data as well as personally identifiable information (PII) and images of suspects listed in Requests for Information (RFIs) and other law enforcement and government agency reports." Karlis, *supra* note 117.

120. *Civil Rights Movement Lawsuits 2020*, The Nat'l Black Lawyers, https://nbltop100.org/civil-rights-movement-lawsuits-2020 [https://perma.cc/W3DT-QVHB]; Nat'l Police Accountability Project, https://www.nlg-npap.org/about-npap-justice [https://perma.cc/V4PY-24KD].

121. In the past, Anonymous has announced its targets before they hack them or broadcast that they already have the private data and threaten to release it. This was the case when Anonymous went up against Mexico's Los Zetas cartel, where it threatened to release both

most prolific example, Anonymous is by no means the only group that carries out these kinds of exploits.

In 2015, an Italian-based company called Hacking Team, known for selling surveillance and hacking tools to governments, was itself hacked by "Phineas Fisher."[122] The company's sensitive documents were then leaked publicly. Some of its stolen documents were leaked through the company's own Twitter account, which was taken over by the hacker(s).[123] Like the Panama Papers, this leak involved internal communications and contracts between the private entity and government customers. The leaked documents revealed that Hacking Team was selling its software to and had contracts with authoritarian regimes such as the governments of Kazakhstan, Sudan, Russia, and Saudi Arabia.[124] In particular, it showed wire transfers from the Sudanese government, a country of interest to the ICC whose government is known to conduct illegal surveillance on its citizens.[125] The ICC has been investigating mass atrocities committed in Darfur, Sudan for over a decade, with an arrest warrant out for the former Head of State Omar al Bashir since 2007.[126] While the information revealed in the Hacking Team hack may not be direct evidence of these crimes, it is certainly relevant to any entity that is investigating the Sudanese government and trying to understand how it operates.

The methods by which private digital documents can be illegally acquired and shared publicly are diverse, as is the information they contain. The variety of cases described in this Part is intended to show the many ways in which different types of leaked information could have investigative or evidentiary value in international criminal cases, including those within the jurisdiction of the ICC. These examples also

---

the names of cartel members as well as corrupt officials in the Mexican government supporting the Zetas. Charles Arthur, *Anonymous Retreats From Mexico Drug Cartel Confrontation*, The Guardian (Nov. 2, 2011, 8:11 AM), https://www.theguardian.com/technology/2011/nov/02/anonymous-zetas-hacking-climbdown [https://perma.cc/7VLV-H7R3].

122. John Zorabedian, *How Hacking Team Got Hacked*, Sophos: Naked Sec. (Apr. 19, 2016), https://nakedsecurity.sophos.com/2016/04/19/how-hacking-team-got-hacked/#:~:text=In%20a%20lengthy%20post%20on,Remote%20Control%20System%20(RCS) [https://perma.cc/2498-2MR7].

123. Jon Russell, *Hack Team, Which Sells Surveillance Tech to Governments, Exposed by Major Hack*, TechCrunch (July 6, 2015, 5:51 AM), https://techcrunch.com/2015/07/06/hacking-team-hacked [https://perma.cc/PWS8-FJ6U].

124. *Id.*

125. Austin Bodetti, *Sudan's Government Is Using a Shady Hacking Group to Hunt ISIS*, Vice (Apr. 27, 2017, 6:00 AM), https://www.vice.com/en_us/article/qkqxxx/sudans-government-is-using-a-shady-hacking-group-to-hunt-isis [https://perma.cc/584S-A2P8].

126. *Situation in Darfur, Sudan*, ICC, https://www.icc-cpi.int/darfur [https://perma.cc/JNZ5-NATL].

demonstrate the ethical dilemmas about whether and how this information can be used. Leaked documents from hacks of authoritarian governments and the corporations with whom they do business may contain useful information. However, their use as evidence in court could set a bad precedent for the use of other hacked information, such as that of private citizens.

III. Relevant Rules of Evidence

Rules of evidence vary by jurisdiction, with divergences between common and civil law systems.[127] As a result, there is no universal claim that can be made or a standardized test that can be applied to determine the admissibility of illegally obtained digital evidence, since what is admissible in one jurisdiction may be excluded in another. ICL courts and tribunals largely adopt a hybrid approach to evidence with minimal statutory guidance and considerable discretion left to the judges.[128] Thus, while the evidentiary and procedural rules differ between international and hybrid criminal courts and tribunals, there are often commonalities.

This Article concentrates on the Rome Statute (Statute) and the ICC's Rules of Procedure and Evidence (Rules) because these documents incorporated many elements from their predecessors[129] and have influenced ICL courts and tribunals established since the ICC's founding.[130] The relevant provisions to this discussion are those that determine how evidence should be handled by investigators, presented in court by the parties, and assessed by judges.

A. Admissibility of Evidence

The main provision governing the assessment of evidence at the ICC is Article 69 of the Statute. In particular, Article 69(4) addresses the issue of admissibility, stating, "[t]he Court may rule on the relevance or admissibility of any evidence, taking into account, *inter alia*, the probative value of the evidence and any prejudice that such evidence may cause to a fair trial or to a fair evaluation of the testimony

127. In jurisdictions with common law systems, evidence laws are often developed through jurisprudence, whereas civil law systems codify their rules in statutes.

128. Robert Cryer et al., An Introduction to International Law and Procedure (3d ed., 2014).

129. International Criminal Tribunals for Yugoslavia and Rwanda.

130. S.C. Res. 1757 (May 30, 2007) (establishing the Special Tribunal for Lebanon); Loi organique n°15–003 du 3 juin 2015 portant création, organisation et fonctionnement de de la Cour Pénale Spéciale [Organic Law No. 15–003 on the Creation, Organization and Functioning of the Special Criminal Court] (Cent. Afr. Rep.).

of a witness, in accordance with the Rules of Procedure and Evidence." This is echoed in Rule 64 of the Rules, which provides that, "[a] Chamber shall have the authority, in accordance with the discretion described in [A]rticle 64, paragraph 9, to assess freely all evidence submitted in order to determine its relevance or admissibility in accordance with [A]rticle 69"[131] and emphasizes that "evidence ruled irrelevant or inadmissible shall not be considered by the Chamber."[132]

The Appeals Chamber has held that Article 69(4) is a mandatory provision that requires the Trial Chamber to rule on the admissibility of each item of submitted evidence "at some point in the proceedings."[133] The determination of admissibility is to be made using a three-pronged test, which examines the relevance, probative value, and the potential prejudice of each item of evidence.[134] If the probative value is outweighed by any prejudicial effect, the item shall not be admitted into evidence.[135] This determination can be made at the time of submission or delayed until the final judgement, when it can be assessed holistically with the entire body of evidence.[136] Evidence is relevant if it has any tendency to make a fact of consequence in determining the action more or less probable than it would be without the evidence.[137] Probative value refers to the ability of a piece of evidence to make a relevant disputed point more or less true.[138] Prejudicial evidence is evidence that may cause an unfair trial.

Over time, the Chambers have established additional criteria for evaluating documentary evidence. In particular, the Chambers assess "the contents of the particular document, its provenance and any other relevant material[,] . . . the document's author if known, as well as his or her role in the relevant events and the chain of custody from the time

131. ICC, *Assembly of the States Parties to the Rome Statute of the International Criminal Court*, ICC-ASP/1/3, at 42 (2002) [hereinafter Rules of Procedural Evidence] (Rule 64(2) of the Rules).

