Article

The Privacy Principle

Frédéric Gilles Sourgens[†]

---

† Professor of Law & Director, Washburn University School of Law, Oil and Gas Law Center; Co-Chair, American Society of International Law Private International Law Interest Group. This article is a direct result of many stimulating discussions between the editorial committee members of the 2016 Jessup Compromis and the compromis author, as well as exchanges with fellow international rounds judges. In particular, I would like to thank Asaf Lubin, Lesley Benn, Dagmar Butte, Andrew Holmes, Lucas Lixinski, Marco Milanovic, Tariq Mohideen, David Quayat, and Stephen Schneebaum. I would also like to thank my colleague Craig Martin for thought-provoking conversations about the article, as well as Jeff Brooks and Kabir Duggal for their insightful comments on an early draft of the article. Finally, I would like to thank the participants at the Washburn University School of Law faculty workshop at which I presented the piece, particularly Andrea Boyack, Gillian Chadwick, Alex Glashauser, Emily Grant, Patricia Judd, Joseph Mastrosimone, Bill Rich, and David Rubenstein.

Near daily news reports remind us that we live in an intelligence world.[1] The U.S. National Security Agency (NSA) collects terabytes of global communications.[2] Most famously, the NSA's PRISM and UPSTREAM programs intercepted and monitored the global internet-based communications and telephone calls of foreign nationals, as well as those initiated or received by persons outside of the United States.[3] These intercepts cover everything from flirtatious emails between teenagers on distant shores to phone calls made by foreign heads of state busied in statecraft with far-flung capitals.[4] Foreign intelligence services do their best to emulate or surpass American efforts.[5] "Signals intelligence"—the collection of remote electronic communications of foreign targets—has become the coin of the security realm.[6]

---

1. *See, e.g.*, Stephen Myers & Neil MacFarquhar, *To Democrats, Email Hack Suggests Trump Has an Ally: Putin*, N.Y. TIMES (July 25, 2016), http://www.nytimes.com/2016/07/26/us/politics/kremlin-donald-trump-vladimir-putin.html (reporting alleged hacking by Russian government into Democratic National Committee database).

2. *See* Robert Stein, Walter Mondale, & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2271-75 (2016) (discussing bulk surveillance programs); *see also* Rory Carroll, *Welcome to Utah, the NSA's Desert Home for Eavesdropping on America*, GUARDIAN (June 14, 2013), http://www.theguardian.com/world/2013/jun/14/nsa-utah-data-facility (detailing the NSA's technical capabilities); Charlie Savage, *U.S. Privacy and Civil Liberty Watchdog Faces Limits in Congress*, N.Y. TIMES (July 14, 2016), http://www.nytimes.com/2016/07/15/us/us-privacy-and-civil-liberty-watchdog-faces-limits-in-congress.html (discussing attempts to weaken NSA governmental oversight).

3. Glen Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (discussing PRISM); Ashley Gorski & Patrick C. Toomey, *Unprecedented and Unlawful: The NSA's Upstream Surveillance*, JUST SECURITY (Sept. 19, 2016, 3:32 PM), https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/ (discussing UPSTREAM).

4. *See* Melissa Eddy, *File Is Said to Confirm N.S.A. Spied on Merkel*, N.Y. TIMES (July 1, 2015), https://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html (discussing NSA efforts to hack the phone of Germany's chancellor); Charlie Savage, *Letter Tells of U.S. Searches for Emails and Calls*, N.Y. TIMES (Apr. 1, 2014), http://www.nytimes.com/2014/04/02/us/politics/letter-puts-focus-on-us-searches-for-americans-emails-and-calls.html (reporting the search of personal electronic communications by the NSA).

5. *See* John Haines, *Everything Old Is New Again: Russia Returns To Nicaragua*, EURASIA REV. (July 25, 2016), http://www.fpri.org/article/2016/07/everything-old-new-russia-returns-nicaragua/ (reporting on Russian increased signals intelligence efforts).

6. *See* Samuel Rascoff, *Presidential Intelligence*, 129 HARV. L. REV. 633, 662 (2016) (discussing U.S. signals intelligence efforts); *Signals Intelligence*, NAT'L SEC. AGENCY (May 3, 2016), https://www.nsa.gov/what-we-do/signals-intelligence/.

Current news coverage also evidences why governments around the world feel compelled to collect ever-expanding troves of data. Apparently normal people commit mass murders at an alarming and growing rate—be it by running a truck through a crowd of revelers in Nice,[7] by emptying ammunition into a once-joyful crowd at an LGBT nightclub in Orlando,[8] or by bombing a peaceful demonstration for minority rights in Kabul.[9] In each of these instances, one of the first questions is: could better security have prevented this attack? Often, one of the first bits of information to surface in answer to this question concerns the internet and cellphone habits of the perpetrator.[10]

Global political discourse has made clear that intelligence gathering is only going to increase in response to the current terror threat. Under the banner of law and order, President Donald Trump has staked out extreme positions on the reach of intelligence and military assets to root out threats to the United States.[11] Fascists in France have similarly sought to claim the mantle of increased surveillance.[12] But even politicians closer to their respective mainstreams appear to concede that increased signals intelligence will inevitably form part of policies aimed at stemming the flow of radicalization, weaponry, and mass atrocities.[13] In this context, global signals intelligence practices have pushed privacy as we know it to the brink of extinction. Efforts to collect intelligence capture deeply intimate conversations of ordinary people around the world.[14] They also capture information that in most contexts would be deemed privileged and as such beyond the scope of prying eyes.[15] Yet to accept that

---

7. *See* Alissa Rubin, *ISIS Claims Truck Attacker in France Was Its Soldier*, N.Y. TIMES (July 16, 2016), http://www.nytimes.com/2016/07/17/world/europe/isis-nice-france-attack.html.

8. *See* Sheryl Stolberg, *Orlando Attack Roils Gay Community*, N.Y. TIMES (June 12, 2016), http://www.nytimes.com/2016/06/13/us/orlando-attack-roils-gay-community.html.

9. *See* Mujib Mashal & Zahra Nader, *ISIS Claims Deadly Bombing at Demonstration in Kabul, Afghanistan*, N.Y. TIMES (July 23, 2016), https://www.nytimes.com/2016/07/24/world/asia/kabul-afghanistan-explosions-hazaras-protest.html.

10. *See* Aurelien Breeden, *Attacker in Nice Plotted for Months and Had Accomplices, French Prosecutor Says*, N.Y. TIMES (July 21, 2016), http://www.nytimes.com/2016/07/22/world/europe/attacker-in-nice-plotted-for-months-and-had-accomplices-french-prosecutor-says.html (discussing the texting habits of the Nice murder).

11. *See* Patrick Healy & Jonathan Martin, *His Tone Dark, Donald Trump Takes GOP Mantle*, N.Y. TIMES (July 21, 2016), http://www.nytimes.com/2016/07/22/us/politics/donald-trump-rnc-speech.html.

12. *See* Bojan Pancevski & Richard Kerbaj, *Nice Official and Marine Le Pen Question French Resolve Against Terror*, AUSTRALIAN (July 17, 2016), http://www.theaustralian.com.au/news/world/the-times/nice-official-and-marine-le-pen-question-french-resolve-against-terror/news-story/02d561a8aa87be86ee28a02ebda0e16d.

13. *See* Nolan McCaskill, *Clinton Urges 'Intelligence Surge' to Counter Terrorist Threat*, POLITICO (June 13, 2016), http://www.politico.com/story/2016/06/hillary-clinton-national-security-224267; Jenna McLaughlin, *Senate Narrowly Rejects Controversial FBI Surveillance Expansion—For Now*, INTERCEPT (June 22, 2016), https://theintercept.com/2016/06/22/senate-narrowly-rejects-controversial-fbi-surveillance-expansion-for-now/ (noting Sen. John McCain's support for broader internet surveillance).

14. *See* Alejandro Abdo & Patrick Toomey, *The NSA Is Turning the Internet into a Total Surveillance System*, GUARDIAN (Aug. 11, 2013), https://www.theguardian.com/commentisfree/2013/aug/11/nsa-internet-surveillance-email; Robert Hackett, *No, NSA Phone Spying Has Not Ended*, FORTUNE (Dec. 1, 2015), http://fortune.com/2015/12/01/nsa-phone-bulk-collection-end/ (noting that foreign surveillance operations can continue under Executive Order No. 12333 despite the recent passage of the Freedom Act).

15. Abdo & Toomey, *supra* note 14.

such communications will be analyzed by government agents to determine who poses a security threat is to destroy the possibility of intimacy: to have communications "of a very personal or private nature" away from public scrutiny.[16]

Sacrificing privacy risks upending basic preconditions for the pursuit of a dignified life. The link between privacy and dignity is at the forefront of recent U.S. jurisprudence on sexual privacy such as *Lawrence v. Texas* and *Obergefell v. Hodges*.[17] Jurisprudential discourses across the Atlantic at least, and as this Article will show, globally, converge on the view that without privacy, "no society can maintain any form of community."[18] Both the concept of a "self" as distinct from society and of "society" as a community distinct from "selves" require privacy protections sufficient to allow meaningful discourse between "selves" through which both self and community can be constituted.[19]

The consequent need for increased regulation is not lost on commentators and government officials. Recent commentary on cyber-surveillance by President Obama's inaugural director for privacy and civil liberties, Timothy Edgar, notes that it is "no longer desirable or even possible to protect the privacy of Americans while leaving the rules for most global surveillance programs entirely to the Executive Branch."[20] In fact, the logic of Mr. Edgar's analysis goes one step further: given the global scale of surveillance programs, one needs a global solution to protect privacy everywhere.[21] Privacy in the internet age is secured globally or not at all.[22]

Problematically, existing international law approaches to the protection of global privacy rights face significant hurdles when applied to the digital age of signals intelligence, leading to an apparent normative gap in the law. As discussed in Section I.A, much of the literature focuses on human rights treaty protections of privacy rights.[23] This approach faces three major limitations: (1) territorial limitations on the scope of core treaties such as the International Covenant on Civil and Political Rights (ICCPR) make these treaties facially inapplicable to existing programs such as those reportedly conducted by the

16. *Intimate*, MERRIAM-WEBSTER COLLEGIATE DICTIONARY (11th ed. 2014).

17. Obergefell v. Hodges, 135 S. Ct. 2584, 2594 (2015); Lawrence v. Texas, 539 U.S. 558, 577 (2003).

18. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1167 (2004). Whitman's article argues that when put to the test, U.S. law does not follow such a dignity conception of law. As proof, writing in 2004, he notes that "we can declare that American gays can realistically expect only to have their liberty rights protected. The prospects for the kind of dignitary protections embodied in a law of gay marriage, we could say, are remote." *Id.* at 1221. It might well be argued that Professor Whitman's distrust of American jurisprudence and its willingness fully to embrace dignity within its mainstream has been misplaced.

19. *See* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 963, 973-74, 1006-07 (1989).

20. Timothy Edgar, *Go Big, Go Global: Subject the NSA's Overseas Program to Judicial Review*, LAWFARE (July 6, 2016, 4:48 PM), https://www.lawfareblog.com/go-big-go-global-subject-nsas-overseas-programs-judicial-review.

21. *Id.*

22. *Id.*

23. *See* Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81 (2015). For a full discussion of the literature, see *infra* Section I.A.

NSA;[24] (2) stakeholders such as China are not meaningfully included in the treaty web;[25] and (3) the treaty rights in question are subject to derogation when they are needed the most.[26] A treaty approach therefore requires additional agreement, though such agreement is unlikely to be forthcoming, as Section I.B. discusses. This problem could be overcome if the privacy protections enshrined in human rights treaties could be extended by reliance upon another source of international law to current global, extraterritorial signals intelligence programs directed at intercepting, storing, analyzing, and using electronic communications. As discussed in Section I.C., efforts have thus far focused upon customary international law as the principal candidate. This approach faces difficulties as custom relies upon the existence of state practice consistent with an international legal norm. With a field as young as digital, global communications, the use of analogies in the literature is easily contested,[27] while state practice tends to favor surveillance over privacy generally.[28]

As the current state of engagement with privacy problems at the intergovernmental and academic level shows, this gap must be filled soon. At worst, this gap invites submissions that global signals intelligence surveillance programs are presumptively permissible because they are not prohibited by any one rule of international law.[29] At best, the current state of the literature provides soft law guidance on best practices in the surveillance realm.[30] A different perspective on the issue therefore could meaningfully advance legal and policy discourses on the need for global privacy protections.

This Article therefore proposes a paradigm shift. It submits the existence of a Privacy Principle, or general principle of law protecting the right to privacy.

The Article proceeds as follows. After addressing the above problems international law faces in protecting privacy rights in Part I, Part II explains that general principles of law are a co-equal source of international law grounded in

---

24. *See* Charlie Savage, *U.S., Rebuffing U.N., Maintains Stance that Rights Treaty Does Not Apply Abroad*, N.Y. TIMES (Mar. 13, 2014), https://www.nytimes.com/2014/03/14/world/us-affirms-stance-that-rights-treaty-doesnt-apply-abroad.html.

25. *See China: Ratify Key International Human Rights Treaty*, HUM. RTS. WATCH (Oct. 8, 2013), https://www.hrw.org/news/2013/10/08/china-ratify-key-international-human-rights-treaty ("China is the only country among the permanent members of the UN Security Council not to have joined the ICCPR.").

26. Paul Schwen, *Human Rights Derogation in France in Response to Terrorism*, NAT'L SECURITY L. BRIEF (Mar. 3, 2016), http://www.nationalsecuritylawbrief.com/human-rights-derogation-in-france-in-response-to-terrorism/.

27. *See infra* Section I.C.

28. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 193 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

29. *See* Cmd. Michael Adams, *Jus Extra Bellum: Reconstructing the Ordinary, Realistic Conditions of Peace*, 5 HARV. NAT'L SEC. J. 377, 403-04 (2014) (applying the principle that no prohibition equals permission in international law).

30. *See* Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 682 (2016) ("[T]he sliding scale interpretive approach to intelligence is a normative proposal, but it contains positive elements as well, because it reflects the general direction rule-of-law states are heading.").

comparative legal research intended to fill gaps in international law.[31] Part III suggests that a critical mass of legal systems agrees upon the existence of a right to privacy thus permitting the derivation of a Privacy Principle. Part IV then explains how the Privacy Principle protects reasonable expectations of seclusion in real and virtual spaces (the home, correspondence, etc.) and in intimacy of content (marital relations, health, etc.). Finally, Part V shows how the Privacy Principle balances reasonable expectations of seclusion against the publicity interest of the intruding party and the interest of the public at large, employing a proportionality test.

The core contribution of the Privacy Principle is to fill the gap left open in international law by human rights treaty and customary international law approaches. It extends many of the same protections already advocated in the human rights context by means of a source of law more immune to the kind of technical pushback plaguing treaty and customary international law arguments.[32] It provides a platform to apply these protections to non-state actors as a matter of transnational law.[33] It further improves upon existing aspirational approaches by providing a positive basis for treating global invasions of privacy as internationally wrongful.[34] It does so by showing that privacy is indeed a central component of common law, civil law, mixed jurisdictions, Confucian, and Islamic traditions and domestic legal systems. The Privacy Principle thus proves that privacy is a global value worthy of global protection.

I. THE PRIVACY PROBLEM IN INTERNATIONAL LAW

This Part briefly appraises the current state of the global privacy literature. It begins with a review of the dominant human rights treaty privacy paradigm. It continues with an examination of possible alternative treaty bases for curtailing signals intelligence programs. It next inquires whether customary international law could be of help in protecting privacy interests. Part I concludes that there remains a gap in privacy protections: existing legal discourses can only incompletely address the challenges posed by extraterritorial signals intelligence programs in the digital world.

---

31. *See* Statute of the International Court of Justice art. 38(1)(c), *opened for signature* June 26, 1945, 59 Stat. 1051, 33 U.N.T.S. 993; *see also* HERSCH LAUTERPACHT, THE FUNCTION OF LAW IN THE INTERNATIONAL COMMUNITY 93 (rev. ed. 2011); Michael D. Nolan & Frédéric Gilles Sourgens, *Issues of Proof of General Principles of Law in International Arbitration*, 3 WORLD ARB. & MEDIATION REV. 505, 509-10 (2009); John G. Sprankling, *The Global Right to Property*, 52 COLUM. J. TRANSNAT'L L. 464, 486 (2014).

32. *See* sources cited *supra* notes 23-26.

33. *See* GRALF-PETER CALLIESS & PEER ZUMBANSEN, ROUGH CONSENSUS AND RUNNING CODE: A THEORY OF TRANSNATIONAL PRIVATE LAW 76-80 (2010) (discussing the need for transnational law in the context of global self-regulation).

34. *See* Deeks, *supra* note 30, at 682.

A. *The Human Right of Privacy Approach*

1. *The Human Rights Treaty Privacy Paradigm*

The right to privacy is codified in a number of human rights instruments.[35] Centrally, it is included in one of the most widely subscribed fundamental international human rights treaties, the ICCPR.[36] Article 17 provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[37] Article 19 adds:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals.[38]

Together, these two provisions make up the backbone of the human right to privacy as it is conceived in contemporary international law.

The ICCPR poses significant interpretive challenges.[39] It is not clear on its face what the ICCPR includes within the scope of "privacy."[40] It further does not provide concrete guidance as to what state conduct would be deemed unlawful.[41] Finally, it does not clearly define exceptions to this general rule.[42] All three questions—what is "private," what constitutes an unreasonable intrusion by the state into a person's private sphere, and what may excuse an otherwise unlawful intrusion—have been discussed in jurisprudence and scholarship.[43]

According to these sources, privacy protection extends to any personal information to which one would develop a reasonable expectation of freedom of intrusion.[44] The fulcrum of this reasonable expectation first requires that con-

---

35. American Convention on Human Rights art. 11, Nov. 29, 1969, 1144 U.N.T.S. 123; European Convention on Human Rights art. 8, Nov. 4 213 U.N.T.S. 221 [hereinafter ECHR]; G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. 12 (Dec. 10, 1948).

36. International Covenant on Civil and Political Rights art. 17(1), Dec. 16, 1966, S. TREATY DOC. No. 95-20, 999 U.N.T.S. 171 [hereinafter ICCPR].

37. *Id.*

38. *Id.* art. 19.

39. Milanovic, *supra* note 23, at 101 (discussing the importance of the ICCPR for the human right to privacy).

40. ICCPR, *supra* note 36, art. 19.

41. *Id.*

42. *Id.*

43. *See infra* notes 389-94 and accompanying text.

44. *See* Jordan Paust, *Can You Hear Me Now?: Private Communications, National Security, and the Human Rights Disconnect*, 15 CHI. J. INT'L L. 612, 628-29 (2015) (developing a "reasonable

duct is substantively personal.[45] Centrally, the ICCPR deems thoughts and opinions, religious beliefs, health, family relationships, friendships, and sexual encounters between consenting adults all sufficiently within the scope of substantively personal matters.[46] It is reasonable to extend such protections to the personal preparations lawfully taken to engage the public in political discourse, artistic expression, or commercial intercourse.[47]

Second, expectations are reasonable when a person acts in a non-public space.[48] The home is the quintessential non-public space.[49] Similarly, items or activities carried on one's person are typically deemed non-public,[50] as well as effects or activities in areas in which a person has the right to exclude others (say a hotel room or business premises).[51] Finally, the ICCPR expressly extends privacy protections to correspondence.[52]

At a minimum, the state must inform persons living under its jurisdiction of how, where, and why it will intrude upon otherwise non-public spaces and which types of information the state will gather.[53] This allows individuals to form minimum expectations of privacy and to adapt their behavior in response to transparent and well-justified programs.[54]

---

expectation of privacy" approach in the context of communications). *But see* Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SECURITY L. & POL'Y 179, 193-94 (2011) (noting that the text of the ICCPR does not define a clear zone of expectation of privacy).

45. *See* Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 L. & CONTEMP. PROBS. 231, 233 (2015) (noting that the human right to privacy attaches to personal information); George E. Edwards, *International Human Rights Challenges to the New International Criminal Court: The Search and Seizure Right to Privacy*, 26 YALE J. INT'L L. 323, 331 (2001) (discussing the link between privacy, autonomy, and intimacy).

46. *See* G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 911-14 (2013) (providing a similar list of personal matters as reflected in the literature); Nadine Strossen, *Recent U.S. and International Judicial Protection of Individual Rights: A Comparative Legal Process Analysis and Proposed Synthesis*, 41 HASTINGS L. J. 805, 843 (1990) (noting the European Commission's expansive interpretation of the right to privacy as protecting the right to establish and maintain relationships with other human beings).

47. *See* F. Jay Dougherty, *Foreword: The Right to Publicity – Towards a Comparative and International Perspective*, 18 LOY. L.A. ENT. L.J. 421, 437 n.116 (1998) (noting that privacy and freedom of expression in Quebec including artistic expression); Strossen, *supra* note 46, at 843 (noting the expansive right of privacy to protect the right to establish and maintain relationships with other human beings); Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, 26 HARV. J.L. & TECH. 165, 170 (2012) (noting the importance of privacy on Facebook "precisely because of its important role" in "facilitating social interaction and political discourse").

48. *See* Edwards, *supra* note 45, at 331, 395 (noting the protection of the home and other non-public spaces).

49. *See* ICCPR, *supra* note 36, art. 17(1); Edwards, *supra* note 45, at 390-91 (discussing the legal origins of the inviolability of the home).

50. *See supra* note 84 and accompanying text.

51. *See* Milanovic, *supra* note 23, at 122 (noting that intrusion into a person's hotel room would violate ICCPR privacy protections).

52. *See* Human Rights Comm., General Comment 16, Twenty-second session, 1988, para. 8 U.N. Doc. HRI/GEN/1/Rev.1 (1994) (hereinafter General Comment 16); *see also* Paust, *supra* note 44, at 628-29 (noting the absolute expectation of privacy in the context of sealed correspondence and analyzing its implications in the digital age using an expectation of privacy approach).

53. *See* General Comment 16, *supra* note 52, para. 10; *see also* Craig Martin, *Kiobel, Extraterrioriality, and the "Global War on Terror,"* 28 MD. J. INT'L L. 146, 155 (2013) (explaining exercises of jurisdiction in international law).

54. *See* Maj. Peter Beaudette Jr., *Compliance Without Credit: The National Security Agency and the International Right to Privacy*, 73 A.F. L. REV. 25, 40-46 (2015) (stressing the importance of

Such information about the existence and scope of governmental programs alone is insufficient to bring them into compliance with human rights obligations.[55] Rather, the state's *unreasonable* intrusion of privacy is unlawful even if it is fully disclosed ahead of time.[56] No state could be permitted to observe sexual acts performed within its territory simply by advertising its intention to do so without running afoul of privacy protections.[57] Rather, the state may only curtail privacy rights in the penumbras of private and public space and may not obliterate an individual's right to engage in a fruitful private life by entirely defining private spaces out of existence.[58] In other words, the state must permit persons a reasonable safe-harbor within which they can interact with each other away from prying eyes.[59]

Human rights treaty norms remain sensitive to national security needs.[60] Thus, the state may intrude upon otherwise private conduct to the extent proportionate with specific threats, as long as the process leading to the intrusion otherwise complies with basic norms of due process.[61] This proportionality analysis typically requires that the state respond with particularity to a specific danger rather than engage in dragnet intelligence collection.[62]

2. *The Asserted Territorial Limitation of Human Rights Law*

One core challenge for the human rights treaty paradigm is the objection lodged by the United States that human rights instruments have purely territorial application.[63] Given the United States' current technological capabilities,

---

foreseeability in human rights privacy jurisprudence); James D. Fry, *Privacy, Predictability, and Internet Surveillance in the U.S. and China: Better the Devil You Know?*, 37 U. PA. J. INT'L L. 419, 440 (2015) ("In general, the law needs to be crafted with adequate precision so that people can adjust their conduct in order to comply with the law, and the law must be knowable by the public, which are basic characteristics of law in general.").

55. *See* Berta E. Hernandez-Truyol, *Querying* Lawrence, 65 OHIO ST. L.J. 1151, 1175-76 (2004) (noting human rights jurisprudence confirming that the definition of privacy is not a matter of purely domestic concern and thus subject to international review).

56. *See* Carlos Torres et al., *Indiscriminate Power: Racial Profiling and Surveillance Since 9/11*, 18 U. PA. J. L. & SOC. CHANGE 283, 305 (2015) (noting jurisprudence that intrusion into privacy must be substantively reasonable).

57. *See* Aaron Fellmeth, *State Regulation of Sexuality in International Human Rights Law and Theory*, 50 WM. & MARY L. REV. 797, 809 (2008) (noting that jurisprudence confirms that intrusion into the most intimate areas of a person's life such as sexuality requires particularly serious reasons).

58. *See* Hernandez-Truyol, *supra* note 55; Torres et al., *supra* note 56; Fellmeth, *supra* note 57.

59. *See* sources cited *supra* note 36.

60. *See* Milanovic, *supra* note 23, at 139 (noting deference to states on national security interests in the human rights context).

61. *See* Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 305-06 (2015) (discussing the European-based proportionality paradigm of privacy limitations and articulating alternative bases to limit privacy rights); Fry, *supra* note 54, at 442-43 (adopting a proportionality test); Elizabeth B. Ludwin King, *A Conflict of Interests: Privacy, Truth, and Compulsory DNA Testing for Argentina's Children of the Disappeared*, 44 CORNELL INT'L L.J. 535, 553 (2011) (same).

62. *See* Milanovic, *supra* note 23, at 137 (noting ECtHR jurisprudence on proportionality to this effect).

63. *See* Margaret L. Satterthwaite, *Rendered Meaningless: Extraordinary Rendition and the Rule of Law*, 75 GEO. WASH. L. REV. 1333, 1353 (2007) (noting consistent U.S. practice regarding territorial application of human rights treaties).

such an objection creates practical problems for global privacy rights. A better understanding of the formal legal basis for the objection is therefore indispensable to developing global privacy rights.

Contemporary global signals intelligence programs can operate entirely outside of the territory of a signatory state.[64] Due to the nature of the internet, this is true even for surveillance of a state's own nationals.[65] Some are therefore concerned that such signals intelligence is beyond the reach of the privacy protections codified in the ICCPR.[66]

The dominant view of international courts and tribunals interpreting human rights treaties is that human rights treaty obligations apply globally. In the *Legal Consequences of the Construction of a Wall* Advisory Opinion, the International Court of Justice (ICJ) interpreted the geographic scope of the ICCPR as codified in Article 2(1).[67] Article 2(1) states that the treaty imposes obligations upon a state party with regard to "all individuals within its territory and subject to its jurisdiction."[68] The ICJ observed that "while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory," and ruled that "[c]onsidering the object and purpose of the International Covenant on Civil and Political Rights, it would seem natural that, even when such is the case, States parties to the Covenant should be bound to comply with its provisions."[69] In doing so, the ICJ expressly endorsed the "constant practice of the Human Rights Committee" tasked with the interpretation and application of the ICCPR.[70]

The interpretation of the ICCPR by the ICJ and the U.N. Human Rights Committee is consistent with jurisprudence by bodies interpreting regional human rights treaties such as the European Convention on Human Rights and the American Convention on Human Rights. The European Convention facially

64. *See* Stein et al., *supra* note 2 (discussing the limitations of current territoriality-based regulation of U.S. cyber-surveillance programs); Carly Nyst, *US-Based Surveillance and Data Collection: New UN Report Provides Guidance on PRISM*, PRIVACY INT'L (June 12, 2013), https://www.privacyinternational.org/node/185 (discussing the extraterritorial application of surveillance laws in the context of PRISM).

65. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 325, 326 (2015) ("An e-mail sent from Germany, for example, may transit multiple nations, including the United States, before appearing on the recipient's device in neighboring France. Contact books created and managed in New York may be stored in data centers in the Netherlands. A document saved to the cloud and accessed from Washington, D.C., may be temporarily stored in a data storage center in Ireland, and possibly even copied and held in multiple places at once. These unique features of data raise important questions about which "here" and "there" matter; they call into question the normative significance of longstanding distinctions between what is territorial and what is extraterritorial. Put bluntly, data is destabilizing territoriality doctrine.")

66. *See* Milanovic, *supra* note 23, at 110.

67. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).

68. ICCPR, *supra* note 36, art. 2(1).

69. *Legal Consequences of the Construction of a Wall*, 2004 I.C.J. at 176.

70. *Id.*; *see also* Human Rights Comm., Lopez v. Uruguay, Communication No. R.12/52: Uruguay, 12.3, U.N. Doc. A/36/40 (July 29, 1981) (rejecting a purely territorial interpretation of ICCPR as "unconscionable"); Human Rights, Comm., Gen. Cmt. 31, Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13, ¶ 10 (Mar. 29, 2004) (rejecting a purely territorial interpretation of ICCPR).

applies to "everyone within [the High Contracting Parties'] jurisdiction."[71] When the European Court of Human Rights (ECtHR) has been asked to define whether "jurisdiction" extends to protect persons residing outside a Contracting Party's territory, but whose data has been routed through the Contracting Party's territory, it has been willing to find liability for violation of the right to privacy.[72] Similar results tend to be obtained under the jurisprudence of the Inter-American Court of Human Rights.[73] International organizations have adopted similar positions outside of the judicial or quasi-judicial context providing a reasonable basis to imply a growing state practice of supporting this interpretation of human rights instruments.[74]

If this position were adopted, privacy rights could be secured against state intelligence collection through further interpretation and application of human rights treaties. Privacy rights developed predominantly in the context of invasions of privacy within a state's territorial boundaries could easily be applied to the extraterritorial conduct of states.

The core problem for such an approach is that the United States has rejected the extraterritorial application of privacy protections in human rights treaties such as the ICCPR.[75] As noted by the ICJ in the *Wall* advisory opinion, Article 2(1) of the ICCPR has two potential interpretations: one which was finally endorsed in the advisory opinion itself as discussed above, and an alternative interpretation that the provision "cover[s] only individuals who are both present within a State's territory and subject to that State's jurisdiction."[76] The United States has adopted this second approach to the ICCPR.[77] It submits that the "and" between "territory" and "subject to its jurisdiction" in Article 2(1) is

---

71. ECHR, *supra* note 35, art. 1.

72. *See, e.g.*, Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R. (2008); *see also* Milanovic, *supra* note 23, at 127 ("In . . . *Liberty and Others v. the United Kingdom*, two of the applicants were Irish organizations that communicated with a British one, and their communication was allegedly intercepted in the United Kingdom. Neither the U.K. government nor the Court *proprio motu* considered that an Article 1 jurisdiction issue arose with respect to the Irish applicants—that is, they both assumed that the ECHR applied, and the Court went on to find a violation of Article 8." (footnote omitted)).

73. Milanovic, *supra* note 23, at 114, n.135 (citing Decision on Request for Precautionary Measures: Detainees at Guantanamo Bay, Inter-Am. Comm'n H.R., Cuba, 41 I.L.M. 532 (2002); Coard v. United States, Case 10.951, Inter-Am. Comm'n H.R., Report No. 109/99, ¶ 37 (1999); Alejandre v. Cuba, Case 11.589, Inter-Am. Comm'n H.R., Report No. 86/99, ¶ 23 (1999); Saldaño v. Argentina P, Inter-Am. Comm'n H.R., Report No. 38/99, ¶¶ 15-23 (1999)).

74. Freedom of Expression and the Internet, Inter-Am. Comm'n H.R. Report No. 11/13, OEA/Ser.L/V/II., 57-79 (2013), http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.

75. *See Second and Third Periodic Reports of the United States of America to the UN Committee on Human Rights Concerning the International Covenant on Civil and Political Rights*, U.S. DEP'T STATE, at annex I (2005), http://www.state.gov/j/drl/rls/55504.htm#annex1.

76. Legal Consequences of the Construction of a Wall, 2004 I.C.J., at 179.

77. ICCPR, *supra* note 36, art. 2(1). For the development of the U.S. position, see Michael J. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, 99 AM. J. INT'L L. 119, 123-24 (2005) (quoting UN Docs. E/CN.4/SR.193, at 13, 18 (1950), E/CN.4/SR.194, at 5, 9 (1950) (statements of Eleanor Roosevelt)). *See also* RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW: JURISDICTION § 203 (Am. Law Inst., Tentative Draft No. 2, 2016) (codifying the territoriality presumption of federal statutes); Martin, *supra* note 53, at 204-05 (discussing inconsistencies in this presumption in the so-called war on terror).

a conjunction rather than disjunction.[78] The ICCPR applies only if both elements (territory and jurisdiction) are established.[79] Consequently, global or extraterritorial conduct is not within the scope of the ICCPR.[80] Adding further complication, the United States has not acceded to the additional protocol to the ICCPR that would require it to submit disputes concerning the application and interpretation of the ICCPR to an international body, the Human Rights Committee.[81] The jurisprudence of that body therefore has limited authority when invoked against the United States.[82]

Recent U.S. Legal Advisers to the State Department have attempted to move the U.S. position with regard to the extraterritorial application of general human rights treaties. As noted by then-Legal Adviser of the United States State Department Harold Koh, the global consensus regarding the application of the ICCPR is that it is not limited to the territory of the signatory state.[83] Harold Koh consequently sought to change the U.S. position on the extraterritorial application of the ICCPR.[84] Although the weight of scholarly authority stands with Harold Koh's position,[85] this attempt has at least formally failed.[86]

---

78. ICCPR, *supra* note 36, art. 2(1)

79. U.S. DEP'T STATE, *U.S. Observations on Human Rights Committee General Comment* 31 (2007), http://2001-2009.state.gov/s/l/2007/112674.htm ("[B]ased on the plain and ordinary meaning of its text, this Article establishes that States Parties are required to ensure the rights in the Covenant only to individuals who are both *within* the territory of a State Party *and* subject to that State Party's sovereign authority." (emphasis in original)).

80. *Id.*

81. U.N. HUM. HIGH RTS. COMMISSIONER, *Status of Ratification*, http://indicators.ohchr.org (noting that the United States is not a member of the first protocol to the ICCPR).

82. *See* Optional Protocol to the International Covenant on Civil and Political Rights art. 1, *opened for signature* Dec. 19, 1966, 999 U.N.T.S. 171 ("A State Party to the Covenant that becomes a Party to the present Protocol recognizes the competence of the Committee to receive and consider communications from individuals subject to its jurisdiction who claim to be victims of a violation by that State Party of any of the rights set forth in the Covenant.").

83. Memorandum from Harold Koh, Office of the Legal Adviser of the U.S. Dep't State (Oct. 19, 2010), https://www.justsecurity.org/wp-content/uploads/2014/03/state-department-iccpr-memo.pdf ("[A]n interpretation of Article 2(1) that is truer to the Covenant's language, context, object and purpose, negotiating history, and subsequent understandings of other States Parties, as well as the interpretations of other international bodies, would provide that in fact, the Covenant does impose certain obligations on a State Party's extraterritorial conduct under certain circumstances.").

84. *Id.*

85. *See* Oona Hathaway et al., *Human Rights Abroad: When Do Human Rights Obligations Apply Extraterritorially?*, 43 ARIZ. ST. L.J. 389, 395 (2011) (discussing the weight of scholarly authority on the extraterritorial application of the ICCPR); Milanovic, *supra* note 23, at 108-09 (also discussing the weight of scholarly authority on the extraterritorial application of the ICCPR).

86. *See* U.N. Human Rights Comm., Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 4, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014) [hereinafter Human Rights Committee Fourth Periodic Report of the United States] (expressing the Committee's regret that the United States maintains its territorial interpretation of ICCPR's applicability). An argument could be made that the United States responded to international legal criticism of its NSA UPSTREAM and PRISM programs. *See* Human Rights Committee Fourth Periodic Report of the United States, *supra* (outlining criticism); SIGNALS INTELLIGENCE REFORM 2015 ANNIVERSARY REPORT, U.S. DIR. OF NAT'L INTELLIGENCE (2015), https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties (detailing changes to U.S. policy following President Obama's Presidential Policy Directive PPD-28 in January 2014); Sarah Childress, *How the NSA Spying Programs Have Changed After Snowden*, PBS (Feb. 9, 2015), http://www.pbs.org/wgbh/frontline/article/how-the-nsa-spying-programs-have-changed-since-snowden/ (discussing the 2015 Signals Intelligence Reform Anniversary Report of the U.S. Director of National Intelligence). Whether this movement was due to a sense of legal constraint or simply as a response to public pressure in light of the Snowden revelations is unclear. In any event, there is a good chance that the current administration will change course, thus limiting the probative value of this poten-

3. *The Limitations of the Human Rights Discourse*

The position of the United States has raised a significant amount of understandable scholarly consternation.[87] A significant literature has developed seeking to confirm the global consensus on the global applicability of the ICCPR.[88] Much of that literature is aimed at critiquing the shortcomings of U.S. global signals intelligence programs,[89] or their asserted compliance with human rights norms.[90]

Laudable and necessary though this literature is, it cannot convincingly provide a vehicle for international law privacy protections in the digital world. It continues to repeat the same arguments already rejected by its main audience: the United States government.[91] If Harold Koh—formerly dean of Yale Law School and leading authority on the subject matter—could not convince Secretary of State Clinton and President Obama when acting as Legal Adviser to the State Department that the ICCPR should bind United States conduct on a global scale, it is reasonably unlikely that any amount of scholarly industry could convince the United States to change its mind on the extraterritorial application of human rights protections as a matter of treaty law.[92] This literature therefore may cogently propose an alternative interpretation of human rights preferable to the U.S. approach, but it does not provide the means of overcoming existing objections.

---

tial change in U.S. state practice. *See* Natasha Lomos, *Trump Order Strips Privacy Rights from Non-U.S. Citizens, Could Nix EU-US Data Flows*, TECHCRUNCH (Jan. 26, 2017), https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/ (discussing moves by the Trump Administration to undo relevant privacy protections put in place by the Obama Administration).

87. *See, e.g.*, Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45, 46 (2016) (attacking territorial paradigms to surveillance as misguided from a U.S. law perspective); Daskal, *supra* note 65, at 330 (2015) (noting that the features of data in the internet age "call into question the normative significance of longstanding distinctions between what is territorial and what is extraterritorial" and arguing for greater international harmonization of privacy laws); Milanovic, *supra* note 23, at 108-09 (criticizing the U.S. position and summarizing international legal scholarship that also criticizes the U.S. position).

88. *See, e.g.*, Milanovic, *supra* note 23, at 108-09 (criticizing the U.S. position and summarizing international legal scholarship doing so); Daniel Joyce, *Privacy in the Digital Era: Human Rights Online?*, 16 MELB. J. INT'L L. 270, 284 (2015) (noting that, while Milanovic's work is a useful first step, more work on human rights in the data privacy context is needed).

89. *See* Ashley Deeks, *Intelligence Communities, Peer Constraints, and the Law*, 7 HARV. NAT'L SECURITY J. 1, 21 n.91 (2015) (collecting recent scholarship critical of the international legality of NSA programs).

90. *See, e.g.*, Beaudette, *supra* note 54, at 26 (arguing that existing U.S. legal constraints render NSA surveillance programs lawful); Peter Marguilies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2139 (2014) (same).

91. Human Rights Comm., Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 4, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014).

92. *Compare* Marko Milanovic, *Harold Koh's Legal Opinions on the US Position on the Extraterritorial Application of Human Rights Treaties*, EJIL: TALK! (Mar. 7, 2014), http://www.ejiltalk.org/harold-kohs-legal-opinions-on-the-us-position-on-the-extraterritorial-application-of-human-rights-treaties/ (discussing the advocacy impact of the publication of the legal opinions), *with* Savage, *supra* note 24 (noting the failure of these efforts due to security concerns).

Moreover, the damage in many ways has been done. China is not a party to the ICCPR or other human rights treaties containing a privacy protection.[93] At present, Chinese domestic public "laws do not expressly (or even implicitly) restrict the government's powers with internet surveillance, let alone when national security and public interests are involved."[94] It stands to reason that no such constraint exists extraterritorially. The current U.S. positioning on the right to privacy is unlikely to place much political pressure on China to change course.[95]

Russia, too, has a problematic track record with regard to compliance of its signal intelligence programs with robustly formulated human rights norms. The European Court of Human Rights recently reviewed a Russian program for the surveillance of mobile communications.[96] The Court held that the program was in violation of Russia's human rights obligations.[97] Russia has since moved to counteract the judgment with domestic legislation, indicating its resistance to the application of human rights norms to intelligence gathering.[98]

France has typically complied with judgments holding it liable for extraterritorial human rights abuses.[99] It is further a robust proponent for privacy rights both territorially and extraterritorially.[100] This, however, recently changed due to the mass shootings in Paris in November 2015.[101] In response, France derogated from basic privacy protections to increase the scope of all forms of surveillance programs.[102]

In sum, the United States appears to be leading a movement of state practice away from a more robust understanding of human rights privacy. This movement was partly on display in recent action by the United Nations General

---

93. *See* Sonya Sceats with Shaun Breslin, *China and the International Human Rights System*, CHATHAM HOUSE (Oct. 2012), https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/r1012_sceatsbreslin.pdf (discussing China's position).

94. Fry, *supra* note 54 , 37 U. PA. J. INT'L L. 419, 480 (2015).

95. *See China: Ratify Key International Human Rights Treaty*, HUM. RTS. WATCH (Oct. 8, 2013), https://www.hrw.org/news/2013/10/08/china-ratify-key-international-human-rights-treaty (noting that "China is the only country among the permanent members of the UN Security Council not to have joined the ICCPR").

96. *See* Roman Zakharov v. Russia, App. No. 47143/06 (Eur. Ct. H. R. Dec. 4, 2015).

97. *Id.* For a discussion of the decision, see Gabor Rona & Lauren Aarons, *State Responsibility to Respect, Protect, and Fulfill Human Rights Obligations in Cyberspace*, 8 J. NAT'L SECURITY L. & POL'Y 503, 527-28 (2016) (discussing the importance of the case for cyber security law).

98. *See Russia Passes Law to Overrule European Human Rights Court*, BBC (Dec. 4, 2015), http://www.bbc.com/news/world-europe-35007059 ("Russia has adopted a law allowing it to overrule judgements from the European Court of Human Rights (ECtHR). The vote in the Duma, Russia's lower house of parliament, came the same day as the ECtHR ruled against Russia's Federal Security Service over spying.").

99. *See* Medvedyev v. France, App. No. 3394/03, 2010-II Eur. Ct. H.R.; *see also* Hathaway, *supra* note 85, at 405-06 (discussing the case).

100. *See* Mark Scott, *France Rejects Google's Efforts to Limit Application of Privacy Ruling*, N.Y. TIMES (Sept. 21, 2015), https://bits.blogs.nytimes.com/2015/09/21/france-rejects-googles-efforts-to-limit-application-of-privacy-ruling/ (discussing Google's compliance with privacy protections and French regulatory responses).

101. For a discussion of the shootings as well as the initial French response, see Frédéric G. Sourgens, *The End of Law: The ISIL Case Study for a Comprehensive Theory of Lawlessness*, 39 FORDHAM INT'L L.J. 355, 420 (2015).

102. Schwen, *supra* note 26.

Assembly in passing a resolution on *The Right to Privacy in the Digital Age.*[103] On its face, this resolution strongly supports privacy rights in cyberspace and urges states to protect privacy rights online in the same manner as they do offline.[104] It further notes the potential danger of dragnet intelligence gathering.[105] Importantly, however, the resolution omitted language included in an earlier draft asserting that human rights obligations (and thus the right to privacy) apply extraterritorially.[106] It was this move that permitted the United States and Russia to support the resolution's ultimate passage.[107] As such, the resolution expresses concern and calls upon states to act, but stops short of supporting a broader conception of privacy rights against foreign cyber-surveillance operations. This issue thus remains unresolved and arguably unresolvable by any source of law relying directly on outward looking state practice to supply normative force.