132. Rules of Procedural Evidence, *supra* note 131 (Rule 63(2) of the Rules).

133. Prosecutor v. Bemba, ICC-01/05-01/08 OA 5 OA 6, Judgment on the Appeals, ¶ 37 (May 3, 2011).

134. *See also* Rome Statute of the International Criminal Court, art. 69(4), July 17, 1998, 2187 U.N.T.S. 38544 [hereinafter Rome Statute].

135. Prosecutor v. Lubanga, ICC-01/04-01/06-1399, Decision on the Admissibility of Four Documents, ¶¶ 27–32 (June 13, 2008).

136. This holistic approach has been the more commonly adopted one. *See* Lindsay Freeman & Raquel Vazquez Llorente, *Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age,* J. of Int'l Crim. Just. (forthcoming June 2021).

137. Fed. R. Evid. 401.

138. *Probative Value*, Cornell L. Sch.: Legal Info. Inst., https://www.law.cornell.edu/wex/probative_value [https://perma.cc/2UXQ-JEVA].

of the document's creation until its submission to the Chamber."[139] The indicia of reliability are broadly assessed and the Chamber has noted that a document, although authentic, may be unreliable.[140]

The Chambers have stated that reliability is not to be considered in the determination of admissibility, but rather will be examined when assessing the weight to be attributed to the evidence.[141] This approach is different from the majority of common law jurisdictions, in which evidence can be excluded based on a lack of reliability—for example, the rule against hearsay found in some national jurisdictions bars the introduction of hearsay into evidence unless it falls within a specific exception.[142] As legal scholar Michaela Halpern explains, the "difference stems from the fact that trials in common law jurisdictions often involve layman jurors" who need to be protected from unreliable evidence, whereas the civil law system uses trained judges who are "deemed capable of discerning the reliability of such evidence for themselves."[143] In *Prosecutor v. Lubanga*, Trial Chamber I stated that "(t)he Nuremberg and Tokyo Charters favored the admission of relevant evidence with determinations of weight made at a later stage, taking into account both the unique circumstances under which international criminal prosecutions take place and the fact that without juries there is no need to guard against the admission of potentially prejudicial evidence that could not be removed from the mind of the judges."[144]

139. Ngudjolo Judgment, *supra* note 22, ¶ 57; Prosecutor v. Lubanga, ICC-01/04-01/06-2842, Judgment Pursuant to Article 74 of the Statute, ¶ 109 (Dec. 26, 2012) [hereinafter Lubanga Judgment].

140. *Id.*

141. *Id.*

142. Michael A. Newton, *Comparative Complementarity: Domestic Jurisdiction Consistent with the Rome Statute of the International Criminal Court*, 167 Mil. L. Rev. 20, 66 (2001); Håkan Friman, *Information from the International Criminal Tribunals when Developing Law on Evidence for the International Criminal Court*, 2 L. & Prac. Int'l Cts. & Tribs. 373, 384 (2003); Fed. R. Evid. 802.

143. Michaela Halpern, *Trends in Admissibility of Hearsay Evidence in War Crime Trials: Is Fairness Really Preserved?*, 29 Duke J. Compar. & Int'l L. 103, 105 (2018).

144. Prosecutor v. Lubanga, ICC-01/04-01/06-1255, Prosecution's Submission on the Admissibility of Four Documents, ¶ 16 (Apr. 1, 2008); Richard May & Marieke Wierda, International Criminal Evidence 95 (2002); *see also* Vladimir Tochilovsky, Indictment, Disclosure, Admissibility of Evidence 57 (2004). This rationale remains prevalent at the ICTY where professional judges are able to consider each piece of evidence and determine appropriate weight: Vladimir Tochilovsky, Jurisprudence of the International Criminal Courts and the European Court of Human Rights: Procedure and Evidence 400 (2008). Citing in support of this principle are the decisions rendered in Prosecutor v. Orić, Case No. IT-03-68-T, Order Concerning Guidelines on Evidence and the Conduct of Parties During Trial Proceedings, ¶ 11 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 21, 2004); Prosecutor v. Hadžihasanović & Kubura, Case No. IT-01-47-T, Decision to Unseal Confidential Decision on the Admissibility of Certain Challenged Documents and Documents

Judges at other ICL courts and tribunals have observed that the ICC's interpretation of Article 69(4)'s application has varied.[145] For example, in *Prosecutor v. Lubanga*, Trial Chamber I held that where evidence is "demonstrably lacking any apparent reliability the Chamber must equally carefully decide whether to exclude the evidence at the outset" or wait to assess it at the end of the case.[146] However, in *Prosecutor v. Katanga*, Trial Chamber II applied a stricter assessment of authenticity at the admissibility stage, holding that "[if] at the time of tendering an item of evidence, the party is unable to demonstrate its relevance and probative value, including its authenticity, it cannot be admitted."[147]

B. Grounds for Exclusion

Even if evidence is relevant and admissible pursuant to Article 69(4), it may nevertheless be excluded pursuant to Article 69(7) of the Statue. Article 69(7) offers a two-step analysis regarding evidence that may be excluded at the discretion of the Trial Chamber. It states that "evidence obtained by means of a violation of [the Rome] Statute or internationally recognized human rights shall not be admissible if: (a) The violation casts substantial doubt on the reliability of the evidence; or (b) The admission of the evidence would be antithetical to and would seriously damage the integrity of the proceedings."[148] Other ICL courts have similar discretionary exclusionary rules.[149] Interestingly, the Statute does not mention the gravity of the offense, nor does it specify whether the violation must be carried out by the OTP. Another unanswered question is whether the violation must be of the rights of the accused or a general violation of any individual's human rights.

---

for Identification, ¶ 17 (Int'l Crim. Trib. for the Former Yugoslavia Aug. 2, 2004); *see also* Fofana—Appeal Against Decision Refusing Bail, ¶ 26, Prosecutor v. Norman, Case No. SCSL-04-14-AR65 (Special Ct. for Sierra Leone, App. Ct. Mar. 11, 2005).

145. Prosecutor v. Ayyash, Case No. STL-11-01/T/TC, Decision on the Admissibility of Documents Published on the WikiLeaks Website, ¶ 10 (Special Trib. for Lebanon May 21, 2015) [hereinafter Prosecutor v. Ayyash].

146. Prosecutor v. Lubanga, ICC-01/04-01/06-1399, Decision on the Admissibility of Four Documents, ¶ 30 (June 13, 2008).

147. Prosecutor v. Katanga, ICC-01/04-01/07-2635, Decision on the Prosecutor's Bar Table Motions, ¶ 13 (Dec. 17, 2010).

148. Rome Statute, *supra* note 134, art. 69(7).

149. For example, Article 162 of the Special Tribunal for Lebanon's Rules of Procedure and Evidence explicitly permits the exclusion of evidence obtained by methods which may cast doubts on its reliability, or damage the integrity of the proceedings: "[n]o evidence shall be admissible if obtained by methods which cast substantial doubt on its reliability or if its admission is antithetical to, and would seriously damage, the integrity of the proceedings." Blair & Gojković, *supra* note 24, at 242.

The ICC has already recognized the right to privacy as an internationally recognized human right, the violation of which could lead to the exclusion of evidence. Citing to customary international law and international treaties, such as Article 17 of the International Covenant on Civil and Political Rights, the Court has asserted that the right to privacy is well established in international law.[150] In *Prosecutor v. Bemba et al.*, the Trial Chamber was asked to determine the admissibility of several types of digital evidence submitted by the prosecution, including Western Union documents and financial records, call data records from a telecommunications provider, and telecommunications intercepts obtained by Dutch law enforcement.[151] The decisions cited Article 8 of the European Convention on Human Rights, which provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[152] The Chamber ultimately admitted these challenged items into evidence, but nevertheless recognized an individual's right to privacy as an internationally recognized human right.

In *Prosecutor v. Mbarushimana*, Pre-Trial Chamber I considered how the search and seizure of hard drives from a residence related to the right to privacy. The Pre-Trial Chamber referred back to the decision in *Prosecutor v. Lubanga*,[153] where Trial Chamber I considered the admissibility of evidence obtained from an illegal search and seizure within the framework of Article 69(7). In *Prosecutor v. Lubanga*, Democratic Republic of the Congo authorities searched the residence of a colleague of the accused in the presence of an OTP investigator. The Chamber confirmed that a breach of the residence owner's right to privacy had occurred and that the breach was disproportionate. However, Trial Chamber I found that Article 69(7)(b) was not triggered because "a) the violation in question was not particularly grave, b) the impact of

150. Prosecutor v. Bemba, ICC-01/05-01/13-1855, Decision on Requests to Exclude Dutch Intercepts and Call Data Records, ¶ 10 (Apr. 29, 2016) (citing Art. 8(2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms); Vivek Krishnamurthy, *A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy*, 114 AJIL Unbound 26, 26–27 (2020).

151. *See* Prosecutor v. Bemba, ICC-01/05-01/13-1854, Decision on Requests to Exclude Western Union Documents and Other Evidence Pursuant to Article 69(7), ¶¶ 1, 11 (Apr. 29, 2016); Prosecutor v. Bemba, ICC-01/05-01/13-1855, Decision on Requests to Exclude Dutch Intercepts and Call Data Records, ¶¶ 1–2 (Apr. 29, 2016).

152. European Convention on Human Rights art. 8, Nov. 4, 1950, E.T.S No. 005.

153. Prosecutor v. Lubanga, ICC-01/04-01/06-1981, Decision on the Admission of Material From the "Bar Table" (June 24, 2009); Prosecutor v. Lubanga, ICC-01/04-01/06-683, Public Redacted Version of Request to Exclude Evidence Obtained in Violation of Article 69(7) of the Statute (Nov. 7, 2006).

the violation on the integrity of the proceedings was lessened because the rights violated were those of a witness and not of the accused and c) the illegal acts were committed by the Congolese authorities over whom the OTP investigator could exercise no influence."[154] Thus, when evaluating the application of Article 69(7), the Chamber considered the gravity of the violation, the victim of the violation (whether it was the accused's rights that were violated or those of a third party), and the identity of the violator (whether the violation was committed by an OTP investigator or third party investigator, as well as the OTP's degree of control over that third party). In evaluating a violation committed by a third party, as was the case here with the Congolese authorities, the Chamber assessed whether the OTP had any control over the actions of that third party—in essence, examining whether the Congolese authorities were acting as agents of the OTP.

In *Prosecutor v. Mbarushimana*, a case in which the charges were dismissed without prejudice after the confirmation hearing, the defense distinguished the facts from those in *Lubanga*, explaining:

> Firstly, the inability of the Prosecution to prove the legality of a search and the parameters thereof is far more grievous than performing a search in the absence of a witness. Secondly, the rights affected are those of Mr. Mbarushimana—the suspect himself and not those of a third party. Finally, the OTP investigator while having affirmed by way of affidavit that he acted merely as a curious spectator, provided no reason as to why he did not obtain a copy of the judicial warrant authorising the search.[155]

In jurisdictions like the United States, the exclusionary rule applies only when the violation is committed by a government official or someone acting as an agent of the government.[156] Therefore, evidence obtained illegally by a civilian, while violating the law, does not implicate the Fourth Amendment in criminal cases.[157] This exclusionary rule is designed to deter law enforcement within that jurisdiction from violating individuals' rights by excluding otherwise relevant evidence.[158] In international human rights law, states have a duty to protect

154. Prosecutor v. Mbarushimana, ICC-01/04-01/10-329, Defence Request for a Ruling on the Admissibility of Two Categories of Evidence, ¶ 5 (Aug. 3, 2011) [hereinafter Prosecutor v. Mbarushimana]; Prosecutor v. Mbarushimana, ICC-01/04-01/10-465-Red, Decision on the Confirmation of Charges (Dec. 16, 2011).

155. Prosecutor v. Mbarushimana, *supra* note 154, ¶ 6.

156. *See* U.S. Const. amend. IV.

157. *Enforcing the Fourth Amendment: The Exclusionary Rule*, Legal Info. Inst., https://www.law.cornell.edu/constitution-conan/amendment-4/enforcing-the-fourth-amendment-the-exclusionary-rule [https://perma.cc/8AMM-JC7G].

158. Katz v. United States, 389 U.S. 347 (1967).

the rights of their citizens. For example, Article 8 of the European Convention on Human Rights states,

> There shall be no interference by a public authority with the exercise of [the right to privacy] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[159]

Here, too, it must be a state actor who violates an individual's right to privacy. Article 69(7) does not provide this clarity, but there is a strong argument based on the *Lubanga* and *Mbarushimana* cases that the exclusionary rule applies only when the right is interfered with by the OTP or agents of the OTP, since it is the exclusion of prosecution evidence that would deter future violations.

In addition to the ICC's discretionary exclusionary rule, there are two other provisions by which the defense could challenge the disclosure and, in turn, the admissibility of hacked and leaked digital evidence. While not necessarily applicable in every case, documents might be excluded from evidence if they are privileged, classified, or sensitive.

Article 69(5) of the Rome Statute provides that the Court must respect and observe privileges on confidentiality as provided for in the Rules, specifically, Rule 73, which outlines the following categories of privileged communications: (1) lawyer-client privilege;[160] (2) communications made in the course of a confidential relationship producing a reasonable expectation of privacy and nondisclosure; and (3) information, documents, or other evidence of the International Committee of the Red Cross. According to Professor Mark Klamberg's commentary on the Rules, "[Rule 73] involves tensions between the interest of admitting evidence to prevent impunity on the one hand and the interest of protecting the confidentiality of certain communications."[161] Klamberg explains that "the ICC has several explicit rules providing for privilege against disclosure, namely the privilege against self-incrimination,

159. European Convention on Human Rights art. 8, Nov. 4, 1950, E.T.S No. 005.

160. Rome Statute, *supra* note 134, art. 67(1)(b); Rules of Procedural Evidence, *supra* note 131, at 45–46 (Rule 73). Article 67(1)(b) of the ICC Statute and Rule 73 of the Rules provide only two exceptions to the privileged nature of lawyer-client communications, waiver and voluntary communication, following the practice of the ICTY in Rule 97 of its own Rules of Procedure and Evidence.