The composition of the group led by the United States is structurally significant. It includes four of the five permanent members of the U.N. Security Council.[108] Each of these permanent members has a veto right with regard to any proposed Security Council resolution.[109] Enforcement of decisions of U.N. judicial organs by constitutional design require U.N. Security Council action, subject to the veto powers of the permanent members.[110] Given that the United States is leading a super-majority of U.N. Security Council permanent members, the view apparent in their collective conduct structurally (if not formally) trumps the contrary interpretation of human rights law announced by the ICJ.[111]

This current positioning has practical implications. In order to vindicate the existence of privacy rights vis-à-vis the United States (and consequently, the NSA) or the super-majority of U.N. Security Council permanent members, one needs to look beyond the human rights treaty paradigm.[112] One needs to find an alternative way to theorize privacy protections so as to open up a second front from which to chip away at standing objections that no global privacy

---

103. G.A. Res 68/167, Resolution on the Right to Privacy in the Digital Age (Jan. 21, 2014).

104. *Id.*

105. *Id.*

106. *See* Alex Grigsby, *UN Committee Adopts Resolution on the Right to Privacy in the Digital Age*, COUNCIL FOR. REL. (Dec. 1, 2014), http://blogs.cfr.org/cyber/2014/12/01/un-committee-adopts-resolution-on-right-to-privacy-in-the-digital-age/ ("Like last year, the first draft also implied that states' human rights obligations extend beyond their borders and jurisdiction, a position which is hotly contested.").

107. *Id.* ("It is likely that the sponsors didn't want to needlessly antagonize Russia, which is one of the few countries that protested the NetMundial outcome and is one of Brazil's BRICS partners," and that "these references [to extraterritoriality] probably constituted redlines for the Five Eyes that were removed or amended into softer language to achieve consensus on the final text."). The drafting history is also recounted in Milanovic, *supra* note 23, at 84-86.

108. *See* Current Members of the United Nations Security Council, http://www.un.org/en/sc/members/ (last visited July 26, 2016).

109. U.N. Charter art. 27, ¶ 3.

110. *Id.* art. 94, ¶ 2.

111. *See supra* note 96.

112. *See* U.N. Hum. Rts. Comm., Concluding Observations on the Fourth Periodic Report of the United States of America, ¶ 4, U.N. Doc. CCPR/C/USA/CO/4 (2014) (voicing the U.S. objection that human rights to not apply extraterritorially and thus to the NSA's global programs).

right exists.[113] Advancing the privacy argument requires a means to "over-determine" the right to privacy.[114] One must show that the United States and others like it not only ought to recognize the virtue of human rights and respect global privacy rights, but that they have already committed themselves to such international privacy norms beyond the human rights context.[115]

4. *The Value of the Human Rights Discourse*

The human rights privacy discourse has significant normative value. Privacy is an indispensable condition for processes constituting social personality and civility to form in a manner consistent with human dignity.[116] We need the possibility of respite and meaningful remove from *autri*, both intimately and personally, in order to engage each other civilly and publicly.[117] Without privacy, there is no room for deliberation or autonomy and thus ultimately no space for social engagement.[118]

The problem might well be put in terms consistent with a photo-negative of Wittgenstein's private language argument.[119] The private language argument presents us with the *aporia* that personal expression in language can never be completely private because it requires the use of public idiom to be intelligible.[120] But the reverse is also true: meaning in public discourse requires resistance, friction, against the public idiom to generate new contributions and thus permit a conversation to continue.[121]

For persons to create this friction requires privacy or remove because meaningful resistance requires both deliberation and courage.[122] It requires courage as each act of resistance puts our dignity at stake: to err in public is to suffer ridicule and ostracism.[123] It requires deliberation as each accepted contribution bestows dignity upon us from our respective communities and each rejected deliberate contribution bestows a sense of integrity and self-worth even if, in extreme cases, through potential tragic choice.[124]

---

113. *Id.*

114. *See* MARTTI KOSKENNIEMI, FROM APOLOGY TO UTOPIA: THE STRUCTURE OF INTERNATIONAL LEGAL ARGUMENT 293 (2005) (describing an argument as overdetermined if it draws upon inconsistent premises of normative state obligation and descriptive state consent).

115. *Id.*

116. *See* Post, *supra* note 19, at 1006-07.

117. *See id.* at 973-74.

118. *See id.*

119. 1 LUDWIG WITTGENSTEIN, WERKAUSGABE 356 (Suhrkamp Verlag ed., 1984) (setting out the private language argument).

120. *See id.* For a discussion of the *aporia*, see Frederic G. Sourgens, *Functions of Freedom: Privacy, Autonomy, Dignity, and the Transnational Legal Process*, 48 VAND. J. TRANSNAT'L L. 471, 516-17 (2015).

121. *See* 1 NIKLAS LUHMANN, THEORY OF SOCIETY 11, 45 (Rhodes Barrett trans., 2012) (noting the importance of resistance for communication and explaining how such resistance operates upon communication as the unity of difference between information, utterance, and understanding).

122. *See id.* at 36 (discussing the volitional component of communication).

123. *See* Whitman, *supra* note 18, at 1206 (discussing the importance of social ridicule for French privacy law).

124. The link between tragic choice, dignity, and public action is still clearly at the forefront of late classical historical literature. *See* TACITUS, THE HISTORIES 4 (D.S. Levene ed., W.H. Fyfe trans.,

Discourse participants therefore must be able to test and formulate their respective discourse contributions. Without it, they could not participate in conversation at all.[125] Language without privacy thus risks leading to inverse *aporia* of Wittgenstein's private language argument: a conversation without speakers is just as meaningless as a speaker without language.[126]

The breaking of privacy, which the world society faces in the current security climate, risks halting the possibility of engagement as it chills the ability to form thoughts, opinions, and expressions with which to engage in public discourse.[127] Firm privacy protections are therefore needed to protect any possibility of social interaction as well as the dignity of its participants.[128] Law—including world law—ought to aspire to this goal.[129] The endeavor of human rights law is therefore worthwhile to pursue despite the formal problems it has encountered. As such, the Privacy Principle seeks to support, rather than to denigrate, its efforts.

B. *Unlikelihood of Impending Treaty Codification*

Current non-human rights treaty practice does not provide a ready alternative basis to fill the gap left by state practice under existing human rights treaties. There is no treaty governing surveillance or intelligence gathering outright.[130] As the two examples below showcase, existing treaties have failed to bring about findings that extraterritorial intelligence activities had international legal consequences for the state on whose behalf they were carried out.

In one instance, Iran sought to rely upon a defense that intelligence operations carried out from the premises of an embassy deprived the premises of otherwise applicable diplomatic protections.[131] The ICJ rejected this argument as a matter of law, noting simply that the remedy for assertions of espionage or interference by a foreign diplomat in internal affairs of the receiving state is expulsion of the diplomat as *persona non grata*.[132] Little can be made of this

---

1997) ("[D]istinguished men bravely facing the utmost straights and matching in their end the famous deaths of older times.").

125. *See* Frédéric G. Sourgens, *Reconstructing International Law as Common Law*, 47 GEO. WASH. INT'L L. REV. 1, 25-29 (2015).

126. *See* LUHMANN, *supra* note 121, at 81-83 (discussing the role of surprise and nonfinality of communication).

127. *See* Sourgens, *supra* note 120, at 516-17.

128. *See* Post, *supra* note 19, at 1006-07.

129. *See* 2 HAROLD D. LASSWELL & MYRES S. MCDOUGAL, JURISPRUDENCE FOR A FREE SOCIETY: STUDIES IN LAW, SCIENCE AND POLICY 737-86 (1992).

130. Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT'L L. 687, 690 (2007) ("The fact that no explicit treaty norms address peacetime espionage is paradoxical in light of the enormous amount of intelligence activities and their relevance for international relations between states.").

131. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, 35 (May 24) (noting Iranian arguments on the role of the U.S. embassy in "espionage and conspiracy").

132. *Id.* at 38-39 (rejecting that espionage directed from the premises of the embassy, if established, "could be regarded by the Court as constituting a justification of Iran's conduct and thus a defence to the United States' claims in the present case").

holding to tease out an international legal prohibition of espionage or a global privacy right.[133]

In another instance, a Cypriot investor in Turkey argued that Turkish signals intelligence intercepts of his calls with his U.S. arbitration counsel concerning matters against the Turkish government violated international law.[134] Although the tribunal recognized that the communications were privileged, and excluded any privileged communication obtained through intercepts from the arbitration record, it recognized the state's right to conduct criminal investigations and did not deem the intercept of privileged communications internationally wrongful.[135]

Further, it is highly unlikely that agreement on a treaty governing signals intelligence could be reached in the near future.[136] To be meaningful, states with significant signals intelligence capabilities would need to consent to restricting the use of intelligence assets.[137] Given the current global security climate, and the asserted use of signals intelligence to limit terrorist attacks, it is unlikely that would happen.[138]

Proponents of a treaty structure may point to efforts such as the U.S.-EU Privacy Shield or the Five Eyes Agreement as some treaty practice to the contrary. The U.S.-EU Privacy Shield is a principally commercial mechanism permitting commercial parties to certify compliance with transatlantic privacy regimes.[139] The Privacy Shield became a necessity when a recent European court ruling that NSA government access to data under PRISM, as revealed by Edward Snowden, meant that the transfer of data by European companies to U.S.-based servers would place them out of compliance with EU privacy directives.[140] Due to language in the Safe Harbor Principles permitting access to data as needed for national security purposes, existing Safe Harbor Principles were deemed to no longer satisfy minimum requirements of EU law.[141]

The problems with the Privacy Shield remain significant. First, the Privacy Shield retained much of the language at issue in the original Safe Harbor regulation—national security remains a reason to access data.[142] The Privacy

133. Fleck, *supra* note 130, at 691 ("The International Court of Justice (ICJ) has not taken a position on the issue of peacetime espionage, although it has had the opportunity to do so on a few occasions.").

134. Libananco Holdings Co. Limited v. Republic of Turkey, ICSID Case No. ARB/06/8, Decision on Preliminary Issues, ¶ 43 (June 23, 2008) (discussing intercept of privileged communication by a state party to ongoing legal proceedings).

135. *Id.* ¶ 82 (ordering the protection of privilege).

136. Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 625 (2007) ("Proposals for international treaties to govern intelligence collection are not only premature, but will likely prove counterproductive to the goal of promoting international peace and stability.").

137. *See id.* at 628 (arguing that espionage is both "necessary for the national security of a nation-state" and "part of the sovereign right of the nation-state").

138. *See* Savage, *supra* note 24.

139. *See* Kristina Daugirdas & Julia Davis Mortenson, *Contemporary Practice of United States Relating to International Laws*, 110 AM. J. INT'L L. 347, 360 (2016) (describing the scope of the Privacy Shield agreement).

140. *Id.* at 362-63.

141. *Id.*

142. *Id.* at 364-65 (noting the limitations of the Privacy Shield).

Shield provides Ombudsman services to address any complaints raised with regard to data access.[143] The structure does not appear to impose any obligations on the U.S. or the EU to conduct intelligence in a certain manner—nor does it provide for a review mechanism to ascertain whether intelligence operations in fact comply with such an agreement.[144]

Second, the Privacy Shield is a political agreement.[145] The Trump Administration may already have taken steps to undermine its purpose with recent executive action.[146] The mechanism, in other words, is not sufficiently robust to provide long-term assurances of compliance. While a helpful step, it is certainly not the final step in providing for privacy protection for global data transfers.

Other agreements like the Five Eyes Agreement are even less likely to yield constraints. Privacy International notes that "[t]he Five Eyes alliance is a secretive, global surveillance arrangement of States comprised of the U.S. National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB)."[147] While the agreement does appear to provide for some agreement to restrain from spying on citizens of the participating states,[148] it is unlikely to prove a particularly fruitful avenue for privacy protection.[149] For one, the agreement itself is still partly secret;[150] it is thus anathema to current formal modes of international law.[151] For another, it is premised upon political and bureaucratic agreement rather than legal enforcement,[152] and it, too, is thus likely to suffer as administrations strike more or less nationalist cords.

In short, reliance upon future codification in treaty law is unlikely to resolve the normative question of how to protect privacy rights in the digital age. Treaty practice can offer some normative direction of what might be desirable.

---

143. *Id.*

144. *Id.* at 367 (discussing the sufficiency of the Privacy Shield under existing European jurisprudence giving rise to it).

145. *Id.* at 360. On the use and (lack of) legal force of such agreements, see Ryan Harrington, *A Remedy for Congressional Exclusion from Contemporary International Agreement Making*, 118 W. VA. L. REV. 1211, 1225 (2016).

146. Natasha Lomas, *Trump Order Strips Privacy Rights from Non-U.S. Citizens, Could Nix EU-US Data Flows*, TECHCRUNCH (Jan. 26, 2017), http://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/.

147. *The Five Eyes*, PRIVACY INTERNATIONAL, http://www.privacyinternational.org/node/51 (last visited Apr. 15, 2017). The Five Eyes agreement structures intelligence cooperation and establishes accepted behavioral norms and practices among the allied intelligence services of the United States, United Kingdom, Canada, Australia, and New Zealand. Although this arrangement, the contents of which are not public, may not contribute heavily to the creation of international norms regarding foreign surveillance, the original U.K.-U.S. Agreement (UKUSA) from which the Five Eyes agreement derives details the types of communications that each state is to collect and treats as impermissible some uses of those communications.

148. Deeks, *supra* note 61, at 347 (discussing the Five Eyes agreement).

149. *Id.*

150. *Id.*

151. *Id.*

152. Daniel Severson, Note, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change*, 56 HARV. INT'L L.J. 465, 509-10 (2015) (discussing the *sui generis* nature of the Five Eyes agreement).

It cannot, however, fully close the gap of getting from normative desire to a means to secure legal compulsion.

C. *Problems with a Customary Approach*

Customary international law is similarly unlikely to fill the normative gap identified so far. Proof of a customary international law rule would require a showing that: (1) there is a widespread and representative state practice, and (2) this practice was brought about by a sense of legal obligation rather than convenience.[153] Intuitively, persistent and aggressive global signals intelligence efforts will make it difficult to find significant state practice prohibiting its use.[154]

Current literature confirms this intuitive insight. There is no firm customary rule enjoining states from using espionage in wartime.[155] At most, international humanitarian law governing international armed conflicts treats wartime espionage as a tolerable delict: it neither enjoins the use of espionage on the international plane nor prohibits the trial of spies caught red-handed and out of uniform in domestic court for the domestic law crime of espionage.[156]

There is even less legal certainty regarding espionage in peacetime.[157] At most, international law prohibits trespass (rather than espionage), and thus does not deal with technologically advanced forms of signals intelligence that can be performed remotely.[158] The derivation of any customary international law rule protecting privacy rights in wartime or in peace is therefore decidedly fragile.[159]

---

153. *See* Frederic L. Kirgis, *Custom on a Sliding Scale*, 81 AM. J. INT'L L. 146, 149-50 (1987) (suggesting that state practice and *opinio juris* are factors on a sliding scale rather than true elements of custom); Timothy Meyer, *Codifying Custom*, 160 U. PA. L. REV. 995, 1002-03 (2012) (defining the elements of customary international law and noting their difficulty in application).

154. *See* Jeffrey H. Smith, *Keynote Address*, 28 MICH. J. INT'L L. 543, 544-45 (2007) (noting the longstanding state practice of the United States to engage in electronic surveillance to support its lawfulness).

155. *See* Simon Chesterman, *The Spy Who Came in From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1077 (2006) ("[I]nconsistencies have led some commentators to conclude that addressing the legality of intelligence gathering under international law is all but oxymoronic."); Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 67 (1987) ("Most writers claim that espionage in war is 'legal,' although the unfortunate spy himself may be executed if not in uniform.").

156. *See* Geoffrey Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 337-38 (1996) (discussing "the paradoxical nature of espionage as a delict").

157. *See* Chesterman, *supra* note 155, at 1087 (noting that the response to the signals intelligence intercepts of diplomatic correspondence "has tended to be pragmatic rather than normative"). The classic distinction is between intelligence gathering that trespasses upon sovereign territory of the state subject to espionage, which is prohibited, and intelligence gathering done without trespass. *Id.* at 1081-87. Some commentators have doubted the usefulness of the distinction, arguing instead that espionage in peacetime violates international law and that trespass aggravates the violation. Delupis, *supra* note 155, at 67-68.

158. *See* Chesterman, *supra* note 155, at 1081-87 (setting out the classic trespass / non-trespass distinction). Some commentators have doubted the usefulness of the distinction, arguing instead that espionage in peacetime violates international law and that trespass aggravates the violation. Delupis, *supra* note 156, at 67-68.

159. *See* Chesterman, *supra* note 155, at 1087.

Some submit that this state of international law makes any kind of espionage—including signals intelligence—presumptively lawful.[160] This view relies upon the so-called *Lotus* principle announced by the Permanent Court of International Justice in a case between France and Turkey.[161] This principle provides that conduct is internationally permissible unless expressly prohibited by a rule of international law.[162] These scholars submit that the absence of an international legal rule prohibiting signals intelligence provides its legality.[163]

This view is on the whole disfavored in current international law scholarship.[164] Rather, much of the scholarship focusing beyond the human rights paradigm submit that states through their conduct have to develop some context-sensitive international policy prescriptions on intelligence gathering.[165] As scholarship shows, there is overlap among global signal intelligence programs, as well as overlap among the statutes authorizing them.[166] An inductive, historical approach to intelligence gathering efforts could further place such programs in a better context.[167] This scholarship is likely to yield a more concrete picture of the process of decision making governing the institution and administration of global intelligence gathering programs.[168] Signals intelligence, in other words, does not operate in a complete international legal vacuum.[169]

Other attempts to grapple with customary international law aided by a human rights lens have also encountered significant difficulty. One such attempt is the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.[170] The *Tallinn Manual 2.0* seeks to find a customary international

160. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 28, at 19 (noting the point of view of a few experts "that the extensive State practice of conducting espionage on the target State's territory has created an exception to the generally accepted premise that non-consensual activities attributable to a State while physically present on another's territory violate sovereignty" and applying this exception to extra-territorial signals intelligence operations); Adams, *supra* note 29, at 403-04 (2017) (applying the *Lotus* principle); Craig Forcese, *Pragmatism and Principle: Intelligence Agencies and International Law*, 102 VA. L. REV. ONLINE 67, 73 (2016) (discussing the relevance of the *Lotus* principle for the international law of espionage); Raul Pedrozo, *Military Activities in the Exclusive Economic Zone: East Asia Focus*, 90 INT'L L. STUD. 514, 528 (2014) (same).

161. Forcese, *supra* note 160, at 73.

162. *Id.*

163. Adams, *supra* note 29, at 403-04; Pedrozo, *supra* note 160, at 528.

164. Forcese, *supra* note 160, at 69 ("There is, therefore, no principled basis to conclude that covert action per se falls into an area in which, to quote the famous *S.S. Lotus* case, states are permitted a 'wide measure of discretion.'").

165. *See* W. MICHAEL REISMAN, THE QUEST FOR WORLD ORDER AND HUMAN DIGNITY IN THE TWENTY-FIRST CENTURY: CONSTITUTIVE PROCESS AND INDIVIDUAL COMMITMENT 177-90 (2012) (distinguishing a textual rule-based mode and a context-sensitive policy-based mode of international law).

166. *See* Deeks, *supra* note 61, at 343-45 (arguing that international policy guidance can be derived from domestic surveillance statutes); Deeks, *supra* note 89, at 28-36 (submitting that domestic statutes provide one predicate for peer constraint in the intelligence community).

167. *See* Asaf Lubin, Book Note (JACKSON MAOGOTO, TECHNOLOGY AND THE LAW ON THE USE OF FORCE: NEW SECURITY CHALLENGES IN THE TWENTY-FIRST CENTURY (2014)), 40 YALE J. INT'L L. 441, 443-44 (2015) (demanding a more context-driven approach to espionage in international law).

168. *See* sources cited *supra* notes 164, 166.

169. *See* REISMAN, *supra* note 165, at 21 (noting the reach of law to the "offshore" zones of international law).

170. *See, e.g.*, TALLINN MANUAL 2.0, *supra* note 28, at 170-71, 189-93, 203-07.

law basis for the human right to privacy.[171] This approach looks to the dual pillars of reasonable expectation of seclusion and intimacy of information already discussed in the human rights context.[172] The approach expands that the confidentiality of communications protects email communications even in the absence of sensitive information within the email communication, thus establishing a per se rule for email communication.[173] The *Tallinn Manual 2.0*, however, however, already crystalizes key problems for such a customary international law approach. First, it notes that "a number of States that accept the existence of the right take the position that it does not apply extraterritorially."[174] This would significantly limit the relevance of customary international law for the current inquiry. Second, the *Tallinn Manual 2.0* notes in general that "[t]he Experts were incapable of achieving consensus as to whether remote cyber espionage reaching a particular threshold of severity violates international law," thus foreclosing an alternative means of dealing with extraterritorial surveillance by looking at its severity.[175]

Similarly, the United Nations Human Rights Council appointed a special rapporteur to address internet privacy concerns raised by bulk cyber surveillance in the context of the promotion and protection of the right to freedom of opinion and expression.[176] The special rapporteur concluded the existence of a human rights obligation to protect privacy rights online.[177] Like the *Tallinn Manual 2.0*, however, the most recent report notes that "practice often fails to meet such standards," noting particularly Russian, French, UK, and Brazilian conduct that is arguably inconsistent with the obligations induced by the Special Rapporteur.[178] Such state practice significantly complicates any argument that a customary international law rule prohibiting online, extraterritorial intrusions of privacy has crystallized.[179]

---

171. *Id.* at 187, 189 (suggesting in Rule 35 that "[i]ndividuals enjoy the same international human rights with respect to cyber-related activities that they otherwise enjoy" and that this rule is applicable to cyber privacy, which is "of a customary international law character").

172. *Id.* at 191-92.

173. *Id.* at 189-90.

174. *Id.* at 189.

175. *Id.* at 170.

176. *See* G.A. Res. 25/A/HRC/25/L.2, Freedom of Opinion and Expression: Mandate of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (Mar. 4, 2014) (setting the mandate for the Special Rapporteur).