161. Mark Klamberg, *ICC Commentary (CLICC)*, *Commentary Rules of Procedure and Evidence*, Case Matrix Network (Aug. 10, 2017), https://www.casematrixnetwork.org/cmn-knowledge-hub/icc-commentary-clicc/commentary-rules-of-procedure-and-evidence/commentary-rpe-ch-4/#c2205 [https://perma.cc/22LY-C94C].

the lawyer-client privilege, the doctor-, psychiatrist-, psychologist-, counsellor or clergy-person privilege and privileges for ICRC officials, employees[’] information, documents or other evidence.”[162] Therefore, if leaked documents contain information that is privileged and the privilege is not waived, then they will not be disclosable and thus not admissible in the proceedings. Attorney-client privilege and attorney work product are two categories of privileged communications and information that commonly arise in online leaks, particularly leaks of private business records.

Article 72(4) of the Statute states, “If a State learns that information or documents of the State are being, or are likely to be, disclosed at any stage of the proceedings, and it is of the opinion that disclosure would prejudice its national security interests, that State shall have the right to intervene in order to obtain resolution of the issue in accordance with this article.”[163] This Article represents a conflict between two different views, “one that [o]nly the State can properly assess when its national security is in jeopardy, the other that the Court should be the ultimate arbiter in such issues.”[164] Based on the language in the Statute, the balance tilts towards the states. While the Court may determine whether documents are relevant, necessary, and should be disclosed, such decisions are not necessarily enforceable.[165]

Professor Otto Triffterer’s commentary further explores how the word “security” should be interpreted, pointing out that a narrow understanding of security is the “threat or use of force against the territorial integrity or political independence of [another] state”[166] as understood in Article 2(4) of the United Nations Charter. A broader definition of national security would include the state’s territorial integrity, sovereignty, national defense, and military operations. The risk of having a broad definition of national security is that the concept becomes meaningless in practice.[167] Under such a broad definition, the scope of the provision becomes wide enough to apply at any stage of the proceedings and can frame disclosure in terms of information being revealed generally rather than the normal understanding of its restriction to the

162. *Id.*; Rome Statute, *supra* note 134, art. 72(4).

163. Rome Statute, *supra* note 134, art. 72(4).

164. Commentary on the Rome Statute of the International Criminal Court 550 n.602 (Mark Klamberg ed., 2017).

165. *See* Rodney Dixon, Helen Duffy & Christopher K. Hall, *Article 72*, *in* Commentary on the Rome Statute of the International Criminal Court: Observers’ Notes, Article by Article 1361, 1363–64 (Otto Triffterer ed., 2008).

166. U.N. Charter art. 2(4).

167. *See* Dixon et al., *supra* note 165, at 1365–66.

prosecution's disclosure to the defense.[168] If leaked government documents are classified or sensitive, a state could intervene to prevent their disclosure. Thus, the defense with state support could draw on this national security privilege, sometimes referred to as "state secrets privilege," to prevent the admission of leaked documents into evidence.

The intriguing legal question relating to both attorney-client privilege and national security privilege is whether the privilege still exists if the documents are already made public through leaking. Can states legitimately argue that disclosure of documents jeopardizes their national security if the documents are already disclosed to the public? In addition, neither privilege is absolute. The nondisclosure of privileged communications and information must, in all cases, be balanced with the rights of the accused and the guarantee of a fair trial.[169] In order to understand how this might play out in practice, we must examine the law in the context of facts.

IV. Evidentiary Challenges

The hacks and leaks described in Parts I and II provide facts to which the rules can be applied in order to analyze and assess how the legal framework in Part III might apply in practice. This analysis does not necessarily apply to all categories of illegally obtained evidence. Rather, it focuses specifically on publicly available information that was obtained through illegal hacking or leaking. Further, this Article concentrates on digital hacked and leaked documents, which come with a unique set of challenges. The authenticity of illegally obtained physical evidence tends to be less of an issue since the provenance of physical objects stolen or improperly seized from a home or office is known, whereas such provenance is often unknown with anonymous digital material. If the ICC prosecution submits hacked and leaked digital documents at trial, the defense can use four main provisions discussed in the previous Part to challenge their admissibility into evidence. While arguments to exclude evidence may fail, such challenges may nevertheless diminish the weight given to the evidence by the judges, which should not be overlooked.

168. *See* William A. Schabas, The International Criminal Court: A Commentary on the Rome Statute 866 (2010).

169. *See generally* Ariel Zemach, *National Security Evidence: Enhancing Fairness in View of the Non-Disclosure Regime of the Rome Statute*, 47 Isr. L. Rev. 331 (2014); Int'l Bar Ass'n, Offences Against the Administration of Justice and Fair Trial Considerations Before the International Criminal Court (Aug. 2017).

A. Lack of Authenticity

Opposing parties can argue that leaked documents do not meet the basic requirements for admissibility under Article 69(4) of the Rome Statute if they have not been authenticated. The Statute and Rules do not explicitly mention authenticity as a requirement for admissibility. However, authenticity is logically a consideration tied to the relevance requirement, since evidence is only relevant if it is authentic.[170] In *Prosecutor v. Ayyash et al.* at the Special Tribunal for Lebanon, the admission of WikiLeaks cables was challenged based on lack of authenticity.[171] One of the defense teams moved to admit into evidence two purported American diplomatic cables found on WikiLeaks describing meetings between Lebanese politicians and American diplomats.[172] The defense argued that emerging jurisprudence trended toward admitting such documents.[173] The prosecution challenged the admission, citing to *American Civil Liberties Union v. Department of State* in which WikiLeaks documents were also challenged on authenticity.[174] Ultimately, the Trial Chamber was satisfied that the subject-matter of the documents might be relevant to the proceedings;[175] however, it accepted the prosecution's argument on authenticity, explaining, "The Defence has not proved that the documents—apparently downloaded from the

170. Authenticity is established when the proffering party establishes that the document is what it purports it to be. "Authentication and identification represent a special aspect of relevancy." Fed. R. Evid. 901, note to subdiv. (a); *see also* Jerome Michael & Mortimer J. Adler, *Real Proof: I*, 5 Vand. L. Rev. 344, 362 (1952); Charles T. McCormick, McCormick on Evidence §§ 179, 185 (8th ed., 2020); Edmund M. Morgan, Basic Problems of Evidence 378 (Charles E. Clark ed., 1963). Thus, a telephone conversation may be irrelevant because on an unrelated topic or because the speaker is not identified. The latter aspect is the one involved here. Wigmore describes the need for authentication as "an inherent logical necessity." 7 John Henry Wigmore, A Treatise on the Anglo-American System of Evidence in Trials at Common Law § 2129 (3d ed., 1940).

171. Prosecutor v. Ayyash, *supra* note 145, ¶¶ 9–13. *See also R v. Sec'y of State for Foreign & Commonwealth Affs. [2018] UKSC 3 (appeal taken from Eng.),* in which the cornerstone of the case is a document published on Wikileaks and by The Guardian on December 2, 2010 and by The Daily Telegraph on February 4, 2011. It is claimed to be a copy of a "cable" (in fact, a communication sent, received and stored electronically but which can, if required, be printed) sent on May 15, 2009 by the U.S. Embassy in London to departments of the U.S. federal government in Washington, to elements of its military command, and to its Embassy in Port Louis, Mauritius. *See also* Robert McCorquodale, *Wikileaks Documents Are Admissible in a Domestic Court*, EJIL:Talk! (Feb. 21, 2018), https://www.ejiltalk.org/wikileaks-documents-are-admissible-in-a-domestic-court [https://perma.cc/8ZAK-RELU].

172. Prosecutor v. Ayyash, *supra* note 145, ¶ 1.

173. *Id.* ¶¶ 9, 23.

174. Prosecutor v. Ayyash, Case No. STL-11-01/T/TC, Transcript of Hearing, at 85 (Special Trib. for Lebanon Mar. 26, 2015); *see also* ACLU v. Dep't of State, 878 F. Supp. 2d 215 (D.D.C. 2012).

175. Prosecutor v. Ayyash, *supra* note 145, ¶ 15.

WikiLeaks website—are authentic US diplomatic cables. The documents may be authentic, but the Trial Chamber has no evidence of the US Government acknowledging their authenticity, or indeed their accuracy."[176] The two WikiLeaks cables were not admitted into evidence, although the defense was allowed to question one witness based on the documents. Had the witness been able to authenticate the documents, they would have likely been admitted. Without that corroboration, however, they were not sufficiently reliable to be admitted into evidence.

Digital material is relatively easy to alter, and such alterations are often difficult to detect. Therefore, when it comes to leaked digital material, establishing authenticity is a challenge since there is no clear chain of custody from the source of the documents to their publication online, leaving a window during which they could be altered.[177] In addition, leaked digital documents could be completely fabricated. This challenge will only increase with the introduction of deepfakes and other synthetic media—digital content generated using artificial intelligence—as it will be faster, easier, and cheaper to generate convincing forgeries.[178] A foundation of authenticity must be established for any digital item acquired from the internet rather than from the direct source, because the anonymity of the internet and the malleability of the digital medium make it particularly susceptible to fakery. This is true of all types of digital open source information and leaks that lack provenance or a clear chain of custody.

Another example of the challenges around authenticity of leaked documents is the Killian documents, which were provided to the veteran CBS reporter and anchor Dan Rather, who, believing them to be authentic, used them as the basis for a story on his Evening News program.[179] The documents were purported to be Air National Guard internal reports written by Lt. Col. Jerry B. Killian, who was George W. Bush's commanding officer while Bush was an airman, and which

176. *Id.* ¶ 40.

177. Bruce Schneier, *How Long Until Hackers Start Faking Leaked Documents?*, The Atl. (Sept. 13, 2016), https://www.theatlantic.com/technology/archive/2016/09/hacking-forgeries/499775 [https://perma.cc/R9QA-K4BP].

178. Synthetic media is digital content generated by artificial intelligence, and deepfakes are a type of AI-generated video content. Merriam Webster Dictionary has "deepfakes" on their words to watch list, since the definition is still be developed. *Words We're Watching: 'Deepfake'*, Merriam-Webster, https://www.merriam-webster.com/words-at-play/deepfake-slang-definition-examples [https://perma.cc/NA6G-6YVS]; *see also* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security*, 107 Cal. L. Rev. 1753 (2019).

179. Mary Mapes, Truth and Duty: The Press, the President, and the Privilege of Power 1–3 (2005).

were critical of Bush's job performance. The documents were obtained by CBS News producer Mary Mapes from a former officer in the Texas Army National Guard, whom she believed to be a reliable source. After Rather's report aired, multiple people came forward to challenge the authenticity of these documents based on a number of factors including typography, content, and formatting.[180] While it is often impossible to establish with absolute certainty the authenticity of documents without the originals, as was the case here, a variety of information can be used to prove the documents are inauthentic or put the authenticity of the documents into question.

The prosecution has two main channels to combat these challenges: presenting additional evidence to authenticate the documents, such as witness testimony, or acquiring original versions of the files directly from a source. For example, in regard to the Panama Papers, the U.S. Department of Justice was able to do the latter, using their subpoena power to acquire communications between Mossack Fonseca and certain banks from those entities within U.S. jurisdiction.[181] If that is not possible, investigators need to take additional measures to acquire corroborating information to establish the authenticity before they are admitted. They might call a witness who can testify to the creation of a document or the veracity of its contents, or the prosecution may call the whistleblower or hacker to the stand in order to prove the source of the documents and chain of custody. On its website, WikiLeaks explains its vetting process in which staff members examine the documents and make note of any suspected inauthenticity based on "a forensic analysis of the document, means, motive and opportunity, cost of forgery, what the authoring organization claims and so on."[182] There are a number of ways in which leaked documents could be authenticated, such as through the testimony of a witness with direct knowledge or an expert who has conducted forensic analysis. Business records could be authenticated through comparison with previously acquired and verified records from that business, as was the case with the Panama Papers, but the same approach would not apply necessarily to other types of leaks, such as those derived from corporate data breaches or

180. Maureen Balleza & Kate Zernike, *The 2004 Campaign: National Guard; Memos on Bush Are Fake but Accurate, Typist Says*, N.Y. Times (Sept. 15, 2004), https://www.nytimes.com/2004/09/15/us/the-2004-campaign-national-guard-memos-on-bush-are-fake-but-accurate.html [https://perma.cc/N74J-FUTJ].

181. Hou et al., *supra* note 63.

182. WikiLeaks, https: //wikileaks.org/wiki/Wikileaks:About [https://perma.cc/N4CN-UZUG].

exposing personal emails.[183] Since many whistleblowers and hackers want to stay anonymous to avoid retribution or criminal prosecution, getting them to appear in court will often be a challenge. Without confirming where the documents came from or verifying the information therein, it will be difficult to justify their admission at trial.

B. Violation of Privacy

Alternatively, the opposing party can argue that leaked documents should be excluded pursuant to Article 69(7) of the Statute, because they were obtained in violation of the right to privacy, and that this violation makes them unreliable or prejudicial. Obtaining private documents without a warrant or consent has been well-established as a violation of the right to privacy. The European Court of Human Rights has held that interference by way of search and seizure will constitute a breach of the right to privacy unless it can be shown that it was both "necessary in a democratic society" and done "in accordance with the law" for a legitimate purpose.[184] Hacking is illegal and therefore would not qualify for this exception.[185] The European Court of Human Rights has ruled that business premises and business records are covered by the right to privacy under Article 8 of the Convention.[186]

If the documents were obtained through hacking or were leaked inappropriately without serving the public interest, then it is probable that the ICC will determine that they were obtained in violation of the right to privacy. This raises two additional questions—does it matter who committed the violation and does it matter whose rights were violated? In other words, does this provision only apply to the manner in which the prosecution, or an agent of the prosecution, obtained the evidence, or does it apply to anyone who violates the Statute or an internationally recognized human right in obtaining the evidence? Some insight into this question can be found in *Mbarushimana*, a decision in which the Trial Chamber considered the OTP's involvement in the interference and the OTP's degree of control over the entity committing

183. Obermaier & Obermayer, *supra* note 34, at 109–10; *The Panama Papers* (Epix television broadcast Oct. 6, 2018).

184. European Convention on Human Rights art. 8, Nov. 4, 1950, E.T.S. 5; *see* Eur. Ct. H.R., *Guide on Article 8 of the European Convention on Human Rights*, at 7 (Aug. 31, 2020), https://www.echr.coe.int/documents/guide_art_8_eng.pdf [https://perma.cc/5ACC-3EM8].

185. Stefanov v. Bulg., App. No. 65755/01, ¶¶ 57–60 (May 22, 2008), http://hudoc.echr.coe.int/eng?i=001-86449 [https://perma.cc/6MPV-9P6M]; *see also* Prosecutor v. Mbarushimana, *supra* note 154, ¶ 3.