177. *See* Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, ¶ 20, U.N. Doc. A/71/373 (Sept. 6, 2016) (by David Kaye).

178. *Id.*

179. For another such attempt, see *International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (May 2014), https://necessaryandproportionate.org/principles. Problematically, this attempt, too, notes that "many governments routinely engage in bulk surveillance of international communications with very little regard for the privacy of those communications, possibly in the mistaken belief that their legal obligations only extend as far as their own citizens or residents. Even more problematically, it appears that countries seek intelligence-sharing arrangements with other countries in order to obtain surveillance material concerning their own citizens that they could not obtain under their domestic legal framework." *Background and Supporting International Legal Analysis for the International Principles for the Application of Human Rights to Communications Surveillance* 5, NECESSARY & PROPORTIONATE (May 2014), http://necessaryandproportionate.org/files/2016/03/29/background_and_supporting_legal_analysis_en.pdf.

As many proponents of such context-sensitive prescriptions would themselves admit, however, the principles they develop are "soft."[180] These principles can guide state conduct but cannot compel it.[181] They are helpful in informing policy making of when and how to spy;[182] they are decidedly less valuable to those spied upon in developing legal support for the proposition that existing or future efforts are internationally wrongful.[183] Such support would have to be developed by other means, if it can be developed at all.

II. PROVING GENERAL PRINCIPLES OF LAW

As the remainder of this Article will submit, the current state of international law requires a paradigm shift. The traditional sources of international law discussed so far have been called "oxymoronic."[184] They suggest the existence of norms to limit global signals intelligence programs. But they ultimately fail to convincingly substantiate a path to integrate these norms into international law. Perhaps symptomatically, the *Tallinn Manual 2.0* reports in the context of an attempt to ground privacy protections in customary international law that "the Experts concluded that, *notwithstanding State practice*, espionage remains subject to States' applicable human rights law obligation to respect the right to privacy."[185] Custom without state practice will prove difficult to defend on anything but the hope that the principle proposed has sufficient normative pull to bring about future compliance.[186] Given the current security environment, it is not likely that such state practice will be forthcoming, thus limiting the argument for a customary international rule of online privacy. It is therefore time to consider whether a less traditional source of international law is able to overcome the obstacles faced in treaty practice and custom.

As the Article will develop, general principles of law recognized by civilized nations succeed in closing the normative gap on signals intelligence left open by other sources of international law. General principles of law recognized by civilized nations are the third formal source of international law alongside treaty law and customary international law.[187] Although used with significantly less frequency than the other formal sources of international law, general principles of law were specifically intended to address areas underdeveloped by treaty law and custom.[188] The function of general principles of

180. *See* Deeks, *supra* note 61, at 343-45 (noting the limitations of the approach to provide concrete rules of privacy protection).

181. *Id.*

182. *Id.*

183. *Id.*

184. Chesterman, *supra* note 155, at 1077.

185. TALLINN MANUAL 2.0, *supra* note 28, at 193 (emphasis added).

186. *See* Kirgis, *supra* note 153, at 149-50 (discussing how custom could be created in the context of opinio juris with very limited state practice).

187. *See* Prosper Weil, *Towards Relative Normativity in International Law?*, 77 AM. J. INT'L L. 413, 425 (1987) (listing as "formal sources of international law: conventions, custom, general principles of law").

188. *See* Prosper Weil, *"The Court Cannot Conclude Definitively . . ." Non Liquet Revisited*, 36 COLUM. J. TRANSNAT'L L. 109, 111 (1997) (noting ICJ practice to use general principles of law in limited circumstances when faced with disputes in underdeveloped areas of law).

law, in other words, is to fill gaps within the fabric of international law.[189] This is precisely the state of the law on signals intelligence.[190]

Although general principles of law functionally are gap fillers, they are formally sources of general international law co-equal with treaty law and custom.[191] A general principle of law is not a subsidiary source of law.[192] It is not less authoritative than other sources of international law.[193] Proof of a general principle therefore can provide a robust basis for an international legal right even in the absence of treaty or customary law.[194] In fact, that is the very purpose for which general principles were included as a formal source of international law.[195]

A. *Proof of a Principle*

Proof of a general principle of law recognized by civilized nations in international law classically has two components. First, one must prove that a general principle of law exists at all. Does comparative legal analysis of relevant legal systems establish a requisite degree of convergence to formulate a common, shared legal principle of domestic laws? It is not necessary to show universal support; rather, one must demonstrate "[s]ome sort of general acceptance or recognition by States."[196] Such principles recognized in jurisprudence include a broad range of principles, from joint and several liability for a wrong committed, to imposing obligations of good faith, to the consequences of res judicata in international adjudication.[197]

Second, one must prove that this common, shared principle of domestic laws is compatible with existing norms of general international law. Does public international legal analysis of relevant analogous international legal norms establish the requisite degree of convergence with the common, shared legal

189. LAUTERPACHT, *supra* note 31, at 93; Roberto G. McLean, *Judicial Discretion in the Civil Law*, 43 LA. L. REV. 45, 52-54 (1982) (noting the predominant civil law jurisdictions in which general principles of law have a similar function).

190. Chesterman, *supra* note 155, at 1077.

191. Rosalyn Higgins, Keynote Address, *A Just World Under Law*, 100 AM. SOC'Y INT'L L. PROC. 388, 391 (2006) ("[T]here is no hierarchy as such between sources of international law.").

192. Statute of the International Court of Justice art. 38, June 26, 1945, 59 Stat. 1031, 33 U.N.T.S. 993; *see also* Steven Schneebaum, *What Is This Case Doing Here? Human Rights Litigation in the Courts of the United States*, 44 CASE W. RES. J. INT'L L. 183, 195-96 (2011) (discussing the primary sources of international law).

193. PATRICK DAILLER & ALAIN PELLET, DROIT INTERNATIONAL PUBLIC 348 (7th ed. 2002) (grounding general principles as a source of international law); Higgins, *supra* note 192, at 391 ("[T]here is no hierarchy as such between sources of international law."). *But see* ULRICH FASTENRATH, LUCKEN IM VÖLKERRECHT 101-02 (1991) (arguing that general principles of law are not positively grounded in state consent or practice).

194. *See* LAUTERPACHT, *supra* note 31, at 93-96 (discussing the importance of general principles in absence of other sources of international law).

195. BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 1-26 (2006) (discussing the reason for inclusion of general principles of law as a source of international law).

196. *See* Nolan & Sourgens, *supra* note 31, at 525-28 (cataloguing general principles recently recognized in jurisprudence).

197. *See* Bruno Simma & Philip Alston, *The Sources of Human Rights Law: Custom, Jus Cogens, and General Principles*, 12 AUST. Y.B. INT'L L. 82, 102 (1989).

principle of domestic laws to permit the seamless incorporation of the general principle in question? This is an essentially inductive process of legal reasoning.[198]

An alternative way to conceive of proof of a general principle is through deductive reasoning.[199] This approach assumes that international law has a core or essence beyond summing up every rule of positive treaty or customary law.[200] When a problem cannot be answered by means of one of these rules, general principles can close the gap by analogy.[201] In this case, a general principle projects a rule that must be applicable to the new problem by extending the logic of existing international law.[202] Such an analysis short circuits the need to prove inductively that a privacy principle exists by pointing to the overwhelming support among legal publicists that a human rights principle of privacy must apply to global surveillance programs notwithstanding state practice to the contrary.[203]

In fact, in their seminal article on the use of general principles in the human rights context, Bruno Simma and Philip Alston suggest just such a course of action by looking to the importance of the principle for international law as expressed for instance in UN General Assembly resolutions.[204] This method therefore would yield a general principle by looking to the sources treated as indicative of custom. This Article nevertheless attempts to prove inductively that this essentialist principle actually obtains as a classically derived general principle of law. In so doing, it aims to cement inductively the existence of a robust privacy right in international law.[205]

This Section addresses the first component of the classical way to prove a general principle. The question of whether comparative legal analysis of relevant legal systems establishes the requisite degree of convergence to formulate a common, shared legal principle can be broken into three parts.[206] *First*, how does one select relevant legal systems?[207] *Second*, by what means does one

198. For a fuller articulation of the distinction between deductive and inductive reasoning in international law, see Frédéric G. Sourgens, *Reconstructing International Law as Common Law*, 47 GEO. WASH. INT'L L. REV. 1, 25-29 (2015).

199. *Id.* A deductive approach is one way to present an essentialist argument. It assumes in essence that there is one right answer to any legal problem due to the essence of law or legal process. Law in this sense would emulate Spinoza's *Ethics*. *See* Aaron Garrett, *Spinoza as Natural Lawyer*, 25 CARDOZO L. REV. 627, 634-35 (2003) (discussing the deductive, fixed mode of natural law for Spinoza).

200. *See* CHENG, *supra* note 195, at 3-19 (discussing the essentialist-naturalist view of general principles of law).

201. *See* James L. Dennis, *Interpretation and Application of the Civil Code and the Evaluation of Judicial Precedent*, 54 LA. L. REV. 1, 11-12 (1993) (discussing the use of analogy in civil code jurisdictions).

202. *Id.*

203. TALLINN MANUAL 2.0, *supra* note 28.

204. Simma & Alston, *supra* note 197, at 105; *see also* Richard B. Lillich, *The Growing Importance of Customary International Human Rights Law*, 25 GA. J. INT'L & COMP. L. 1, 14-15 (1996) (discussing Simma & Alston's approach).

205. This attempt is also intended to overcome the concern, expressed already by Simma and Alston, that general principles are plagued by a natural law flavor. *See* Lillich, *supra* note 204, at 15; Simma & Alston, *supra* note 197, at 107.

206. For a full discussion, see Nolan & Sourgens, *supra* note 31, at 506.

207. *Id.*

identify convergences in selected legal systems?[208] *Third*, how much convergence is required to establish that the jurisdictions share a common general principle?[209]

1. *Method for Selecting Legal Systems to Be Examined*

Proof of a general principle does not require an examination of every legal system in the world.[210] Typically, the ICJ has limited its own comparative legal analysis to three to five legal systems.[211] Alternatively, the Court has relied upon comparative studies prepared by leading academics.[212]

The selection of legal systems has been controversial. Historically, general principles were established by comparing leading common law and European civil law jurisdictions.[213] This historical practice has been criticized as too narrowly drawn because it fails to account for legal systems of the developing world.[214] Current best practices therefore have broadened to include non-Western jurisdictions.[215]

The selection of jurisdictions will be most persuasive if it takes the key stakeholders' jurisdictions affected by the principle to be proved into account.[216] The stronger the link between the principle and the state to whom the

---

208. *Id.*

209. *Id.*

210. For a full review of I.C.J. jurisprudence and recent arbitral decisions, see Nolan & Sourgens, *supra* note 31, at 525-28 (working methodically through recent decisions).

211. *See, e.g.*, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 324, 354-57 (Nov. 6) (separate opinion by Simma, J.) (relying upon French, Swiss, German, Californian, and Canadian law); "); Oil Platforms (Iran v. U.S.), Counter-Claim, 1998 I.C.J. 190, 224, 230-31 (Mar. 10) (dissenting opinion by Rigaux, J.) (relying upon French, Belgian, and European Communities law); North Sea Continental Shelf (Federal Republic of Ger. v. Den.), 1969 I.C.J. 3, 101, 121-22 (Feb. 20) (separate opinion by Ammoun, J.) (relying upon "the concept of estoppel by conduct of Anglo-American equity, or by virtue of the principle of western law that allegans contraria non audiendus est, which has its parallel in Muslim law"); Certain Norwegian Loans (Fr. v. Nor.), 1957 I.C.J. 9, 34, 49-50 (July 6) (separate opinion by Lauterpacht, J.) (relying upon French, English, and American law).

212. *See, e.g.*, Barcelona Traction, Light & Power Co. (Belg. v. Spain), 1970 I.C.J. 30, 114, 155 (Feb. 5) (separate opinion of Tanaka, J.) (relying upon a comparative legal analysis compiled by the Max-Planck Institute); Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 12, 54, 66 (Apr. 12) (separate opinion of Koo, J.) (relying upon "a comparative study by Professor Max Rheinstein").

213. Wolfgang Friedmann, *The Use of "General Principles" in the Development of International Law*, 57 AM. J. INT'L L. 279, 285 (1963) ("[T]he relevant principles of the most representative systems of the common-law and the civil- law world" are constitutive of general principles of law).

214. *See, e.g.*, North Sea Continental Shelf (F.R.G. v. Den.), 1969 I.C.J. 3, 101, 132 (Feb. 20) (separate opinion of Ammoun, J.) (noting the colonial remnants in general principles of "civilized" nations and advocating a broader scope to establish general principles); VLADIMIR DEGAN, SOURCES OF INTERNATIONAL LAW 70 (1997) (same).

215. *See* Interpretation and Application of the 1971 Montreal Convention (Libya v. U.S.), 1998 I.C.J. 115, 155, 171 (Feb. 27) (dissenting opinion of Schwebel, J.) (rejecting judicial review as a general principle of law due to its restriction to developed democracies); Desert Line Projects LLC v. Republic of Yemen, ICSID Case No. ARB/05/17, Award, ¶ 207 (Feb. 6, 2008) (referring to Islamic law in establishing a general principle of law).

216. *See* Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 6, 44 (Apr. 12) (stating that specific practice between states dispenses with the need to have regard for customary international law or general principles of law); *see also* DEGAN, *supra* note 214, at 71-75.

principle is to be applied, the greater the principle's ultimate legitimacy will be.[217]

2. *Choice of Comparative Law Methodology*

The ICJ has employed two comparative law methodologies when proving a general principle of law. First, the Court has looked to the "formal" overlap between the legal systems analyzed.[218] The Court's formal analysis compared the text of applicable statutes and seminal cases and further consulted treatises or commentary authoritatively interpreting the jurisdiction's black letter law.[219] For example, Judge Simma in a separate opinion in the *Oil Platforms Case* established a general principle of joint and several liability by comparing the code provisions applicable to delictual liability of the French, Swiss, and German Civil Codes and seminal cases of U.S. tort law, as well as their interpretation in the leading treatises on the law of obligations and tort law.[220]

Alternatively, the Court has directly or indirectly relied upon a functional comparative methodology.[221] Functional analysis does not look to the convergence of black letter rules, but to the convergence of outcomes in hypothetical case scenarios.[222] The benefit of functional analysis is to limit the risk of false negatives when two jurisdictions achieve similar results by different legal paths.[223] It also limits the risk of false positives when two jurisdictions apply facially similar legal principles in radically different ways in practice.[224] Functional legal comparison has become the predominant method used by comparative legal scholars when codifying transnational law or harmonizing laws of regional trading blocs such as the European Union.[225]

The approaches used by the Court suggest that proof of a general principle should begin with a formal comparison.[226] This formal comparison should

---

217. *See supra* notes 169-71.

218. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 324, 354-58 (Nov. 6) (separate opinion of Simma, J.) (consulting leading commentators and seminal cases on tort/delict law); Oil Platforms (Iran v. U.S.), Counter-Claim Order, 1998 I.C.J. 190, 224, 230 (Mar. 10) (dissenting opinion of Rigaux, J.) (relying upon concordant code provisions); Norwegian Loans (Fr. v. Nor.), 1957 I.C.J. 9, 34, 49-50 (July 6) (separate opinion of Lauterpacht, J.) (consulting leading treatises on French, English and American law of contracts).

219. *See supra* note 173.

220. *Oil Platforms*, 2003 I.C.J. at 161, 324, 354-58 (separate opinion of Simma, J.) (consulting leading commentators and seminal cases on tort/delict law).

221. Barcelona Traction, Light & Power Co. (Belg. v. Spain), 1970 I.C.J. 3, 114, 155 (Feb. 5) (separate opinion by Tanaka, J.) (relying upon a comparative legal analysis compiled by the Max-Planck institute); North Sea Continental Shelf (F.R.G. v. Den.), 1969 I.C.J. 3, 101 ¶ 22 (Feb. 20) (separate opinion of Ammoun, J.) (comparing Anglo-American equity with civilian good faith and civilian good faith as received in Muslim countries); Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 12, 54, 68 (Apr. 12) (separate opinion of Koo, J.) (relying upon "a comparative study by Professor Max Rheinstein").

222. *See supra* note 176.

223. *Id.*

224. Rodolfo Sacco, *Legal Formants: A Dynamic Approach to Comparative Law I*, 39 AM. J. COMP. L. 1, 24 (1991).

225. Reinhard Zimmermann & Simon Whittaker, *Good Faith in European Contract Law: Surveying the Legal Landscape*, *in* GOOD FAITH IN EUROPEAN CONTRACT LAW 39-40 (Reinhard Zimmermann & Simon Whittaker eds. 2008).

226. *See* sources cited *supra* note 173.

then be checked for potential false positives or false negatives by applying a functional comparison, as well.[227] The result will be a nuanced and robust understanding of convergence consistent with both the Court's jurisprudence and comparative law best practices.[228]

3. *The Criterion of Critical Mass*

The Court has established general principles even in the absence of complete agreement between major legal systems. Some of the Court's pronouncements on general principles may give the false impression that complete agreement is necessary.[229] Such pronouncements are inconsistent with the Court's jurisprudence.[230] Thus, the Court has relied upon good faith as a general principle of law since its earliest jurisprudence.[231] Early international jurisprudence held that good faith required both honesty and fact and reasonable conduct.[232] At the time of the Court's establishment of such an expansive principle, however, neither English nor U.S. common law recognized the existence of such an expansive good faith principle.[233]

Instead of relying on a standard of complete agreement, the appropriate standard of convergence is critical mass. The requirement for convergence in general principles has been likened to the requirement of convergence in the proof of a customary international law rule.[234] Current scholarship usefully analyzes the convergence necessary for the establishment of a customary rule by reference to critical mass.[235]

Critical mass refers to a transformative point of criticality – in our context, the point at which a principle of law ceases to be parochial to any number of legal systems and becomes a common and shared general principle of law.[236]

---

227. *See* sources cited *supra* note 176.

228. *See* sources cited *supra* note 173-76.

229. *See, e.g.*, Barcelona Traction, Light & Power Co. (Belg. v. Spain), 1970 I.C.J. 286, 324 (separate opinion of Ammoun, J.) (noting that the notion of "abuse of right" is "enshrined in a general principle of law which emerges from the legal systems of all nations"); North Sea Continental Shelf (F.R.G. v. Den.), 1969 I.C.J. 3, 21 (Feb. 20) ("[T]he principle of the just and equitable share was one of the recognized general principles of law which, by virtue of paragraph 1 *(c)* of the same Article, the Court was entitled to apply as a matter of the *justitia distributiva* which entered into all legal systems."); Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 123, 136 (Apr. 12) (dissenting opinion of Ferrandes, J.) (noting that "the laws of all civilized nations recognize the right of access to enclaved property in favour of its owner").

230. Friedmann, *supra* note 213, at 284 (stating that "it is not necessary that the principles should be found to exist in identical form in every system of civilized law").

231. CHENG, *supra* note 195, at 105-60.

232. *Id.*

233. Dennis M. Patterson, *Wittgenstein and the Code: A Theory of Good Faith Performance and Enforcement Under Article 9*, 137 U. PA. L. REV. 335, 381 (1988) (discussing the limited role of good faith in pre-1950s U.S. contract law); Zimmermann & Whittaker, *supra* note 225, at 39-40 (discussing the lack of a good faith principle in the English law of contract).

234. Simma & Alston, *supra* note 197, at 105.

235. *See, e.g.*, Adeno Addis, *The Concept of Critical Mass in Legal Discourse*, 29 CARDOZO L. REV. 97, 145 (2007) (using critical mass to analyze custom formation); Steven R. Ratner, *Is International Law Impartial?*, 11 LEGAL THEORY 39, 57 (2005); William Thomas Worster, *The Transformation of Quantity into Quality: Critical Mass in the Formation of Customary International Law*, 31 B.U. INT'L L.J. 1, 56-71 (2013) (using critical mass to analyze custom formation).

236. Addis, *supra* note 235, at 104.

This point of criticality "is actually not just a matter of the amount of resource, but also of the density and purity of that resource."[237]

Critical mass scholarship is helpful in three principal ways when determining the sufficiency of convergence between legal systems to establish a general principle. First, it has shown that criticality is not a precise measure.[238] There is no number or percentage of agreement that itself will yield criticality.[239] Critical mass looks to establish whether the quantity has begun a qualitative shift or chain reaction.[240] Critical mass therefore requires both quantitative and qualitative engagement.[241]

Further, density and purity matter.[242] Critical mass will look to the density of agreement between the studied jurisdictions.[243] Convergence, or divergence, is never absolute.[244] Rather, there will be a difference in density of functional convergence: how many legal systems treat an intrusion in the home as wrongful? How many jurisdictions extend liability to correspond? The denser the agreement on outcomes between jurisdictions, the stronger the case for a general principle.[245] Further, the purity of agreement—for example, whether jurisdictions in fact agree upon a rationale for liability—similarly matters to critical mass.[246] In the absence of an overlap in rationale, a greater density of agreement may well be required to establish a general principle and vice versa.

Finally, diversity matters. To arrive at a critical mass, the broader the support among legal traditions, the stronger a claim that a principle is in fact "general."[247] The diverse converging jurisdictions serve as agents towards a tipping point of increasing acceptance of the principle in question.[248] Critical mass denotes the point of criticality at which that tipping point has been reached or passed.[249] A broad coalition of converging jurisdictions crossing legal, regional, and developmental boundaries is more likely to reflect a tipping point than a narrow coalition.[250] The broader the diversity, the greater the

---

237. *Id.*

238. *Id.* at 127.

239. *Id.*

240. *Id.* at 104.

241. *Id.* at 127.

242. *Id.* at 104.

243. *Id.* at 104.

244. *See* KLAUS PETER BERGER, THE CREEPING CODIFICATION OF THE LEX MERCATORIA 47 (1999) (explaining how to deal with divergence in establishing general principles).