186. Swiss Ctr. of Expertise in Hum. Rts., *The European Court of Human Rights: Protecting Businesses*, at 5 (Aug. 2017), https://www.skmr.ch/cms/upload/pdf/180830_ECHR_Protecting_Businesses.pdf [https://perma.cc/2HDF-JHKT].

the violation.[187] In addition, Article 69(7) leaves open the possibility that it is not just the accused whose rights must have been violated to lead to the exclusion of the evidence. It remains possible that the violation of the rights of a third party might also lead to exclusion under this provision. The jurisprudence of *Lubanga* sheds some light on this question. In *Lubanga*, the Trial Chamber explained that its determination might differ based on the rights holder—namely, whether it was the accused's right to privacy that was violated or whether it was the right to privacy of a third party.[188] Thus, if the prosecution seeks to admit evidence obtained by hacking or leaking, the Chambers will consider whether it was an ICC investigator or an agent of the ICC that committed the violation. In the data breach scenario, for example, the right to privacy violated is that of the user whose data was exposed, as well as the corporation in possession of the data. Unless the accused was one of those users or the custodian, this violation of a third party right might not trigger Article 69(7), or it might not be seen as equally grave and meriting exclusion.

In *Bemba et al.*, the right to privacy was discussed in the context of privileged communications, as well as the telecommunications intercepts and financial records, as mentioned above. In the case of the former, the Trial Chamber noted that such a right can only be interfered with "in accordance with the law."[189] In doing so, the Chamber provides a three-part test for assessing whether an interference with the right to privacy is in accordance with the law:

> (i) the measure or measures in question should have some basis in law; (ii) the law in question should be accessible to the person concerned and foreseeable as to its effects; and (iii) as regards foreseeability, the law must set forth with sufficient precision the conditions in which a measure may be applied, to enable the persons concerned—if need be, with appropriate advice—to regulate their conduct.[190]

187. Prosecutor v. Mbarushimana, *supra* note 154, ¶ 6.

188. *Id.* ¶ 5.

189. Prosecutor v. Bemba, ICC-01/05-01/13-1855, Decision on Requests to Exclude Dutch Intercepts and Call Data Records, ¶ 10 (Apr. 29, 2016) (citing Art. 8(2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms).

190. Prosecutor v. Bemba, ICC-01/05-01/13-1257, Decision on Kilolo Defence Motion for Inadmissibility of Material, ¶ 16 (Sept. 16, 2015); *see* Khoroshenko v. Russ., App No. 1418/04, ¶ 110 (June 30, 2015), http://hudoc.echr.coe.int/fre?i=001-156006 [https://perma.cc/BT64-4BYR]; *see also* U.N. Hum. Rts. Comm., *CCPR General Comment No. 16: Article 17 (Right to Privacy): The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, ¶¶ 3, 8, 10 (Apr. 8, 1988); Donoso v. Pan., Preliminary Objection, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶¶ 55–57 (Jan. 27, 2009).

Thus, in addition to assessing who violated the right to privacy and whose right to privacy was violated, a third consideration will be whether the violation was justified by law while applying this test. These considerations fit into the second part of the Article 69(7) test to assess what impact the violation of privacy has on the reliability of the evidence or the fairness of the proceedings.

C. Attorney-Client Privilege

If the documents are not excluded based on a lack of authenticity or a violation of the right to privacy, the opposing party could argue that the content of leaked documents is not disclosable nor admissible into evidence pursuant to Article 69(5) of the Statute. This only applies if the documents in question contain privileged information and communications between attorneys and their clients, as well as attorney work product, or are communications of a similarly privileged relationship. Therefore, even if a set of documents is admissible and not excluded under Article 69(7), the defense could challenge the documents' disclosure on the grounds that they contain privileged communications and information. This potential challenge only works, of course, if the leaked documents contain communications that could reasonably be seen as falling into a protected category—for example, communications made between lawyers and their clients or in the course of a confidential relationship producing a reasonable expectation of privacy and nondisclosure. Some of the confidential relationships that have been established as privileged in national and international jurisdictions are those "between wife and husband, clergy and communicant, psychotherapist and patient, physician and patient, and attorney and client."[191] If the leaked documents contain privileged communications, there are two additional considerations. First, who is the privilege holder and, second, has the privilege been waived?

While this might at first appear to be a narrow use case, many past leaks reveal that privileged communications, particularly those between attorneys and clients, are not uncommon.[192] In the case of Sony Pictures, the company asserted that the hacked emails contained communications privileged based on attorney-client relationship and work product protections.[193] Sony's attorney, David Boies, wrote in a

191. *Privileged Communication: Further Readings*, L. Libr.–Am. L. & Legal Info., https://law.jrank.org/pages/9428/Privileged-Communication.html [https://perma.cc/H4G6-5UE6].

192. Anne E. Conroy, *Reevaluating Attorney-Client Privilege in the Age of Hackers*, 82 Brook. L. Rev. 1817, 1823 (2017).

193. Sweeny, *supra* note 91.

letter to media outlets that "the stolen data includes, but is not limited to, documents and information protected under US and international legal doctrines protecting attorney-client privileged communications, attorney work product, and related privileges and protections."[194] In the Ashley Madison case, the company argued that leaked communications between its parent company and its lawyers were confidential attorney-client communications and thus protected by privilege.[195] Even if they were widely disseminated, it argued, "stolen documents do not lose their privileged status because they are published without the consent of the privilege holder."[196]

In addition to the incidental disclosure of attorney-client communications and attorney work product in big leaks, there is the example of the Panama Papers, a case in which the entire trove of documents came from a law firm and could arguably be protected as privileged communications. This issue was raised when the U.S. Department of Justice indicted four individuals based on information in the Panama Papers in December 2018.[197] The documents from the Panamanian law firm contained sensitive personal information about the firm's clients as well as privileged communications between the clients and the firm's lawyers.

One key exception to the protection of attorney-client privilege is if the lawyer is in any way implicated in the crime or the communications are in furtherance of a crime—an issue that has been addressed at the ICC. The ICC encountered this issue of the admissibility of communications between counsel and accused persons in *Prosecutor v. Bemba et al.*, a case in which Mr. Bemba and others were charged with offenses against the administration of justice emerging from the conduct of Bemba and his counsel in the main trial *Prosecutor v. Bemba*.[198] The defense argued that the prosecution's acquisition of privileged communications violated Articles 67(1)(b) and 69(5) of the Statute and Rules 73(1) and 81(1) of the Rules.[199] In this instance, the questioned materials were not excluded because the Trial Chamber affirmed the decision of the Single Judge, who determined that the communications were in

194. *Id.*

195. Elaine Lee, Carolyn S. Toto & Kimberly Buffington, *From Ashley Madison to the Panama Papers: Is Hacked Data Fair Game?*, Internet & Soc. Media L. Blog (Apr. 22, 2016) https://www.internetandtechnologylaw.com/ashley-madison-panama-papers-is-hacked-personal-data-fair-game [https://perma.cc/5RVX-D7S8].

196. *Id.*

197. *See* Hou et al., *supra* note 63.

198. Prosecutor v. Bemba, ICC-01/05-01/13-2351, Judgement on the Appeal, ¶ 5 (Nov. 27, 2019); Jonas Nilsson, *Prosecutor v. Bemba et al.*, 112 Am. J. Int'l L. 473, 475 (2018).

199. Prosecutor v. Bemba, ICC-01/05-01/13-1257, Decision on Kilolo Defence Motion for Inadmissibility of Material, ¶ 10 (Sept. 16, 2015).

furtherance of a crime and, therefore, were exempt from professional privilege.[200] In addition, materials were admitted because safeguards, such as the appointment of an independent counsel to separate privileged from nonprivileged materials, were in place.[201]

In the case of leaked documents containing potential privileged communications, the Chamber could appoint an independent counsel to review the documents and determine whether they contain privileged information. This step would be more symbolic in the case of publicly available documents, but it would nevertheless serve to acknowledge the importance of safeguarding this privilege. In addition, the Chamber might want to consider whether the charges could be proved without these documents or whether the case depends on their admission. While there exists limited guidance to predict what the Chambers would do in this scenario, the ICC has consistently opted for an admit-all approach. Therefore, while common law jurisdictions like the United States might be more likely to respect privilege despite public exposure, the ICC could determine that it is in the interests of justice to consider the contents of the documents holistically with other evidence, whether or not they ultimately rely on them in the final judgment.

D. National Security Privilege

Finally, the party opposing admissibility can argue that leaked documents are not disclosable, and therefore not admissible into evidence, pursuant to Article 72(4) of the Statute, because they contain classified or sensitive information that could jeopardize a state's national security interests. Beyond attorney-client privilege, leaked documents might contain classified or sensitive government documents that a state would want to protect. Leaks of private government documents are quite common,[202] and it is likely that a state would try to assert state

200. *Id.* ¶ 12; Situation in the Cent. Afr. Rep., ICC-01/05-52-Red2, Decision on the Prosecutor's "Request for Judicial Order to Obtain Evidence for Investigation Under Article 70, ¶¶ 3–5; *see also* Prosecutor v. Bemba, ICC-01/05-01/13-408, Decision on the Filing in the Record of the Items Seized Upon the Searches of the Person and Cell of Jean-Pierre Bemba Gombo, at 5 (May 19, 2014).

201. Prosecutor v. Bemba, ICC-01/05-01/13-1257, Decision on Kilolo Defence Motion for Inadmissibility of Material, ¶ 13 (Sept. 16, 2015).

202. Many countries have experienced public disclosures of classified information. *See, e.g.*, Ellyne Phneah, *Anonymous, Hacktivists Helped WikiLeaks With 'Syrian Files'*, ZDNET (July 9, 2012), https://www.zdnet.com/article/anonymous-hacktivists-helped-wikileaks-with-syrian-files [https://perma.cc/VM6U-AG8A]; David Manning, *The Secret Downing Street Memo*, The Sunday Times (July 23, 2002), https://web.archive.org/web/20110723222004/http://www.timesonline.co.uk/tol/news/uk/article387374.ece; *The Hamood-ur-Rahman Commission Report*, Story of Pak. (June 1, 2003), http://storyofpakistan.com/the-hamood-ur-rahman-commission-report [https://perma.cc/Y73H-YHB3].

secrets privilege or more general national security privilege if it or one of its citizens is implicated in a case.

In the United Kingdom, the case of *R (Bancoult) v. Secretary of State for Foreign and Commonwealth Affairs (No 3) [2018]* addressed the admissibility of a leaked Wikileaks cable as evidence in a dispute over the legality of a marine-protected area in the British Indian Ocean Territory. The UK Supreme Court held that the cable was, in fact, admissible as evidence before the Court:

> The Court determined that, on the balance of probability, the document was unlikely to have remained part of the archives of the London mission or to have been leaked from there. It was further held that the document's "inviolable" status could potentially be lost due to a document from the mission archive coming into the public domain, albeit that each case would need to be determined on its facts following, by analogy, the reasoning around the law of confidentiality.[203]

Article 72(4) states that if a state learns that its documents are being disclosed at any stage of the proceedings and believes the disclosure will prejudice its national security interests, then the state has the right to intervene. Depending on the content of any hacked or leaked evidence, the opposing party could benefit from reaching out to the state in question so that the state intervenes to block the disclosure.

At the ICC, the state itself could also assert this privilege. However, it is unclear whether a state can claim national security privilege for documents that are already technically in the public domain. Even if the hacked or leaked documents are classified and contain sensitive information, the national security interest comes from their public disclosure, not their use as evidence or disclosure to the defense, since the defense already has access to the information. This issue could come up in a situation in which the OTP tries to acquire documents that have been leaked directly from the state source. In such an instance, the state could argue that what is public is not authentic and that they cannot share the actual documents because of national security despite their duty to cooperate with the prosecution.[204] As researcher Edward Liu explains, "Whether the assertion of the state secrets privilege is fatal to a particular suit, or merely excludes privileged evidence from further

203. Emma Dowden-Teale & Joanna Howard, *A "Phenomenon of Our Time": When Are Intelligence Leaks Admissible in Court?*, The L. of Nations (Feb. 26, 2018), https://lawofnationsblog.com/2018/02/26/phenomenon-time-intelligence-leaks-admissible-court [https://perma.cc/YY9R-Z6PY].

204. *See* Rome Statute, *supra* note 134, art. 86 ("States Parties shall, in accordance with the provisions of this Statute, cooperate fully with the Court in its investigation and prosecution of crimes within the jurisdiction of the Court.").

litigation, is a question that is highly dependent upon the specific facts of the case."[205]

Conclusion

Online leaks, whether the result of legitimate whistleblowing, unauthorized leaking, or illegal hacking, fit the definition of open source information; and yet, there is something inherently different about information in the public domain that was not *intended* to be public. While international and domestic laws recognize the importance of protecting private information, there is a reality that, once public, it is difficult to put information back behind a veil of privacy. The dissemination of incriminating information obtained by a third party through unauthorized or illegal means, and then made public, creates a complex situation. On one hand, the illegal method of acquisition should not be rewarded. On the other hand, openly exposed illegal acts should not go unpunished. The public interest argument cuts both ways.

While a common test for deciding the admissibility of unlawfully obtained digital evidence has yet to be developed,[206] some overarching principles have formed in the time between the founding of WikiLeaks in 2006 and today, when "WikiLeaks evidence" has become a common term of reference.[207] These principles can be used by investigators and lawyers to develop their own thinking about how to consider hacked and leaked information.

A. The Slippery Slope of Agency

Unlawfully obtained evidence is not automatically inadmissible. If Article 69(7) applies only if the violation is committed by an OTP investigator or an agent of the OTP, then information hacked and leaked by a third party should be admissible. Therefore, based on the Trial Chamber's interpretation of the Rules, the prosecution can admit leaked documents into evidence, so long as they did not order, elicit, or solicit the illegal conduct in any way. However, accepting that simple

205. Edward C. Liu & Todd Garvey, Cong. Rsch. Serv., Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act 1–2 (2016).

206. Blair & Gojković, *supra* note 24, at 235.

207. Harriet Cornell, *WikiLeaks Evidence in Court*, Glob. Just. Blog (June 13, 2014), https://www.globaljusticeblog.ed.ac.uk/2014/06/13/wikileaks [https://perma.cc/9NBC-LC94]; Isabella Bogunovich, *I Object! The Use of WikiLeaks Evidence in International Courts and Tribunals*, Perth Int'l L.J. (Aug. 21, 2016), https://www.perthilj.com/blog/2019/2/19/i-object-the-use-of-wikileaks-evidence-in-international-courts-and-tribunals [https://perma.cc/P33C-MEDJ].

interpretation fails to grasp the complex reality in which such lines may be blurred. With vigilante and hacktivist groups like Anonymous paying attention to the evidentiary gaps in high profile criminal cases as they did in the Steubenville rape case, as well as informal and anonymous avenues through which law enforcement can communicate their investigative needs to persons not bound by the same rules, there is an expanding gray area around the idea of agency. While the ICC Prosecutor is unlikely to encourage hackers, even jokingly, to illegally acquire documents as President Trump did with Hillary Clinton's emails, it is certainly possible that a public statement by the Prosecutor about her inability to acquire evidence through state cooperation might influence civil society groups to take the initiative to retrieve the missing evidence on her behalf. While this might not seem all that problematic the first time it happens, this might be viewed differently once the Prosecutor is on notice that hackers will act on her statements, especially if it becomes a pattern.