245. Addis, *supra* note 235, at 104.

246. *Compare* BERGER, *supra* note 244, at 47 (noting the steps required to overcome doctrinal divergence in establishing general principles), *with* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 324, 354-58 (Nov. 6) (separate opinion of Simma, J.) (establishing a general principle in the context of comparative doctrinal convergence).

247. *See* DEGAN, *supra* note 214, at 70 (noting the need for diversity in establishing general principles); Christopher A. Ford, *Judicial Discretion in International Jurisprudence: Article 38(1)(c) and "General Principles of Law,"* 5 DUKE J. COMP. & INT'L L. 35, 65 (1994) (same).

248. *See* Worster, *supra* note 235, at 56-58.

249. *See* Addis, supra note 235, at 104.

250. *See* DEGAN, *supra* note 214, at 70 (noting the need for diversity in establishing general principles); Ford, *supra* note 248, at 65 (same).

chance of adoption of the principle by other, similarly situated jurisdictions.[251] In fact, one can assess whether there is movement within the dissenting jurisdiction towards convergence with the majority of jurisdictions in question—i.e., whether a chain reaction towards the general principle is currently underway.[252]

B. *Integration into International Law*

The fact that a general principle exists does not mean that it forms part of international law.[253] Rather, general principles of law must also satisfy a further requirement of compatibility with existing general international law.[254]

Two leading English judges of the ICJ have explained the relationship between general principles of domestic law and international law. Judge Fitzmaurice noted in his separate opinion in *Barcelona Traction* that "it is scarcely less important to bear in mind that conditions in the international field are sometimes very different from what they are in the domestic, and that rules which these latter conditions fully justify may be less capable of vindication if strictly applied when transposed on to the international level."[255] Judge McNair further submitted in his concurring opinion in the *South West Africa* advisory opinion that "the way in which international law borrows from [general principles of law] is not by importing private law lock, stock, and barrel, ready-made and fully equipped with a set of rules."[256] Rather, "the true view of the duty of international tribunals in this matter is to regard any features or terminology which are reminiscent of the rules and institutions of private law as an indication of policy and principles rather than as directly importing these rules and institutions."[257]

The jurisprudence of the Court indicates that any principle must be compared with existing rules of international law. To the extent that the principle would outright displace existing rules of international law, a general principle cannot exist.[258] In other words, in such a context, the general principle would not fulfill its function to *fill* gaps in international law, but would instead create new gaps.[259]

---

251. *See* Addis, *supra* note 235, at 127-28 (discussing a similar development in the context of political agendas).

252. Nolan & Sourgens, *supra* note 31, at 510-13, 521-22.

253. *Id.*

254. *Id.*

255. Barcelona Traction, Light and Power Co., Ltd. (Belg. v. Spain), 1970 I.C.J. 3, 66 (Feb. 5) (separate opinion of Fitzmaurice, J.).

256. International Status of South West Africa, Advisory Opinion, 1950 I.C.J. 128, 148 (July 11) (separate opinion of McNair, J.); *see* Gerald Fitzmaurice, *The Law and Procedure of the International Court of Justice, 1951-1954: General Principles and Sources of Law*, 30 BRIT. Y.B. INT'L L. 1, 18-19 (1953) (discussing the separate opinion of McNair, J.); *see also* Barcelona Traction, 1970 I.C.J. at 66 n.4 (Feb. 5) (separate opinion of Fitzmaurice, J.) (supporting the analysis of general principles by McNair, J.).

257. *South West Africa*, 1950 I.C.J. at 148 (separate opinion of McNair, J.).

258. Fitzmaurice, *supra* note 256, at 22 ("[I]t must be assumed that Article 38 was intended to recite or place on record only those elements which, under existing international law, were already material to any decision purporting to be given 'in accordance with international law.'").

259. *See* LAUTERPACHT, *supra* note 31, at 93.

The jurisprudence of the Court means further that any principle should also be compared to analogous rules of international law. If there is significant convergence between analogous rules of international law and the general principle to be introduced, adoption of the general principle as part of international law would truly fill a gap.[260] It would extend the logic of existing prescriptions to an area that remains underdeveloped in international law.[261] This extension would be consistent with reasonable state expectations precisely because it does not impose truly new obligations.[262] Rather, it gives full effect to the meaning of existing international legal obligations.[263]

III. THE PRIVACY PRINCIPLE

The remainder of the Article is devoted to proving the Privacy Principle. Section III.A will first address the choice of sources for establishing the Privacy Principle. It will next show that a critical mass of these source jurisdictions suggest that invasion of privacy is tortious conduct. It will confirm and strengthen this principle through a functional legal comparison of the legal systems examined. It will also argue that the Privacy Principle should be adopted as part of international law because of the yet under-determined contours of the law of espionage and the theoretical coherence of the Privacy Principle with human rights law.

The latter portion of this Part will establish that the Privacy Principle can rely upon a consistent definition of privacy from domestic law and that the domestic law definition of privacy is consistent with policies underlying international law. Finally, the last Section will supply the scope of permissible state intrusion into privacy on the basis of the private law principle of necessity and the international legal principle of proportionality.

A. *Selection of Legal Systems*

The first step to prove the existence of a general principle is to select sources for examination. The Article will look to the laws of the United States, France, the People's Republic of China, the Russian Federation, Iran, and Israel. These jurisdictions capture a reasonable diversity in legal traditions,[264] cover a broad geographic range, and encompass a significant cultural diversity.[265]

---

260. *See id.*

261. *South West Africa*, 1950 I.C.J. at 148 (separate opinion of McNair, J.).

262. Fitzmaurice, *supra* note 256, at 22.

263. *See* LAUTERPACHT, *supra* note 31, at 93.

264. *See* H. PATRICK GLENN, LEGAL TRADITIONS OF THE WORLD: SUSTAINABLE DIVERSITY IN LAW 266 (2010) ("Common law thinking retains a vital place in U.S. law."); *id.* at 147 (noting the place of France in the spectrum of civil law jurisdictions); *id.* at 349-50 ("Just as communism had to bend to deep-rooted east Asian thought, however, so too is western-style law clearly the object of confucianization, as filtered through communist authority [in the People's Republic of China]."); Tamar Gidron, *Israel*, *in* MIXED JURISDICTIONS WORLDWIDE: THE THIRD LEGAL FAMILY 577, 578 (Vernon Palmer ed., 2012) ("Israeli private law has moved considerably from its common law origin and may now be classified as primarily reflecting concepts that derive from the civil law world."); A.L. Makovsky, *Preface to the English Translation* of THE CIVIL CODE OF THE RUSSIAN FEDERATION, at xlix, li (Peter Maggs & A.N. Zhiltsov eds. & trans. 1997) ("The new Civil Code neither repeats nor copies the civil and commercial codes and statutes of other countries. It has its own 'personality,' with its own vir-

This choice of jurisdictions is by no means exhaustive. It is driven by an examination of representative legal systems equipped with significant signals intelligence capabilities.[266] An agreement among these global leaders is going to carry the greatest authority vis-à-vis possible repeat offenders against the principle in question.[267] It is also the likely source of the most engagement with privacy questions at the domestic level given the availability of sophisticated technology to these states and the private residents under their jurisdiction.[268]

The principle developed below will be drawn from the private law of the legal systems examined. This focus upon private law comparison differs from the predominant focus upon public law in signals intelligence scholarship.[269] The choice of private law is consistent with the generation of a significant number of general principles in recent jurisprudence of the International Court of Justice.[270] Historically, many if not most general principles had some Roman civil law derivation.[271] The focus upon private law therefore has pedigree.

It is further important that for understandable policy reasons, public law forays into regulating surveillance—particularly extraterritorial surveillance—have been comparatively weak in generating robust protections.[272] The state has an understandable interest in reducing barriers to its own intelligence collection. There being no constituents to complain about foreign data collection, ordinary democratic checks on governmental overreach are at a minimum.[273]

---

tues and vices."); William Tetley, *Mixed Jurisdictions: Common Law v. Civil Law (Codified and Uncodified)*, 60 LA. L. REV. 677, 679 (2000) (listing Iran as a "mixed jurisdiction . . . partly derived from non-occidental legal traditions").

265. *See* sources cited *supra* note 264.

266. Nicole Perlroth, *Google Says It Has Uncovered Iranian Spy Campaign*, N.Y. TIMES (June 12, 2013, 6:36 PM), http://bits.blogs.nytimes.com/2013/06/12/google-says-it-has-uncovered-iranian-spy-campaign/ (describing sophistication of Iranian internet surveillance capabilities); *see also* Henry Porter, *The West is Moving Towards China in Its Quest for Mass Surveillance*, OBSERVER (June 8, 2013), https://www.theguardian.com/commentisfree/2013/jun/08/west-china-mass-surveillance (discussing the size of US and Chinese surveillance efforts); David Shamah, *Israeli Authorities Use Far Wider Surveillance Powers than Those Causing Storm in US*, TIMES OF ISRAEL (June 9, 2013), http://www.timesofisrael.com/israeli-authorities-use-far-wider-surveillance-powers-than-those-causing-storm-in-us/ (describing scope of Israeli signals intelligence); Shaun Walker, *Russian Data Law Fuels Web Surveillance Fears*, GUARDIAN (Sept. 1, 2015), https://www.theguardian.com/world/2015/sep/01/russia-internet-privacy-laws-control-web; Kim Willsher, *France Approves 'Big Brother' Surveillance Powers Despite UN Concern*, GUARDIAN (July 24, 2015), https://www.theguardian.com/world/2015/jul/24/france-big-brother-surveillance-powers (describing French signals intelligence programs).

267. *See* Right of Passage over Indian Territory (Port. v. India), 1960 I.C.J. 6, 44 (Apr. 12) (stating that specific practice between states dispenses with the need to have regard for customary international law or general principles of law); Nolan & Sourgens, *supra* note 31, at 510 (discussing same).

268. *See* sources cited *supra* note 229.

269. *See* Deeks, *supra* note 61, at 343-45 (arguing that international policy guidance can be derived from domestic surveillance statutes); Deeks, *supra* note 89, at 28-36 (submitting that domestic statutes provide one predicate for peer constraint in the intelligence community).

270. *See* Nolan & Sourgens, *supra* note 31, at 525-28 (cataloguing recent jurisprudence).

271. *See* OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 54 (1991) (noting cynically that "expressing tautologies in Latin apparently adds to their weight in judicial reasoning"); Randall Lesaffer, *Argument from Roman Law in Current International Law: Occupation and Acquisitive Prescription*, 16 EUR. J. INT'L L. 25, 29 (2005) (noting the intended private law grounding of general principles of law).

272. *See* sources cited *supra* note 269.

273. *See* Sidney A. Shapiro, *Why Administrative Law Misunderstands How Government Works: The Missing Institutional Analysis*, 53 WASHBURN L.J. 1, 12-13 (2013) (discussing the link be-

Public law on this issue is therefore the least neutral means to assist in formulating a principled approach for much the same reason that *nemo iudex in propria sua causa*: the state is simply not a disinterested or otherwise accountable actor with regard to foreign intelligence gathering.[274]

This lack of accountability has functional consequences. The right of people to exclude the state from their personal affairs is typically governed by public law: criminal procedure, authorizing statutes, and administrative regulation.[275] Police powers permit the state to intrude into the personal affairs of its subjects far more readily than would otherwise be allowed in orderly civil relations.[276] The state's broader margin of action under public law relies upon a functional premise: the state acts in the public interest, including the interest of the people intruded upon, to keep the public safe.[277]

This functional premise fails when the state acts extraterritorially with regard to foreign nationals. The state no longer acts in the public interest: the interest of those intruded upon as well as the public at large.[278] The state acts in self-interest when spying upon foreigners in a foreign land.[279] The state does not seek to protect the foreigner, nor would it have any jurisdiction to do so.[280] It seeks to protect only (or at least principally) itself and its subjects.[281]

When the state acts beyond its own territory, beyond its right to regulate, it slips into the position of everyman. The state's actions no longer benefit from regulatory right.[282] Extraterritorial conduct of the state is thus not a priori permissible as sovereign prerogative,[283] but nor is it a priori impermissible as in-

---

tween democratic accountability and administrative law posited in some U.S. administrative law scholarship).

274. *See* CHENG, *supra* note 195, at 284 (discussing the rationale for the general principle).

275. *See* Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 1538 (2014) (noting the public law nature of surveillance laws); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 487 (2011) [hereinafter Kerr, *Equilibrium*] (arguing that "judges adjust Fourth Amendment protection to restore the preexisting level of police power").

276. Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 425 (2014).

277. *Id.*

278. Mark D. Rosen, *Extraterritoriality and Political Heterogeneity in American Federalism*, 150 U. PA. L. REV. 855, 878-82 (2002) (tethering the extraterritorial reach of police powers to state citizenship in the U.S. due process context).

279. *See, e.g.*, Jim Michaels, *NSA Chief: Surveillance Programs Protect Americans*, USA TODAY (June 13, 2013), http://www.usatoday.com/story/news/politics/2013/06/12/alexander-nsa-cyber-snowden/2415217/ (quoting the former Director of the National Security Agency, General Keith Alexander as saying "I think what we're doing to protect American citizens here is the right thing").

280. *Compare* Ronald J. Sievert, *War on Terrorism or Global Law Enforcement Operation?*, 78 NOTRE DAME L. REV. 307, 348 (2003) (discussing the scope of territorial, passive personality and protective principle jurisdiction), *with* JAMES R. CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 462 (8th ed. 2012) ("Ultimately, the identification of exorbitant jurisdiction may be a matter of knowing it when one sees it.").

281. *See* citations *supra* note 238.

282. *See* citations *supra* note 233.

283. *See* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1035-36 (2007) (noting the broad rejection of the *Lotus* principle in state practice).

terference in the internal affairs of its neighbors.[284] Rather, in the absence of a treaty or customary international law rule on point, the conduct is governed by the same principles of lawful intercourse in civil society and thus should be subject to civil law.[285]

Pragmatically, two concerns should further weigh in favor of a choice of private law. First, private law and public law on privacy are typically correlated. Louis Brandeis and Samuel Warren's article on *The Right to Privacy* radiated both in constitutional law and tort law in the U.S. and beyond.[286] Many of the regimes discussed below straddle the private/public law divide. As the state is more disinterested in the regulation of private intercourse, private law may frequently be a step ahead of public law in articulating liability rules for unwarranted intrusions into privacy. But the logic of private law, as Brandeis and Warren's article proves, is similarly at work in the public law setting.[287]

Second, looming in the background is the question of whether it makes a difference to distinguish between state and non-state actors in cyberspace.[288] One need not be a state to have significant hacking capabilities.[289] And states frequently hide behind non-state actors to deny involvement in their cyber misdeeds.[290] A private law premise for a general principle can easily serve as a baseline for broader transnational codification efforts.[291] These efforts would promise to regulate more than just state (mis)conduct. The Article harbors the hope to develop such a broader transnational framework in the future.

B. *A Formal Right To Privacy*

A formal comparison of the legal systems of the United States, France, the Russian Federation, the People's Republic of China, Israel, and Iran strongly supports the existence of a general principle of law. As discussed below, five of these legal systems expressly recognize a right to privacy as a matter of their private law, and one appears to be moving towards recognizing a privacy right.

This overlap in the formal acceptance of a right to privacy as such in private law is significant for critical mass. It suggests not only that there is signifi-

---

284. *See* Forcese, *supra* note 44, at 201 (noting the lack of judicial support or state practice to support that spying in general is an unlawful interference in internal affairs).

285. See LAUTERPACHT, *supra* note 31, at 93.

286. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 156 (2007) ("[B]oth *Botsford* and Brandeis's views of Fourth Amendment privacy were later used by the Court to help fashion the constitutional 'right to privacy.' In *Griswold v. Connecticut* and *Roe v. Wade*, the Court relied on the ideas first articulated in Warren and Brandeis's article to articulate the scope of the constitutional protection of privacy rights. Warren and Brandeis's conception of privacy thus did not just influence the privacy torts; it also had a wide-ranging effect on the law of privacy more generally.") (internal citations omitted).

287. *Id.*

288. *See* Mark Pomerleau, *State vs. Non-State Hackers: Different Tactics, Equal Threat?*, DEF. SYS. (Aug. 17, 2015), https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers-tactics.aspx (discussing state and non-state hacking threats to the U.S.).

289. *Id.*

290. David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. TIMES (Oct. 7, 2016), https://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html.

291. BERGER, *supra* note 244, at 71.

cant quantitative support for a privacy right, but also that the support materially overlaps in rationale. In terms of critical mass terminology, the convergence between legal systems has a high degree of doctrinal purity. Convergence with a high degree of purity is probative of the existence of a Privacy Principle.

1. *Legal Systems Recognizing a Private Law Right to Privacy*

Comparative law scholarship on privacy rights in the civil liability context confirms the near global agreement on the existence of a privacy right in domestic private law.[292] Formal comparison of the legal systems chosen as the baseline for this Article confirms this conclusion. Particularly, the domestic private laws of the United States, France, Russia, Israel, and China each recognize a right to privacy.

U.S. private law protects privacy by imposing civil liability for invasions of privacy.[293] U.S. common law premises such tort liability upon a distinct right to privacy.[294] The *Restatement (Second) of Torts* provides the most authoritative statement on the right of privacy in U.S. tort law.[295] The *Restatement* approach has been adopted by the predominant civil law jurisdiction in the United States, Louisiana, through judicial interpretation of the Louisiana Civil Code.[296] The *Restatement* states as follows:

(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

(2) The right of privacy is invaded by

(a) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or

(b) appropriation of the other's name or likeness, as stated in § 652C; or

(c) unreasonable publicity given to the other's private life, as stated in § 652D; or

(d) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.[297]

The French Civil Code, like U.S. law, recognizes an explicit right to privacy.[298] The French Civil Code, unlike the Louisiana Civil Code, protects pri-

---

292. *See* GERT BRÜGGEMEIER, MODERNISING CIVIL LIABILITY LAW IN EUROPE, CHINA, BRAZIL, AND RUSSIA: TEXTS AND COMMENTARIES 33 (2011) ("[N]owadays, despite remaining differences in individual instances, there is broad consensus on the protection of personality interests in civil liability law. . . . Privacy ('the right to be left alone') has become another key area of protection of the persona by liability law.").

293. *See* RODNEY A. SMOLLA, LAW OF DEFAMATION § 10.2 (2d ed. 2016) (noting the influence of the Prosser classification); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (setting out the four-fold division of the tort of privacy).

294. *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (theorizing the right to privacy as a tort law right).

295. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 907 (2009) ("Over the course of the twentieth century, and under the helpful influence of William Prosser, author of the relevant sections of the RESTATEMENT (SECOND) OF TORTS, nearly all states have recognized some branches of the tort right of privacy.").

296. *See* Jaubert v. Crowley Post-Signal, Inc., 375 So. 2d 1386, 1388-89 (La. 1979). For a discussion of current Louisiana law on point, see Patrick N. Broyles, Comment, *Intercontinental Identity: The Right to the Identity in the Louisiana Civil Code*, 65 LA. L. REV. 823, 848-63 (2005).

297. *See* RESTATEMENT (SECOND) OF TORTS §§ 652A-E (1977).

vacy by express codification rather than through the general provision on delictual liability.[299] Article 9 of the Civil Code states as follows:

Everyone has a right to the respect of her private life.

Judges may, without prejudice to compensation for damages suffered, order all measures appropriate to enjoin or put to an end the violation of the intimacy of private life; these measures, if urgent, can be ordered by one judge sitting in chambers.[300]

The post-Soviet Russian codification project similarly included a privacy protection since its very inception. This privacy protection, too, is couched as a right.[301] Article 150.1 of the Russian Civil Code provides:

The life and health, the personal dignity and personal immunity, the honour and good name, the business reputation, *the immunity of private life*, the personal and family secret, the right of a free movement, of the choice of the place of stay and residence, the right to the name, the copyright and the other personal non-property rights and non-material values, possessed by the citizen since his birth or by force of the law, *shall be inalienable and untransferable in any other way.*[302]

Israeli law incorporates privacy protection in private law through special legislation. The 1981 Protection of Privacy Law recognizes a right to privacy.[303] It makes infringement of privacy a civil wrong.[304] In relevant part, it creates liability for

(1) spying or trailing a person in a manner likely to harass him, or any other harassment;

(2) listening prohibited under the Law;

(3) photographing a person while he is in a private domain;

...

(5) copying the contents of a letter or other scripts not intended for publication, or the use of contents thereof, without the permission of the addressee or the writer, unless the script is of historical value and no more than fifteen

298. *See* Jeanne M. Hauch, *Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris*, 68 TUL. L. REV. 1219, 1231-42 (1994) (discussing the historical development of French civil law on privacy).

299. *Compare* CODE CIVIL [C. CIV.] [CIVIL CODE] at c (Fr.) (Dalloz 2015) (summarizing current jurisprudence on the right to privacy), *with* Jaubert v. Crowley Post-Signal, Inc., 375 So. 2d 1388-89 (interpreting the general delictual provision of the Louisiana Civil Code).

300. CODE CIVIL [C. CIV.] [CIVIL CODE] art.9 (Fr.).

301. Gadis Gadzhiev, *The Constitutionality of Civil Law Norms*, *in* PRIVATE AND CIVIL LAW IN THE RUSSIAN FEDERATION 91 (William Simons ed., 2009) (including the right to privacy in the civil rights codified as part of the 1993 Russian Civil Code).

302. GRAZHDANSKII KODEKS ROSSIISKOI FEDERAISII [GK] [CIVIL CODE] art. 150.1 (Russ.) (emphasis added).

303. *See* Tamar Gidron, *The Publicity Right in Israel: An Example of Mixed Origins, Values, Rules, Interests and Branches of Law*, 12 STELLENBOSCH L.R. 405, 407 (2007).

304. Protection of Privacy Law, 5741-1981 SH No. 1011, art. 4 (Isr.), available at http://www.wipo.int/wipolex/en/text.jsp?file_id=347462 ("An infringement of privacy constitutes a civil wrong, and the provisions of the Torts Ordinance [New Version] shall apply therein, subject to the provisions of this Ordinance."); *see also* Usama Halabi, *Legal Analysis and Critique of Some Surveillance Methods Used by Israel*, *in* SURVEILLANCE AND CONTROL IN ISRAEL/PALESTINE: POPULATION, TERRITORY, AND POWER 199, 202 (Elia Zureik et al. eds., 2011) (confirming tort status of the violation of the Law).

years have passed since the time when it was written; for this purpose, script – including an electronic message as defined in the electronic signature Law, 5761-2001;

...

(7) infringement of duty of confidentiality prescribed by law in respect of a persons private affairs;

...

(9) use or passing on of information on a persons private affairs, for a purpose other than which was prescribed;

(10) publication of or the passing of anything that was obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);

(11) publication of any matter that relates to a persons intimate life, including his sexual history, or state of health or conduct in the private domain.[305]

Finally, Chinese law since the 2009 adoption of the Tort Law has incorporated privacy protections in its private law.[306] Privacy protections again are couched in terms of an underlying privacy right.[307] Article 2 of the law states:

Those who infringe upon civil rights and interests shall be subject to the tort liability according to this Law.

"Civil rights and interests" used in this Law shall include the right to life, the right to health, the right to name, the right to reputation, the right to honor, right to self image, right of privacy, marital autonomy, guardianship, ownership, usufruct, security interest, copyright, patent right, exclusive right to use a trademark, right to discovery, equities, right of succession, and other personal and property rights and interests.[308]

2. *The Iranian Outlier*

Iran is an outlier jurisdiction in its treatment of privacy. As it stands, Iranian private law does not recognize a broad right to privacy as part of the civil

305. Protection of Privacy Law (Isr.), *supra* note 304, art. 2, *translated in Israel Protection of Privacy Law, 5741-1981*, WIPO, http://www.wipo.int/wipolex/en/text.jsp?file_id=347462 (last visited Apr. 14, 2017).

306. *See* Ann Bartow, *Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853, 854-56 (2013) (discussing the historical development of privacy law in China); Bo Zhao, *Posthumous Reputation and Posthumous Privacy in China: The Dead, the Law, the Social Transition*, 39 BROOK. J. INT'L L. 269, 284 (2014) (discussing the history and context of the provision).

307. *See* Jingzhou Tao & Gregory Louvel, *Latest Trends in Cloud Computing in China*, 15 No. 9 ELEC. BANKING L. & COM. REP. 12, 2 (2012) ("China's Tort Law recognizes the right to privacy as a stand-alone legal principle."); Zhao, *supra* note 306, at 284. *But see* Bartow, *supra* note 306, at 863 (treating privacy as a referenced concept rather than a right in Article 2).

308. Qinquan Zeren Fa, Tort Law (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010) (China), *translated in Tort Law of the People's Republic of China*, THE STATE COUNCIL, http://english.gov.cn/archive/laws_regulations/2014/08/23/content_281474983043584.htm (last visited Apr. 14, 2017).

code.[309] Further, Iran so far has not introduced private law statutory protections apart from the civil code directly protecting privacy rights.[310]

Despite this outlier status of Iran, it appears that Iran is moving towards the recognition of a right to privacy in private law.[311] As discussed in more detail in the context of functional legal comparison, Islamic law recognizes key principles central to the right to privacy.[312] Scholarship increasingly treats these concepts as part and in the language of a broader privacy right.[313]

3. *Conclusion*

Formal legal analysis showcases a significant convergence on the existence of privacy protections as a general principle of law. Significantly, the legal systems studied conceive of privacy as a right. This right to privacy has support from a diversity of legal traditions, including common law, civil law, and mixed jurisdictions. There is no regional trend rejecting the right to privacy. Cultural diversity between legal systems studied is not an impediment to the adoption of a right to privacy. All of this supports that the right to privacy is, indeed, a general principle of private law.

C. *Functional Comparison*

As discussed above, formal legal comparison is not in itself sufficient to support a general principle of law. Rather, it is necessary to establish by means of functional comparison whether the convergence of legal systems established on the basis of formal legal comparison provide a false positive. Further, functional comparison can increase the density of convergence by focusing upon specific functional problem solutions adopted by the various legal systems studied—as opposed to looking exclusively to legal form.

In this case, the need for functional comparison is made greater by the broad nature of the Privacy Principle itself. Relevant to the purpose of this Article, the mere fact that a Privacy Principle exists does not necessarily mean that it prohibits surveillance or that it prohibits the use of private information once gathered. These narrower questions require a functional comparison of the legal systems studied.

---

309. QANUNI MADANI [CIVIL CODE] Tehran 1314 [1935] (Iran).

310. *See* Mohammad Habibi Mojandeh, Privacy in Islam and Iranian Law (Nov. 30, 2007) (unpublished manuscript) (British Institute of Int'l & Comparative Law Workshop on Privacy), www.biicl.org/files/3198_dr__habibi_presentation.doc (last visited Apr. 14, 2017).

311. *Id.*

312. *See, e.g.*, Sadiq Reza, *Islam's Fourth Amendment Search and Seizure in Islamic Doctrine and Muslim Practice*, 40 GEO. J. INT'L L. 703, 792-95 (2009) (laying out a privacy theory of Islamic law); Kristen Stilt, *Islamic Law and the Making & Remaking of the Iraqi Legal System*, 36 GEO. WASH. INT'L L. REV. 695, 697 (2004) ("Islamic law is the supreme law of the land in Iran.").

313. *See, e.g.*, Ansari Bagher, *Protection of Privacy in Islam and Iran's Legal System (Comparative Study)*, 2005 L.Q. J. FAC. L. & POL'Y SCI. 1 (2005) (introducing a privacy right rationale to Iranian law); Kamal Halili Hassan & Parviz Bagheri, *Data Privacy in Electronic Commerce: Analyzing Legal Provisions in Iran*, J. INTERNET BANKING & COM. (Jan. 15, 2016), http://www.icommercecentral.com/open-access/data-privacy-in-electronic-commerce-analysing-legal-provisions-in-iran.php?aid=67480.

1. *The Potential False Positive*

The comparative analysis so far has hidden from view that the right to privacy in the private law of the legal systems studied varies significantly from jurisdiction to jurisdiction. Two functional divergences are particularly significant. *First*, while there is convergence upon the existence of a right to privacy, legal systems differ significantly upon the function of this right. *Second*, and as a natural result of the different function of the right to privacy in the legal systems studied, the standards according to which liability for violation of the right to privacy are established also differ greatly. Both of these differences raise the potential that formal analysis of the right to privacy in private law leads to a false positive.

First, a functional analysis of the place of privacy in the private law of the legal systems studied reveals three different rationales for the privacy right. In some jurisdictions, privacy functions as a negative right.[314] The right to privacy exists only because of a corresponding prohibition or duty.[315] By analogy, traffic rules provide a coherent set of duties on all motorists that coherently allow one to derive a right of reasonable safe-travel on public streets—the right to be free from unsafe driving by others, not to drive unimpeded.[316] The United States' treatment of privacy paradigmatically treats privacy as such a negative right.[317] The essence of the right to privacy is the prohibition of others to intrude.[318] Liability then is premised upon some form of intentional conduct or fault in intruding.[319] Of the legal systems studied, the United States, Israel, and China adopt this rationale.[320]

In some jurisdictions, privacy functions as a form of right of autonomy.[321] The point of privacy is not to keep others out so much as to have a right in one's personhood.[322] French law is firmly part of this tradition by treating privacy as a moral right, part and parcel of personhood itself.[323] The practical con-

---

314. *See* 62A AM. JUR. 2D *Privacy* § 1 (2016) (defining privacy as freedom from intrusion).

315. *See* Robin West, *Rights, Capabilities, and the Good Society*, 69 FORDHAM L. REV. 1901, 1920 (2001) (defining negative right as a "freedom from").

316. *See* C. Edwin Baker, *Unreasoned Reasonableness: Mandatory Parade Permits and Time, Place, and Manner Regulations*, 78 NW. L. REV. 937, 1005 (1987) (discussing rights in the context of traffic rules).

317. *See Privacy*, *supra* note 314.

318. *Id.*

319. *Id.*

320. *Id.*; Protection of Privacy Law, 5741-1981, S.H. 1011 p. 1284 (Isr.); Qinquan Zeren Fa, Tort Law (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010) (China), *translated in Tort Law of the People's Republic of China*, THE STATE COUNCIL, http://english.gov.cn/archive/laws_regulations/2014/08/23/content_281474983043584.htm (last visited Apr. 14, 2017).

321. *See* Jonathan Kahn, *Privacy as a Legal Principle of Identity Maintenance*, 33 SETON HALL L. REV. 371, 381-82 (2003) (discussing the link between privacy and autonomy).

322. *See id.*

323. *See* HUW BEVERLY-SMITH ET AL., PRIVACY, PROPERTY, AND PERSONALITY, CIVIL LAW PERSPECTIVES ON COMMERCIAL APPROPRIATION 152 (2005) ("Privacy belongs to the moral patrimony of every physical person and constitutes, like his image, the continuation of his personality." (quoting Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Seine, Jan. 23, 1966, ICP 1966, II, 14875 (Fr.)).

sequence is that the right to privacy becomes stronger and inalienable.[324] As one author put it, as a matter of French law, alienating privacy is akin to committing suicide.[325] Of the legal systems studied, French law adopts such a rationale.[326]

Finally, the protection of privacy can be an incidental consequence of liability imposed upon undesirable conduct. There is a prohibition against intruding, but it is too dispersed to permit the formulation of a coherent right. By analogy, the existence of fouls in football is not sufficiently coherent to permit the formulation of a right not to be injured playing the game.[327] This is the approach of Islamic law.[328] Here, privacy protection is at its weakest.

The theoretical difference has significant practical implications. French law creates an absolute right of privacy.[329] It uses a strict liability regime for privacy.[330] One example of this approach is that a person retains the right to revoke consent for publication of his or her image even after the image has entered into the public domain.[331] U.S. law, on the other hand, does not create strict liability for invasions of privacy.[332] It looks to intent and fault in determining liability.[333] Reasonable, not outrageous, invasions of privacy are tolerated.[334] One consequence of this approach is that a person can no longer enjoin the publication of personal information after the information has entered into the public domain.[335]

These differences call into question how robust the convergence of a right to privacy in private law is. It thus requires a functional appraisal of comparative legal systems. This functional appraisal will need to determine the density of legal systems studied when addressing specific types of conduct impacting privacy.[336] In areas of dense convergence, the existence of a privacy principle can be deduced then not only in theory, but also in its specific meaning and prescription.

---

324. *See* Cyrill P. Rigamonti, *Deconstructing Moral Rights*, 47 HARV. INT'L L.J. 353, 361 (2006) ("[M]oral rights are *inalienable* in the sense that they can be neither transferred to third parties nor relinquished altogether.").

325. *See* Hauch, *supra* note 298, at 1230 ("The late Professor Desbois felt that an author's renunciation of the defense of his personality by attempted alienation of his moral rights was tantamount to a 'moral suicide,' which public policy could not allow.").

326. CODE CIVIL [C. CIV.] [CIVIL CODE] art. 9 (Fr.).

327. *See* Benedict Carey, *Study Focuses on Repeated Hits, Not Concussions*, N.Y. TIMES (Mar. 31, 2016), http://www.nytimes.com/2016/04/01/health/study-focuses-on-repeated-hits-not-concussions.html.

328. *See* Reza, *supra* note 312, at 792-95 (laying out a privacy theory of Islamic law).

329. Hauch, *supra* note 298, at 1234.

330. *Id.*

331. Peter Yu, *Moral Rights 2.0*, 1 TEX. A&M L. REV. 873, 895 (2014) (discussing the moral right of withdrawal or retraction).

332. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1828-29 (2010) (discussing the requirement of conduct 'highly offensive to the reasonable person').

333. *Id.*

334. *Id.*

335. RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977) (pointing in its case notes to Reuber v. Food Chemical News, Inc., 925 F.2d 703, 719 (4th Cir. 1991) for the proposition that "if information is already in the public domain when published by a defendant, it does not qualify as private facts").

336. Nolan & Sourgens, *supra* note 31, at 519-22.

2. *Surveillance as Wrongful Invasion of Privacy*

The first relevant fact scenario concerns surveillance. Do the legal systems studied treat surveillance conducted without consent by a hacker as a violation of privacy in private law? This fact scenario most closely resembles existing signals intelligence programs gathering information either through reviewing the electronic footprint left by a person's telephone calls as well as in email and chat rooms, or alternatively using computer cameras to gather intelligence on the person's home.[337]

Each of the legal systems examined would treat such surveillance as a violation of privacy rights under private law. Beginning with the outlier jurisdiction of Iran, Quranic legal principles prohibit intrusion in the home.[338] They further prohibit suspicion, spying, and backbiting.[339] Scholarship has extended these prohibitions to electronic data and traced them through existing statutory Iranian provisions addressing data privacy as a matter of public law.[340] All of these principles can be made actionable under Article 1 of Iran's Civil Liability Code.[341] The current scholarly developments on data privacy in particular support that the physical or virtual means of spying is not dispositive in the establishment of a wrongful act for invasion of privacy.[342]

U.S. law would treat the hypothetical fact scenario as an intrusion upon seclusion.[343] As one court applying the intrusion upon seclusion tort in the cyber context representatively explained:

> The elements of a cause of action for invasion of privacy by intrusion on seclusion or private affairs are: (1) the defendant intentionally intruded on the plaintiff's soli-

---

337. Glenn Greenwald, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data ("The NSA access is part of a previously undisclosed program called PRISM, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says."); Kim Zetter, *How to Keep the NSA from Spying Through Your Webcam*, WIRED (Mar. 13, 2014), https://www.wired.com/2014/03/webcams-mics/ ("According to *The Intercept*, the NSA uses a plug-in called GUMFISH to take over cameras on infected machines and snap photos. Another NSA plug-in called CAPTIVATEDAUDIENCE hijacks the microphone on targeted computers to record conversations.").

338. QURAN 24:27-28 (M.H. Shakir trans.). For a discussion of the legal implications of the passage, see Reza, *supra* note 312, at 792-95.

339. QURAN 49:12 (M.H. Shakir trans.). For a discussion of the legal implications of the passage, see Habibi, *supra* note 310, at 3-4.

340. Hassan & Bagheri, *supra* note 313 (citing HAMIDREZA ASLANI, INFORMATION TECHNOLOGY LAW (2006)).

341. TASBIT MADANI [CIVIL LIABILITY CODE] Tehran 1960, art. 1 (Iran), http://policy.mofcom.gov.cn/GlobalLaw/english/flaw!fetch.action?libcode=flaw&id=83a23796-812e-401c-a516-e543c7675029&classcode=431 ("Any one who injures intentionally or due to his negligence, the life or health or property or freedom or prestige or commercial fame or any other right established for the individuals by virtue of law, as a result of which another one sustains materially or spiritually losses, shall be liable to compensate the damages arising out of his action."). The logic of importing the shari'a based privacy principle into general tort law follows the logic of civil law courts interpreting similar provisions in France and Louisiana in the absence of a specific privacy right. *See* Jaubert v. Crowley Post-Signal, Inc., 375 So. 2d 1386, 1388-89 (La. 1979); Tribunal de première instance [TPI] [ordinary court of original jurisdiction] Seine, June 16, 1858, D.P. III 1858, 52 (also known as the "The Rachel Affair").

342. Hassan & Bagheri, *supra* note 313 (citing HAMIDREZA ASLANI, INFORMATION TECHNOLOGY LAW (2006)).

343. *See* RESTATEMENT (SECOND) OF TORTS, *supra* note 335.

> tude, seclusion, or private affairs, and (2) the intrusion would be highly offensive to a reasonable person. The court concludes that hacking into a person's private computer and stealing personal correspondence would represent an intentional intrusion on the victim's private affairs and that such an intrusion would be highly offensive to a reasonable person.[344]

Israeli law expressly prohibits intrusion upon seclusion.[345] Following United States tort law, it does not matter that the intrusion is virtual as opposed to physical.[346] Surveillance operations would meet the fault requirements of Israeli law.[347] The key exception provided for Israeli law concerns intrusion upon seclusion under color of law.[348] This exception applies only to Israeli government actors.[349] Consequently, *foreign* surveillance activity would violate Israeli private law.

Chinese privacy protections are treated as significantly less robust than those protections extended by other jurisdictions.[350] The principal focus of literature raising this concern is privacy protection of Chinese citizens against cyber-surveillance by their own government;[351] it thus engages in a public law focused analysis.[352]

The private law focus of the Privacy Principle here is helpful in overcoming this concern: recent codification efforts in China show a clear commitment to privacy protections in private law.[353] Chinese tort law would treat surveillance activity under the general privacy tort.[354] Chinese law does not distinguish between virtual and physical conduct, using the term "infringe" as the predicate of liability.[355] Internet-based invasions of privacy are expressly contemplated invasions of privacy by the law.[356]

Russian privacy protections, just like Chinese privacy protections, are treated with some skepticism in the literature.[357] Again, this literature tends to focus on public law—the protection of people in Russia against intrusion into privacy by their own government.[358] The issue again looks different in the con-

---

344. Coal. for an Airline Passengers' Bill of Rights v. Delta Airlines, 693 F. Supp. 2d 667, 675 (S.D. Tex. 2010).

345. Gidron, *supra* note 303, at 4.

346. Halabi, *supra* note 304, at 204.

347. *Id.*

348. *Id.*

349. *Id.*

350. Fry, *supra* note 54, at 480-81 (discussing the limited privacy protections available as a matter of Chinese law).

351. *Id.*

352. *Id.*

353. Qinquan Zeren Fa ,Tort Law (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010) (China).

354. *Id.*

355. *Id.*

356. Connie Carabucci & Mark Parsons, *E-Commerce in China – How Can You Get a Piece of the Action?*, 14(6) E-COM. L. REP. 8, 12 (2012) ("Though there is no comprehensive data privacy law in China at present, the 2010 Tort Law introduced a general right to privacy, including specific rights against the misuse of personal information on the internet.").

357. *See* Anupam Chander & Uyên P. Lê, *Data Nationalism,* 64 EMORY L.J. 677, 701-02 (2015) (discussing recent Russian legislation permitting the FSB to emulate data collection programs akin to U.S. NSA models).

358. *Id.*

text of private law. Privacy is expressly treated as a non-material value in the Russian Civil Code.[359] This treatment is analogous to the creation of a moral right.[360] On its face, there appears to be no need to prove intent or fault.[361] Further, virtual conduct has been recognized as a violation of the private law privacy right.[362]

Finally, one aspect of French privacy law is its prohibition of intrusion upon seclusion.[363] This prohibition extends not just to physical but also virtual reality.[364] So long as the surveillance captures private information, it violates the broad rights-based approach of French law.[365]

In sum, there is complete agreement among the legal systems studied that virtual surveillance is a potential violation of the privacy right. The core question will be whether surveillance captures something private. Further, an invasion of privacy might otherwise be excused as proportionate. As a general rule, however, there is complete convergence upon a Privacy Principle in private law considering virtual surveillance activity of private conduct or information as wrongful.

3. *Use of Private Information as Wrongful Invasion of Privacy*

The next question is whether use of private information is also wrongful. Is it an additional violation of the Privacy Principle for a hacker to not just gather information, but to use it as well? The three most likely scenarios for such actions are the publication of the information obtained, the use of the information for purposes of blackmail, and identity theft.

All of the jurisdictions examined deem the publication of private information or images a private wrong.[366] The core difference between the different

---

359. GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII [GK RF] [Civil Code] art. 150.1 (Russ.).

360. *See Individual Freedom and Civil Rights*, *in* CIVIL HUMAN RIGHTS IN RUSSIA: MODERN PROBLEMS OF THEORY AND PRACTICE 47-49 (F. M. Rudinski ed., 2008) (discussing the relationship between "non-material" rights and values and moral rights in French law).

361. *See* GRAZHDANSKII KODEKS ROSSIISKOI FEDERATSII [GK RF] [Civil Code] art. 12 (Russ.) (requiring only proof of violation of the right in question, not the intent or fault of the infringer).

362. *See* Trevor McDougal, *Establishing Russia's Responsibility for Cybercrime Based on its Hacker Culture*, 11 B.Y.U. INT'L & MGMT. REV. 55, 56-58 (2015) (outlining the existing Russian cybernetic legal regime); *Russia, New Privacy Protection Law*, LIBRARY OF CONGRESS (Nov. 5, 2013), http://www.loc.gov/law/foreign-news/article/russia-new-privacy-protection-law/ (discussing new privacy law amendments to the Civil Code).

363. *See* VIRGINIE LARRIBAU-TERNEYRE, DROIT CIVIL, INTRODUCTION BIEN PERSONNE FAMILLE ¶ 763 (2015) (arguing that respect for private life implies the inviolability of the home and correspondence; and discussing new privacy law amendments to the Civil Code).

364. Cour de cassation [Cass.] [Supreme Court for Judicial Matters] soc., Oct. 2, 2001, Bull. civ. V, No. 291 (Fr.) (Nikon Case).

365. *Id.*

366. *See* RESTATEMENT (SECOND) OF TORTS § 652D (establishing liability as a matter of U.S. law); GUOSONG SHAO, INTERNET LAW IN CHINA 161 (2012) (arguing that publication of private facts without consent creates liability under the right to privacy as a matter of Chinese law); Tamar Gidron, *Privacy Protection as a Case Study in Personal Rights Protection in Israeli Law*, 28 COMPUTER L. & SEC'Y REV. 283, 287 (2012) (discussing Israeli law); Habibi, *supra* note 310, at 5-6 (establishing liability as a matter of Islamic Iranian law); Hauch, *supra* note 298, at 1246-49 (discussing French law); Scott Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights of Public Figures*, 49 AM. BUS. L.J. 125, 178 (2012) (same); Peter Roudik, *Russia: New Privacy Protection Law*, LIB. CONG.

legal systems concerns a situation in which the information was already independently in the public domain.[367] This distinction is reasonably less important in the surveillance context—here, the point is to gather and use non-public information.[368] With regard to such non-public information, the legal systems examined converge upon a general prohibition of publication without consent.[369]

The use of information for blackmail is similarly wrongful.[370] In the blackmail context, the principal cause of action may not always be one of invasion of privacy. Invasion of privacy would be the appropriate cause of action if the blackmailer made good on his or her threat and published the information in question.[371] If the blackmailer is paid off, theories of unjust enrichment or violation of duties of good faith may be more appropriate.[372]

Identity theft similarly is a civil wrong. Increasing the risk for identity theft (rather than committing identity theft) can be a violation of the right to privacy actionable in tort.[373] Committing identity theft is likely going to be treated under the heading of fraud or unjust enrichment rather than violation of the right to privacy.[374] Still, the underlying use of private information in the commission or preparation of identity theft remains a civil wrong.