The prosecution should not be punished for or disadvantaged by the acts of a third party, but there must be safeguards to prevent the perilous, unintended consequences of agency relationships in a digital gray zone. One such safeguard could be a rule similar to the United States' Brady rule that would require the prosecution to disclose any information about their relationship or past communications with any third party involved in unlawful acquisition of private documents. Otherwise, leniency on admissibility could become a motivator for people to hack information in the service of the prosecution, even without being ordered to do so directly. Therefore, legislators and judges must carefully consider the incentive structure created by future decisions around admissibility of hacked and leaked information.

B. The Fair Evaluation of Evidence

While the first question raised with unlawfully obtained evidence is whether or not it is admissible because of a procedural violation, when it comes to online leaks, the more pertinent question will often be whether authenticity can be established. The increase in digital disinformation and deepfakes means that the judges' role as gatekeeper is more important than ever. Hacked and leaked documents downloaded directly from the internet should not be admitted without further investigation and additional authenticating information. In this sense, the ICC judges' preference for the civil law "free evaluation of evidence" approach presents extreme risks to the fairness of proceedings in the Digital Age.

If the documents can be obtained from their original source, that step should be taken whenever possible. When it comes to the submission of leaked documents, the proffering party has the burden of explaining their provenance and reliability. In order to verify hacked and leaked digital documents, an expert should analyze the content of the documents, the source of the documents, and the technical aspects of the document such as filetype and metadata. The testimony of lay witnesses and expert witnesses, therefore, should play an important role in interpreting and authenticating online leaks. Thus, it is recommended that judges favor the submission of this type of material through a witness rather than a bar table[208] and allow for the time and space for evidentiary hearings before or during the trial proceedings.

C. The Importance of Context

All parties to legal proceedings benefit from evidentiary laws that are clear and predictable. At the same time, this need for clarity must be balanced with the recognition of multifaceted situations where the interests of justice are supported by fact-specific assessments. Judges will have to grapple with the nuanced scenarios of online leaks by legitimate whistleblowers, illegal leakers, unknown leakers, and known and unknown hackers. Numerous significant questions are relevant to the decision making, including: Did anyone engage in illegal conduct, and if so, who? Who benefits from the admission of evidence?[209] Who suffers from the exclusion of evidence? What is the relationship between the beneficiary and the hacker/leaker? Whose rights were violated? Is the material privileged and, if so, who can waive the privilege?

Approaches to the admissibility of evidence in different legal systems provide insights into their values and priorities. The lack of consistency on the approach to admissibility of unlawfully obtained evidence across jurisdictions (and sometimes within the same jurisdiction) reflect the sometimes-conflicting notions of the search for the truth, the protection of rights, and the fairness of proceedings. If the rules are to remain flexible, significantly more guidance is needed on how the rules apply to various sets of facts. In order to convey this guidance in a meaningful way, ICC Trial Chambers must present clear and thorough reasoning behind their evidentiary decisions in terms of admissibility

208. A bar table document is a document that have been admitted into evidence without having been introduced during the examination of a witness. *See* Off. of Pub. Counsel for Victims, ICC, *Representing Victims Before the International Criminal Court: A Manual for Legal Representatives* (2019), https://www.icc-cpi.int/iccdocs/opcv/manual-victims-legal-representatives-fifth-edition.pdf [https://perma.cc/S97A-9GLW].

209. Blair & Gojković, *supra* note 24, at 259.

and weight. In order for investigators to know how the rules will apply to their actions during an investigation and to the evidence they collect, consistency and some degree of binding precedent will provide much needed predictability. The holistic assessment of evidence avoids grappling with complex issues presented by individual items of evidence at a time when such head-on engagement is important and necessary.

D. The Protection of Privacy Rights

While the pursuit of the truth is paramount to international justice processes, it is equally important that such institutions respect and protect human rights. In general, the inquisitorial approach of civil law systems often prioritizes truth, whereas the accusatorial tradition of common law systems often prioritizes fairness.[210] This tension is at the crux of exclusionary rules based on rights violations. The hybrid approach adopted by ICL courts and tribunals such as the ICC has the benefit of flexibility but also presents the danger of unpredictability and inconsistency.

The admission of leaked documents could prejudice the rights of the accused in a number of different ways, including the right to confront opposition witnesses, the right to a public trial, and the right to a competent defense. If leaked documents are not properly authenticated, their admission could also prejudice the fairness of the trial and the legitimacy of the proceedings. Alternatively, the exclusion of leaked documents could prejudice the prosecution and deny victims justice. At a time when privacy is under threat and data protection laws are developing rapidly as a result, the ICC has an opportunity to contribute to the development of jurisprudence around the protection of privacy in the Digital Age. While national and regional data protection laws might not apply to the ICC, particularly because of the immunity afforded to certain international organizations, the Court should nevertheless be aware of and seek consistency with laws designed to protect digital privacy. In carrying out its mandate to prosecute the most serious crimes that are of concern to the international community, the ICC should place human rights and digital rights at the center of its work.

E. The Power of Community

Finally, international criminal courts and tribunals should learn from the innovative model developed by the ICIJ to review and analyze the Panama Papers. While the wider international justice and human

210. A. Lawrence Lowell, *The Judicial Use of Torture. Part I*, 11 Harv. L. Rev. 220, 223 (1897).

rights community should not be used to circumvent procedural rules by which professional investigators and prosecutors are bound—for example, by hacking and leaking documents—their assistance should be welcomed in the process of preserving and processing the increasingly large volumes of potentially relevant information that are uploaded to the internet on a daily basis. The ICC and other ICL courts and tribunals do not have the resources or manpower necessary to tackle these challenges on their own. Therefore, they will benefit most by viewing civil society not as agents to skirt restrictions on their work, but rather as equal partners and collaborators in the pursuit for accountability and justice.

The issues articulated above highlight some, but not all, of the challenges to come as more and more hacked and leaked material is offered as evidence in international criminal trials. The ability to authenticate online leaks will likely pose the greatest hurdle to admissibility. While the illegal means of acquisition might be considered in a court's assessment of online leaks, it will not always be a bar to their admission into the evidentiary record. Rather, concerns over protecting individuals' right to privacy, privileged communications and relationships, and classified or sensitive materials will be paramount to judicial decisions on admissibility. Finally, the diverse range of online leak scenarios, as demonstrated by the various case studies discussed in this Article, show the necessity of evidentiary hearings and the importance of clear, fact-specific judicial reasoning on issues raised by hacked and leaked evidence.