Consequently, there is significant convergence that the use of private information is an independent wrongful act in violation of the right to privacy as conceived in the studied legal systems. Again, what remains to be resolved is what constitutes "private" information and if there are any affirmative defenses permitting the use of the information in question without consent. As a general rule, however, the Privacy Principle would consider the use of the fruits of virtual surveillance activity to be wrongful conduct.

(Nov. 5, 2013), http://www.loc.gov/law/foreign-news/article/russia-new-privacy-protection-law/ (discussing new privacy law amendments to the Civil Code).

367. *Compare* RESTATEMENT (SECOND) OF TORTS § 652D (1977) (stating that there is no liability as a matter of U.S. law if the information is in the public domain), *and* Gidron, *supra* note 366, at 288 (recounting Israeli case law to the same effect), *and* SHAO, *supra* note 366, at 161 (stating that there is no liability as a matter of Chinese law if the information is in the public domain), *with* Hauch, *supra* note 298, at 1246-49 (finding liability under these circumstances under French law), *and* Scott J. Shackelford, *supra* note 366 (same).

368. *See* Paul Rosenzweig et al., *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, HERITAGE FOUND. (May 13, 2016), http://www.heritage.org/research/reports/2016/05/maintaining-americas-ability-to-collect-foreign-intelligence-the-section-702-program (discussing the value of non-public communications intelligence gathered by the U.S.).

369. *See* sources cited *supra* note 367.

370. *See* CHENG, *supra* note 195, at 148-49 (noting the general principle of vitiating consent under duress).

371. *See* sources cited *supra* note 367.

372. *See* CHENG, *supra* note 195, at 148-49 (discussing international legal consequences of duress as a general principle of law).

373. *See* Protection of Privacy Law, 5741-1981, SH No. 1011 p. 128, art. 4 (Isr.) (treating confidentiality of database principals as a privacy right); Shqeirat v. U.S. Airways Group, Inc., 515 F. Supp. 2d 984, 998 (D. Minn. 2007) (noting that increasing the risk of identity theft is actionable as a violation of publication of private facts in U.S. law).

374. *See* CHENG, *supra* note 195, at 158 (discussing the general principle of fraud).

E. *Integrating the Privacy Principle in International Law*

The Article so far has established the existence of a Privacy Principle in private law. There is convergence in global private laws upon the existence of a *right* to privacy. Even in the face of doctrinal divergence on the meaning of this right, there is complete convergence among all the legal systems studied that the surveillance of persons in private is presumptively wrongful. There further is convergence among the legal systems studied that the use of private information—be it to publish the information, blackmail a person with the information, or otherwise rely upon the information to the subject's detriment—is an additional violation of the Privacy Principle.

Although the Article will not define precisely what "privacy" is protected by the Privacy Principle, it is reasonably clear that the Privacy Principle will have important ramifications for existing global surveillance programs.[375] Particularly, programs that rely upon the gathering and analyzing of global "big data" would be presumptively unlawful.[376] Such programs, it is natural to assume and the next Section will confirm, are bound to collect private information. The point of these programs is to act upon this information.[377] The Privacy Principle makes gathering this information and acting upon it presumptively wrongful.

1. *The Fit of the Privacy Principle in International Law*

The Privacy Principle, once fully developed, stands to fill the void in the legal literature identified in Part I. The problem, as expressed by the Group of Experts drafting the Tallinn Manual 2.0, is how to justify how "*notwithstanding State practice*, espionage remains subject to State's applicable human rights law obligation to respect the right to privacy."[378] As discussed in the context of customary international law, it is deeply problematic to posit a customary international law rule "notwithstanding State practice."[379] Similarly, it is questionable how such human rights treaty obligations might be said to govern extraterritorial surveillance programs over the continuous—and structurally insurmountable—objections of core signatories like the United States and other permanent members of the UN Security Council discussed above. Finally, existing treaty-drafting efforts analyzed above also were unlikely to yield meaningful privacy protections either when trying to coordinate intelligence gathering efforts or when seeking to harmonize privacy regimes in the commercial sector.

---

375. *See* Laura Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 152-53 (2015) (noting reports on NSA programs).

376. *See* Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 803-05 (2015) (discussing the difference between big data and small data surveillance methods).

377. *See* Donohue, *supra* note 375, at 152-53 (discussing current government programs); Hu, *supra* note 376, at 803-05 (same).

378. TALLINN MANUAL 2.0, *supra* note 28, at 193 (emphasis added).

379. *Id.*

The key point of the Privacy Principle is to recognize privacy as a right. It thus creates protections against intrusion no matter their source. It is no defense, in other words, that one intruded upon seclusion from abroad. The seclusion itself creates the jurisdictional nexus for the Privacy Principle to impose liability.[380]

The Privacy Principle can and must be integrated into general international law because it is entirely consistent with existing human rights law and jurisprudence. The privacy protections extended by the Privacy Principle are analogous to the interpretation of the right to privacy included in human rights treaties.[381] In that context, too, surveillance and use of private information are deemed presumptively wrongful unless it can be shown that state conduct did not affect private information or was otherwise excused.[382] Given this convergence between the right to privacy in human rights law and the Privacy Principle, they each are helpful to the establishment of the right to privacy as a general principle of international law.[383] This principle, importantly, would be globally applicable no matter the status of ratification of human rights instruments or interpretation of their scope of application.

The Privacy Principle cannot be displaced by reference to customary international law. As discussed in Part I, there is no readily available customary international legal prescription on surveillance. The absence of customary prescription in international law is not license for states to act out the limits of their physical and technological might with reckless abandon.[384] Quite to the contrary, the lack of treaty or customary prescription with regard to certain kinds of conduct calls for the establishment of a general principle of law to guide lawful state conduct and rein in sovereign abuse.[385]

The Privacy Principle is finally immune to criticism of legal "Occidentalism"—the view that international law imposes pernicious Western individualist values upon the rest of the world.[386] A recent joint declaration by Russia and the People's Republic of China accused much of international law of such an occidental bias.[387] The two countries instead sought to strengthen sovereign in-

380. *Compare* Sievert, *supra* note 280, at 348 (discussing jurisdiction), *with* BROWNLIE, *supra* note 280, at 462 (same).

381. Milanovic, *supra* note 23, at 137.

382. *Id.* at 139.

383. Nolan & Sourgens, *supra* note 31, at 522-23.

384. *Compare* Adams, *supra* note 29, at 403-04 (justifying the international legality of intelligence gathering by reference to the absence of a clear prohibition in international law enjoining such efforts, premised in the *Lotus* principle), *with* Abhimanju Jain, *The 21st Century Atlantis*, 50 STAN. J. INT'L L. 1, 32 (2014) ("The *Lotus* principle is now the subject of much criticism and is generally subordinated to the reverse-Lotus principle: that whatever is not permitted by international law is prohibited.").

385. LAUTERPACHT, *supra* note 31, at 93 (discussing the purpose of general principles as a source of international law).

386. Sundhya Pahuja, *The Post-Coloniality of International Law*, 46 HARV. INT'L L.J. 459, 461 (2005) (deconstructing Western claims to universal values in international law).

387. The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law, RUSSIAN MINISTRY OF FOREIGN AFFAIRS (June 25, 2016), http://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2331698; Lauri Mälksoo, *Russia and China Challenge the Western Hegemony in the Interpretation of International*

dependence and autonomy over internal affairs.[388] Whatever the merit of the joint declaration may be with regard to other areas of international legal prescription (and recent Western responses to events in Ukraine and Syria certainly give fodder for vivid disagreement on the role of international law in the world community), it cannot undercut the right to privacy. This right, as the establishment of the general principle has shown, is not a figment of the Western mind. It is a principle that has found support throughout diverse legal cultures and traditions (including Russia and China) and around the world.[389] The Privacy Principle thus confirms the original aspiration of the right to privacy in human rights law—it is truly universal, and truly a part of positive international law.[390]

2. *But Can a General Principle be Substantive?*

It remains to tackle a likely objection to the Privacy Principle. It might be argued that general principles of law are primarily procedural in nature (e.g., res judicata).[391] To the extent that a general principle should be recognized beyond such procedural rules, one would need to show an unquestionable convergence upon the principle in formulation and application. A Privacy Principle therefore, critics might argue, falls flat on its face.

Ultimately, the objection is not based in an understanding of general principles as they are recognized in international law today. Good faith is the paradigmatic example of a general principle.[392] Good faith is hardly a procedural obligation.[393] Similarly, the right of access to enclaved property (and thus a right of passage) is not procedural.[394] Existing jurisprudence further has recognized general principles in the context of tort law liability.[395] Commentary has submitted that human rights obligations are reflected in general principles of law.[396] This commentary has been confirmed in jurisprudence deeming that fair access to justice constitutes a general principle of law,[397] and further permitting

---

Law, EJIL: TALK! (July 15, 2016), http://www.ejiltalk.org/russia-and-china-challenge-the-western-hegemony-in-the-interpretation-of-international-law/.

388. See sources cited *supra* note 387.

389. *Id.*

390. G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.").

391. *See* Giorgio Gaja, *General Principles of Law*, *in* MAX PLANCK ENCYCL. PUB. INT'L L. (May 2013) (listing procedural general principles including res judicata).

392. *See* CHENG, *supra* note 195, at 105-62 (defining the general principle of good faith).

393. *Id.*

394. *See* Right of Passage Over Indian Territory (Port. v. India), 1960 I.C.J. 6, 136 (Apr. 12) (dissent of Fernandes, J.).

395. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, 324, 354-55 (Nov. 6) (separate opinion of Simma, J.).

396. Simma & Alston, *supra* note 197, at 102-10; Gaja, *supra* note 391.

397. Dr. Horst Reineccius et al. v. Bank for International Settlements, 23 R.I.A.A. 252, 291 ¶ 126 (Perm. Ct. Arb. 2003).

the inference that such access to justice correlates to the protection of substantive rights from arbitrary and discriminatory government interference.[398]

Further, general principles do not look to an absolute overlap of legal systems. In practice, the principle of good faith has been incorporated into international law despite the fact that it was not recognized in English common law.[399] The establishment of a general principle resembling requirements of substantive due process might raise objections from at least some U.S. constitutional lawyers.[400] These objections have not stood in the way of crystalizing general principles of law in international jurisprudence.

More fundamentally, the objections fail in the context of privacy protections given the significant overlap in the recognition of a privacy *right*. This discourse then is backed by a functional overlap that would at the very least apply the right to the kind of surveillance activity at issue in this Article. As discussed above, it is certainly true that different source systems disagree on the ultimate derivation and full implementation of privacy. But this fact of different theoretical justifications for the privacy right in the respective source systems is a strength rather than a weakness. The Privacy Principle is not thinly supported by requiring that legal systems take exactly the same steps to reach its normative conclusion. It robustly survives different outlooks, derivations, and approaches. The Privacy Principle is not a Rubik's Cube that must always be solved just so.[401] It is like the map of an ancient city that allows people to arrive at the same destination using different, well-trodden, and equally meaningful paths.

3. *The Value of the Privacy Principle*

The value of the Privacy Principle is to step into a normative gap and provide firmer formal and functional rationales for extraterritorial privacy protection in international law. As a formal matter, the most the objection to the human rights treaty or customary international law paradigm has been able to establish is the absence of treaty obligations or customary rules establishing privacy rights against global surveillance programs.[402] Objectors have not been able to prove that there exists an affirmative right of the state to conduct such activities under international law.[403]

To overcome this formal objection against the establishment of a privacy right, it is thus only necessary to prove the existence of a source of law that yields the desired prescription without running afoul of the technical defect af-

---

398. Merrill & Ring Forestry LP v. Canada, ICSID Case No. UNCT/07/1, Award, ¶ 187 (Mar. 31, 2010).

399. Zimmerman & Whittaker, *supra* note 225, at 39-40.

400. *See* Joshua D. Hawley, *The Intellectual Origins of (Modern) Substantive Due Process*, 93 TEX. L. REV. 275 *passim* (2014) (outlining the heated debate surrounding the concept in U.S. jurisprudence).

401. *See* Niall Firth, *Google Cracks Rubik's Cube by Proving Only 20 Moves Ever Needed to Solve It*, DAILY MAIL (Aug. 13, 2010), http://www.dailymail.co.uk/sciencetech/article-1302414/Study-uncovers-possible-Rubiks-Cube-solution-Only-20-moves-needed.html.

402. *See* Adams, *supra* note 29, at 403-04 (discussing the *Lotus* principle).

403. *See id.*

fecting its siblings.[404] A general principle meets this requirement.[405] It derives an international law rule that cannot be outmaneuvered by reference to incongruent state practice in foreign affairs. It does so by providing a different source other than such outward state conduct as the voluntarist hook for the recognition of an international legal obligation: the state's own domestic law.

The value of a general principle, however, goes deeper than clever technicality. The insight of a host of legal publicists that privacy protections are binding "notwithstanding state practice" points to the importance of the privacy right for international law, as such.[406] Leading international jurists see privacy rights—and the extension of privacy rights into the new world of cyberspace—as an essential characteristic of what international law must be.[407] In civil law terms, these jurists reason by legal analogy that the extension of privacy protections to this new prescriptive frontier is a necessary feature of the logic of the law as a whole.[408] To deny privacy protections on purely voluntarist grounds would be to misunderstand the normative force of the human rights edifice the world has created since the end of, and to respond to the atrocities of, the Second World War.[409]

General principles of law were precisely introduced to permit such essentialist, analogical reasoning to bear fruit. As Bin Cheng noted in his seminal work on general principles, their inclusion within the list of recognized sources of international law had deeply naturalist underpinnings.[410] These naturalist underpinnings did not devolve law into moral philosophy, or worse, metaphysics.[411] Rather, it permitted an outlet by which law could close gaps by analogical reasoning, as Hersch Lauterpacht has urged.[412] General principles therefore are the intended source of law to give force to normative principles so deeply enwoven in the fabric of international law that to imagine international law without them would be to unravel it.[413]

In other words, hosts of the most highly esteemed publicists in international law did not err in their assessment that international law must extend meaningful privacy protections to cyberspace.[414] The use of general principles, however, provides a better outlet for their insight. And in this case, reliance upon general principles provides more than a means to justify an essentialist *desideratum*. As demonstrated in the prior sections, it provides concrete evidence

404. *See* LAUTERPACHT, *supra* note 31, at 93 (discussing the purpose of general principles as a source of international law).

405. *See id.*

406. TALLINN MANUAL 2.0, *supra* note 28, at 193.

407. *See id.*

408. *See* James L. Dennis, *Interpretation and Application of the Civil Code and the Evaluation of Judicial Precedent*, 54 LA. L. REV. 1, 11-12 (1993) (discussing the use of analogy in civil code jurisdictions).

409. Molly Beutz Land, *Protecting Rights Online*, 34 YALE J. INT'L L. 1, 2 (2009).

410. CHENG, *supra* note 195, at 3-4, 19.

411. *Id.*

412. *Id.* at 19; LAUTERPACHT, *supra* note 31, at 93.

413. *See* Simma & Alston, *supra* note 197, at 105 (discussing use of general principles in the human rights context).

414. *See supra* Section I.A.1 (outlining the literature of privacy right proponents).

for the inductive establishment of a privacy right on the basis of contemporary convergence upon this principle by widely diverse legal systems. It thus showcases that privacy is not simply a legal mirage reflecting the Western (or more precisely Roman) undergirding of the law of peoples. It is a principle of legality recognized across the legal traditions of many of the principal detractors of a broader conception of the human right to privacy in cyberspace.

IV. DEFINING PRIVACY

The discussion so far has established that domestic private law recognizes a general principle of law on privacy. Further, this Privacy Principle is compatible with, and furthers principles inherent in, international law. A core functional question that so far has remained unaddressed is whether there is in fact a consistent definition of privacy in domestic private law to which the principle could be applied – and whether this definition, in turn, is compatible with international law. This Part takes up each of these questions in turn.

A. *Definition of Privacy in Private Law*

Current comparative legal research confirms the existence of a common definition of privacy in domestic private law.[415] As a recent study succinctly explained

> Privacy guarantees the protection of quasi-spatial areas ('private/ intimate sphere'), in which other private persons, the media, or the State are not permitted to intrude upon without consent. The unauthorized intrusion can manifest itself in different ways: through eavesdropping with a technical device, through photographing and filming with a telephoto lens, video camera, or night vision devices; through reading (and publishing) of private records (diaries, private correspondence, etc.) or through online searching of private electronic information systems. A further subcategory of privacy is the interest in anonymity, i.e., not to be dragged into public light against his/ her will.[416]

Privacy, in other words, concerns first and foremost non-public spaces.[417] Further, it concerns intimate or personal subject matters.[418] When combined, both of those factors give rise to a reasonable expectation of seclusion.[419] It is these expectations that the law protects.[420]

As discussed below, the core non-public spaces covered by the definition of privacy are the home and traditional correspondence, as well as the telephone, email, and certain kinds of online fora. As further discussed below, pri-

---

415. *See* Franz Wero, *Comparative Studies in Private Law*, *in* THE CAMBRIDGE COMPANION TO COMPARATIVE LAW 115, 120-21 (Mauro Bussani & Ugo Mattei eds., 2012) (discussing the convergence of privacy protections).

416. *See* GERT BRÜGGEMEIER, MODERNISING CIVIL LIABILITY LAW IN EUROPE, CHINA, BRAZIL, AND RUSSIA: TEXTS AND COMMENTARIES 33 (2011).

417. *Id.*

418. *Id.*

419. Shulman v. Grp. W. Prods., Inc., 955 P.2d 469, 490 (Cal. 1998), *as modified on denial of reh'g* (July 29, 1998) ("The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source.").

420. *Id.*; BRÜGGEMEIER, *supra* note 292, at 33 (noting the overlap in question); Wero, *supra* note 415, at 120-21 (noting the constitutionalization of the privacy protection).

vacy only protects non-public spaces to the extent that the conduct in those spaces is personal in nature. The last section outlines the distinction between personal conduct (protected as private) and public conduct conducted outside of a public space (not protected in its own right as private even if conducted from or in a non-public space).

1. *The Home*

All legal systems studied agree that conduct in the home is presumptively private. Iran, a jurisdiction that does not recognize an express right to privacy in its private law as such, extends express protection from intrusion to the home.[421] All jurisdictions recognizing an express right to privacy similarly consider that there is a significant reasonable expectation of seclusion in the home.[422]

2. *Traditional Correspondence and Telephone Calls*

All legal systems studied treat correspondence and telephone calls as presumptively non-public spaces, giving rise to a reasonable expectation of seclusion. The Iranian legal system includes such a protection both by way of Islamic law and by constitutional principle.[423] Similarly, the legal systems recognizing an express right to privacy include correspondence within the scope of spaces creating a reasonable expectation of seclusion.[424]

3. *Email and Online Fora*

In principle, the same protections covering traditional correspondence also apply to virtual conduct. The United States, France, China, and Israel all have recognized that virtual correspondence or online conduct is functionally entitled to the same protections as traditional correspondence.[425] The same logic applies in Russian and Iranian law, if by analogy.[426]

---

421. *See* QURAN, 24:27-28. For a discussion of the legal implications of the passage in Iranian jurisprudence, see Reza, *supra* note 312, at 792-95.

422. Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 552 (2006) (as a matter of U.S. law, "[f]or hundreds of years, the law has strongly guarded the privacy of the home"); *see* LARRIBAU-TERNEYRE, *supra* note 363, at ¶ 762 (same as a matter of French law); SHAO, *supra* note 366, at 142 (same for China); Gidron, *supra* note 366, at 284 (same as a matter of Israeli law).

423. QURAN, 49:12. For a discussion of the legal implications of the passage, see Habibi, *supra* note 310, at 3-4.

424. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (noting that correspondence gives rise to expectation of seclusion as a matter of U.S. law); TAMARA KUZNETSOVA ET AL., RUSSIAN CONSTITUTIONAL LAW 46 (2014) (discussing the Russian privacy rationale for correspondence); SHAO, *supra* note 366, at 142 (same for China); Gidron, *supra* note 366, at 284 (same as a matter of Israeli law); Hauch, *supra* note 298, at 1296 (same as a matter of French law).

425. Coal. for an Airline Passengers' Bill of Rights v. Delta Airlines, Inc., 693 F. Supp. 2d 667, 675 (S.D. Tex. 2010) (extending intrusion to online conduct in the U.S.); SHAO, *supra* note 366, at 142 (same for China); Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMM. & TECH. L. REV. 317, 351-52 (2009) (same for Israel); Yoshei Suda, *Monitoring Emails of Employees in the Private Sector: A Comparison Between Western Europe and the United States*, 4 WASH. U. GLOBAL STUD. REV. 209, 256-58 (2005) (discussing the French *Nikon* case, which suggests an increase in the level of privacy protection for employees' e-

But reasonable expectations of seclusion present greater complexities online compared to traditional forms of communication.[427] Some forms of online communications, such as emails, are typically intended for specific recipients.[428] Here, the analogy to privacy in traditional correspondence is at its strongest. But web-based forms of communications, such as posting on Facebook, present a greater challenge.[429] Facebook permits a selection of who can view a post—but is a generally public site.[430] The reasonable expectation of seclusion will be significantly diminished in such fora precisely because they are intended to communicate to broader, semi-public audiences.[431] The specific nature of the forum, the availability of password protection to exclude others, as well as the scope of recipients will be important to determine the strength of expectations of seclusion in information shared online.[432]

4. *Personal or Intimate Nature of Protected Conduct*

Reasonable expectations of seclusion look not only to the place (real or virtual) of an intrusion, but also the substance upon which a stranger intrudes.[433] Expectations of seclusion extend only to personal or intimate conduct.[434] In other words, the expectation of seclusion in public conduct conducted from a non-public space is severely limited.[435] Concretely, a political candidate who made an embarrassing gaffe in a pre-taped television interview cannot enjoin the publication of the interview by the television station simply because it was shot in the candidate's living room. The statement, embarrassing though it may be, is not private or intimate.

---

mails); Christophe Vigneau, *Information Technology and Worker's Privacy: The French Law*, 23 COMP. LAB. L. & POL'Y J. 351, 355-56 (2002) (same).

426. Ruslan Nurullaev, *The Right to Be Forgotten in the European Union and in Russia* (Nat'l Res. U. Higher Sch. of Econ. Research Paper No. WP BRP 54/LAW/2015, 2015), http://ssrn.com/abstract=2669344 (discussing existing Russian regulation relating to online privacy); Hassan & Bagheri, *supra* note 313 (same regarding Iran).

427. *See* Raymond Ku, *Data Privacy as a Civil Right: The EU Gets It?*, 103 KY. L.J. 391, 391 (2015) ("The growth in individuals using social media, as well as the growing ubiquity of data about those individuals online in general, increasingly challenge the legitimacy of individual expectations of privacy.").

428. *See* Ned Snow, *A Copyright Conundrum: Protecting Email Privacy*, 55 U. KAN. L. REV. 501, 522 (2015) (noting that even in the context of emails sent to shared email accounts such as editors@lawreview.edu, "the email sender still has an expectation of privacy in the email sent to each recipient").

429. *See* Christina Gagnier, *On Privacy: Liberty in the Digital Revolution*, 11 J. HIGH TECH. L. 229, 269-70 (2011) ("This perception is facilitated by the fact that in its privacy options, users can select to show individuals a 'Limited Profile,' selecting from a list of options of which information one wants to reveal and which information they choose not to. This option in itself creates the illusion of a 'reasonable expectation of privacy' when one chooses to use these options.").

430. *Id.*

431. *Id.*

432. *See* Allyson Haynes, *Virtual Blinds: Finding Online Privacy in Offline Precedents*, 14 VAND. J. ENT. & TECH. L. 603, 646-48 (2012) (proposing a four-factor balancing test to establish the strength of online privacy expectations).

433. BRÜGGEMEIER, *supra* note 292, at 33.

434. *Id.*

435. *Id.*

Problematically, there is no unifying definition of what constitutes personal, intimate conduct or information.[436] Instead, the private laws examined for purposes of this Article have followed a (non-exclusive) list method to explain what information is personal or intimate.[437] All of the legal systems examined expressly recognize the following kind of conduct or information as private: conduct or information relating to health;[438] marital status or relationships;[439] parental status or relationships;[440] romantic relationships;[441] and sexual conduct.[442] Collectively, these legal systems have further recognized that friendships,[443] political ideas,[444] religious beliefs,[445] and financial information[446] are intimate and personal.

5. *Public Conduct*

The flipside of the intimacy requirement to reasonable expectations of seclusion is that public conduct gives rise to reasonable expectations of publicity. Like privacy, public conduct is defined both in terms of space and content. The jurisdiction with the strongest privacy protections, France, confirms that participation at an event open to the public creates a presumption of publicity of

---

436. Joanna Kulesza, *Walled Gardens of Privacy or "Binding Corporate Rules?": A Critical Look at International Protection of Online Privacy*, 34 U. ARK. LITTLE ROCK L. REV. 747, 755 (2012) ("Civil law offers no definition of 'intimacy.'").

437. *Id.*

438. Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 751, 761 (N.D. Ohio 2013) (noting that health information is highly personal); KUZNETSOVA, *supra* note 424, at 46 (discussing Russian law); SHAO, *supra* note 366, at 143-44 (discussing Chinese law); Gidron, *supra* note 366, at 288 (discussing Israeli law); Hassan & Bagheri, *supra* note 313 (discussing Iranian law); Hauch, *supra* note 298, at 1246-49 (discussing French law); Shackelford, *supra* note 366, at 178 (discussing French law).

439. McSurely v. McClellan, 753 F.2d 88, 112 (D.C. Cir. 1985) (holding that marital status is highly personal); RUDINSKI, *supra* note 360, at 49 (discussing same in Russian law); SHAO, *supra* note 366, at 142 (discussing same in Chinese law); Habibi, *supra* note 310, at 7 (discussing same in Iranian law); Hauch, *supra* note 298, at 1246-49 (discussing French law); Shackelford, *supra* note 366, at 178 (discussing same in French law); Karin Yefet, *Unchaining the Agunot: Enlisting the Israeli Constitution in Service of Warren's Martial Freedom*, 20 YALE J.L. & FEMINISM 441, 471 (2009) (discussing same in Israeli law).

440. RUDINSKI, *supra* note 360, at 49 (discussing Russian law regarding privacy of family life); SHAO, *supra* note 366, at 142 (discussing same in Chinese law); Christine Emery, *Relational Privacy – A Right to Grieve in The Information Age*, 42 RUTGERS L.J. 765, 773-75 (2011) (discussing same in U.S. law); Habibi, *supra* note 310, at 7 (discussing Iranian law); Hauch, *supra* note 298, at 1246-49 (discussing same in French law); Shackelford, *supra* note 366, at 178 (discussing same in French law); Yefet, *supra* note 441, at 471 (discussing same in Israeli law).

441. RESTATEMENT (SECOND) OF TORTS § 652B, *supra* note 424, cmt. b (laying out U.S. law); RUDINSKI, *supra* note 360, at 49 (discussing Russian law); SHAO, *supra* note 366, at 143-44 (discussing Chinese law); Habibi, *supra* note 310, at 7 (discussing Iranian law); Hauch, *supra* note 298, at 1246-49 (discussing French law); Shackelford, *supra* note 366, at 178 (same).

442. Shackelford, *supra* note 366, at 178; Hassan & Bagheri, *supra* note 313 (discussing Iranian law).

443. SHAO, *supra* note 366, at 143-44 (discussing Chinese law); Hauch, *supra* note 298, at 1246-49 (discussing French law); Shackelford, *supra* note 366, at 178 (same).

444. RUDINSKI, *supra* note 360, at 49 (discussing Russian law); Hauch, *supra* note 298, at 1246-49 (discussing French law); Shackelford, *supra* note 366, at 178 (same).

445. Shackelford, *supra* note 366, at 178; SHAO, *supra* note 366, at 142 (discussing Chinese law); Gidron, *supra* note 366, at 293 (discussing Israeli law).

446. Elizabeth DeArmond, *A Dearth of Remedies*, 113 P. ST. L. REV. 1, 41 (2008) ("The tort of intrusion also applies to the disclosure of financial information" in United States law.); SHAO, *supra* note 366, at 142 (discussing Chinese law).

one's presence and conduct at the event.[447] Importantly, public events can take place online to the extent that information is available to the world at large.[448]

This is not to say that reasonable expectations of seclusion entirely disappear when in public, just that they are severely diminished.[449] Thus, a man relieving himself against a tree at a particularly lengthy political rally would maintain a minimal expectation of seclusion by turning his back to the crowd while urinating—but typically could not complain when issued a fine for disorderly conduct that the arresting officer indecently intruded upon the rally-goer's privacy by observing him *in flagrante delicto*. He nevertheless might, depending upon the jurisdiction, complain if photographed by a paparazzo for personal gain.[450]

Beyond public spaces, the conduct at issue itself can further be public. For instance, the making of policy decisions is not itself a personal affair.[451] The question whether conduct is public or private is fact-specific, as the recent dispute about the foreign-directed hacking and disclosure of Secretary Clinton's emails, as well as emails associated with her campaign, has demonstrated.[452] To the extent that conduct or information is considered public, the Privacy Principle would apply to such conduct only obliquely, i.e., to gather the relevant information on policy decisions or the planning and preparation of public events the intruder may also have gained access to personal information as a byproduct of surveillance activity.[453] In those instances, the privacy expectations in the personal information intruded upon extends some protection to public conduct and thus provides some reasonable expectations of seclusion. But these expectations, again, are significantly limited.

B. *Integrating the Definition of Privacy in International Law*

As discussed above, the Privacy Principle can rely upon a common understanding of privacy. This understanding of privacy can be synthesized into a formula of reasonable expectations of seclusion based on the space intruded upon and the substance of the information at issue. The Privacy Principle has

---

447. Hauch, *supra* note 298, at 1249 (discussing French law).

448. *See* sources cited *supra* notes 386-89.

449. RESTATEMENT (SECOND) OF TORTS § 652B, *supra* note 424, cmt. b (laying out U.S. law); SHAO, *supra* note 366, at 142-44 (discussing Chinese law); Gidron, *supra* note 366, at 285 (discussing Israeli law); Hassan & Bagheri, *supra* note 313 (discussing Iranian law); Hauch, *supra* note 298, at 1249 (discussing French law).

450. *See* Int'l Herald Tribune, *Strict Press Laws Govern Any Invasion of Privacy: France No Paparazzi Market*, N.Y. TIMES (Sept. 1, 1997), http://www.nytimes.com/1997/09/01/news/01iht-laws.t.html (discussing French privacy law in the wake of Princess Diana's death).

451. *See* RESTATEMENT (SECOND) OF TORTS § 652B, *supra* note 424, cmt. d (intrusion must be highly objectionable as a matter of U.S. law); Hauch, *supra* note 298, at 1249 (discussing French law).

452. *See* Josh Gerstein & Rachel Bade, *State Dept. Releases Final Haul of Clinton Emails*, POLITICO (Feb. 29, 2016), http://www.politico.com/story/2016/02/hillary-clinton-emails-top-secret-219988 ("Critics have noted that Clinton's lawyers selected the emails turned over to State and that she instructed her staff to delete about 32,000 messages deemed personal by her team.").

453. *See* John F. Decker, *Overbreadth Outside the First Amendment*, 34 N.M. L. REV. 53, 84-85 (2004) (discussing overbreadth in the privacy context as related to contraceptives).

developed a core agreement between legal systems on the protection of the home and correspondence, as well as intuitively intimate data.

This definition of privacy can be readily integrated into international law. It tracks the same kind of spaces already covered by human rights law.[454] It further covers the same kind of information protected by human rights law.[455] The Privacy Principle, in other words, is consistent with existing international legal obligations.

To the extent that there is a conflict between international law and the Privacy Principle, this conflict concerns state-to-state surveillance.[456] Thus, customary international law would suggest an acquiescence by states in surveillance of governmental conduct.[457] This acquiescence has expressly been made part of key diplomatic treaties.[458] If governmental data typically subject to human and signals intelligence were protected by the Privacy Principle, the Privacy Principle would arguably protect too much to be consistent with state-to-state practice.[459]

The Privacy Principle is responsive to such concerns. The reasonable expectation of seclusion in governmental data is comparatively low. The subject matter at issue in official governmental communications is neither personal nor intimate. It does not cover the kind of information typically protected by the Privacy Principle. Quite to the contrary, the information at issue is by definition public. And it is gathered by targeting governmental information infrastructures as opposed to personal computer programs. Given acquiescence in prior state practices of espionage, the expectation of seclusion will be further limited.[460] The expectation of seclusion does not, however, completely disappear; as discussed below, it can give rise to a determination of wrongfulness when the interest of publicity of the surveilling state is even less pronounced (as would be the case were the espionage in question motivated purely by the desire to settle a personal score, as appears to be the case in the context of current Russian surveillance and publication of emails of Democratic National Committee executives).[461]

An additional concern is that the Privacy Principle is overly restrictive of state action to protect the public against terrorist threats. This concern will be addressed in more detail in the next Part. Notably, however, the surveillance of open web-based platforms and the tracking of persons visiting websites associated with terrorist activities are not prohibited by the Privacy Principle. Signals intelligence in this context would simply monitor global public (cyber-)spaces. The Privacy Principle precisely permits such conduct. Armed with this intelli-

454. Milanovic, *supra* note 23, at 122.

455. *Id.*

456. Chesterman, *supra* note 155, at 1077.

457. *Id.*

458. *See supra* Section I.B (discussing ICJ jurisprudence).

459. Chesterman, *supra* note 155, at 1077.

460. *Id.*

461. Simon Shuster, *Vladimir Putin's Bad Blood with Hillary Clinton*, TIME (July 25, 2016), http://time.com/4422723/putin-russia-hillary-clinton (discussing the likely personal motivations for e-mail surveillance and publication of DNC materials at Vladimir Putin's alleged orders).

gence, it is then possible to tailor appropriate signals intelligence programs by identifying targets for further intelligence.

The Privacy Principle therefore can provide strong guidance for global signals intelligence programs. The Privacy Principle not only provides a coherent understanding of what kind of conduct is internationally wrongful, but it also provides a coherent and workable definition of privacy consistent with international law.

V. PROPORTIONALITY

The Privacy Principle does not deal in absolutes. To the contrary, the Privacy Principle defines privacy by reference to reasonable expectations of seclusion. The reasonableness—and thus the strength—of these expectations can fluctuate depending upon the circumstances. This in and of itself means that privacy rights do not have an on-off switch.[462] The Privacy Principle does not have a minimum threshold over which its protection is absolute and below which it permits unbridled intrusion.[463]

As discussed in this final Part, private law confirms that privacy rights are limited by concerns of proportionality. Determining the scope and strength of privacy rights requires balancing. This balancing test at the core of the Privacy Principle is consistent with general international law. Consequently, the fully constituted Privacy Principle must be incorporated into general international law.

A. *Proportionality as a Limit on Privacy in Private Law*

Intuitively, protecting privacy must be a balancing act. As one comparative legal study on privacy law in Europe put it, privacy analysis "is a sensitive, contextual balancing exercise, resolved through examination of the value of the [competing] claims."[464] The legal systems studied for this Article confirm as much: privacy protections require a proportional balancing of the reasonable expectation of seclusion of the person negatively affected by an intrusion or publication in light of the reasonable interest of the intruding party and the interests of the public at large. Should this analysis conclude that, on balance, the intrusion is proportionate to the strength of the competing claims, the conduct is not a civil wrong despite the effect on a person's sphere of intimacy.[465]

As this section sets out, the balancing test has two analytically distinct components. First, the balancing test measures the relative strength of the interests at stake. Second, the balancing test is means sensitive – how is the intru-

462. *See* Paul M. Schwartz, *From Victorian Secrecy to Cyberspace Shaming*, 76 U. CHI. L. REV. 1407, 1433 (2009) (discussing literature supporting that privacy is not an on-off switch).

463. *See* Anita L. Allen, *Unpopular Privacy: The Case for Government Mandates*, 32 OKLA. CITY U. L. REV. 87, 92 (2007) ("It is generally agreed that privacy rights, are not absolute even if fundamental rights and human rights are.").

464. Gavin Phillipson, *The "Right" to Privacy in England and Strasbourg Compared*, *in* NEW DIMENSION IN PRIVACY LAW 184, 219 (Andrew Kenyon & Megan Richardson eds., 2006).

465. Suda, *supra* note 425, at 256-58 (discussing the French *Nikon* case); Vigneau, *supra* note 425, at 355-56 (same).

sion carried out and are other less restrictive means reasonably available to satisfy the interests countervailing privacy? Each of these two components is discussed below in turn.

1. *Balancing Interests*

The private laws examined for this Article balance conflicting interests to determine whether there has been a wrongful intrusion of privacy. The balance begins with the assessment of the factual strength of the reasonable expectations of seclusion at issue in a given case. As discussed above, this analysis is already part and parcel of determining whether a privacy interest is at stake at all.

It next takes into account the strength of the reasonable expectation of publicity of the intruding party.[466] Why does the intruder wish to gather or publish information? For instance, an employer may wish to monitor employee work email accounts to protect confidentiality of intellectual property or ensure appropriate customer care.[467] Similarly, privacy and freedom of expression can in some instances come into conflict.[468] This part of the balancing test establishes the contextual strength of these interests; it measures the reasonable expectations of publicity.

The balancing test finally takes into account the interest of the public at large.[469] Again in the context of publication of information, one typical interest is the freedom of the press.[470] The public has an interest in vigorous discussion of matters of public concerns.[471] This interest requires the disclosure of certain kinds of information that the target of inquiry would rather have kept from public view.[472] Similarly, public safety may well be an interest, as might be the

---

466. Gidron, *supra* note 366, at 289 (discussing the balance between privacy and freedom of expression in Israeli law); Marc A. Sherman, *Webmail at Work: The Case Against Employer Monitoring*, 23 TOURO L. REV. 647, 652-53 (2007) (applying such a balancing test in the context of worker email privacy in the U.S.); Suda, *supra* note 425, at 256-58 (discussing the French *Nikon* case).

467. Sherman, *supra* note 466, at 657-59 (discussing why employers monitor employees' email).

468. Gidron, *supra* note 366, at 289 (discussing the balance between privacy and freedom of expression in Israeli law).

469. *See* CHARLES J. GLASSER, INTERNATIONAL LIBEL AND PRIVACY HANDBOOK 434-35 (2013) (discussing public interest as a matter of Russian law); SHAO, *supra* note 366, at 142 (public interest analysis as a matter of Chinese law); Gidron, *supra* note 366, at 289 (discussing public interest as a matter of Israeli law); Natasha Lehrer, *D'Artagnan's Tune*, *in* TUNE PRIVACY IS DEAD 56, 57-58 (Jo Gainsville ed., 2011) (discussing public interest as a matter of French law); Paul Schwartz & Karl-Nikolas Peifer, *Prosser's Privacy and the German Right of Personality*, 98 CAL. L. REV. 1925, 1956-60 (2010) (public interest analysis as a matter of U.S. law). *But see* Hassan & Bagheri, *supra* note 313 ("Iranian law neither clarifies the exceptional issues such as public interests or security instances in which the consent of data subjects may not be necessary nor differentiate[s] between sensitive and normal data . . . .").

470. *See* GLASSER, *supra* note 469, at 434-35 (discussing freedom of the press); Gidron, *supra* note 366, at 289 (same); Lehrer, *supra* note 469, at 57-58 (same).

471. *See* Marc J. Blitz, *The Right to Map (and Avoid Being Mapped): Reconceiving First Amendment Protection for Information-Gathering in the Age of Geotagging and Google Earth*, 14 COLUM. SCI & TECH. L. REV. 115, 171-72 (2013) (discussing public interest as a core element of freedom of the press in United States law).

472. *See, e.g.*, *Privacy: the French President, the Actress and the Public Interest*, INFORRM'S BLOG (Jan. 13, 2014), https://inforrm.wordpress.com/2014/01/13/privacy-the-french-president-the-

case in the context of the disclosure of health or safety risks.[473] This part of the balancing test establishes the contextual strength of these interests – it measures the reasonable expectations of the public.[474]

The proportionality analysis tests the relative strength of each of these interests in their factual context.[475] It looks to establish the relationship of the case at bar to other more paradigmatic instances in the past in which the law protected the interest at issue.[476] Does the intrusion into privacy more resemble the Panama Papers or an explicit Paris Hilton video?[477] Such contextual analysis avoids the problem of balancing the underlying interests in the abstract (should we value privacy more than freedom of expression?).

To say that an intrusion is proportionate in this sense thus simply means that publicity interests contextually outweigh privacy interests. The factual link of the case at bar to paradigmatic instances of public interest are significant. However, the factual link of the case to paradigmatic instances of personal or intimate conduct are more attenuated. Contextually, the intrusion is proportionate to the privacy interests, the reasonable expectation of seclusion, at stake.

2. *Means Used to Intrude*

Proportionality also measures the propriety of means.[478] Proportionality refers to the comparison of the case at bar to past instances in which publicity interests outweighed privacy interests. This does not take into account whether the intruder reasonably could have used a different means to achieve its goals.[479]

Once it has been established that there is a genuine interest to intrude in a given case, the means used to protect this interest become significant. It may well be true that there is a genuine interest in publishing the Panama Papers.[480]

---

actress-and-the-public-interest/ (discussing the disclosure of an affair between President Hollande and an actress by the French press).

473. *See* GLASSER, *supra* note 469, at 434-35 (public interest analysis); SHAO, *supra* note 366, at 142 (same).

474. *See* sources cited *supra* notes 470-71.

475. *See* Cass R. Sunstein, *Incommensurability and Valuation in Law*, 92 MICH. L. REV. 779, 831-34 (1994) (discussing privacy in incommensurate balancing exercises).

476. *See id.*

477. *Compare* Bruce Zagaris, *ICIJ Panama Papers Cause Waive in Transparency and Accountability*, 32(4) INT'L ENFORCEMENT L. REP. 123 (2016) (discussing the Panama Papers), *with* Joseph Siprut, *The Naked Newscaster, Girls Gone Wild, and Paris Hilton: The True Tale of the Right to Privacy and the First Amendment*, 16 FORDHAM INTELL. PROP. MEDIA L. & ENT. L.J. 35 (2005) (discussing explicit celebrity tapes and the right to privacy).

478. *See* Vicki C. Jackson, *Constitutional Law in an Age of Proportionality*, 124 YALE L.J. 3094, 3099 (2015) (discussing this aspect of proportionality in comparative public law).

479. *See id.* (discussing different means-end based inquiries in public law).

480. *See* Claire Lauterbach, *Panama Papers law firm founder says massive offshore company leak is 'campaign against privacy'. We disagree*, PRIVACY INT'L (Apr. 4, 2016), https://www.privacyinternational.org/node/824 (arguing that the Panama Papers leak does not implicate privacy but implicates transparency); Lili Levi, *Journalism Standards and "The Dark Arts:" The U.K.'s Leveson Inquiry and the U.S. Media in the Age of Surveillance*, 48 GA. L. REV. 907, 909 (2014) (noting the $400 million in settlements paid by News of the World for phone hacking of celebrities).

That does not give journalists license to hack every law firm with impunity in search of more troves like the Panama Papers.[481]

Proportionality of means again refers to two distinct analyses. First, it refers to how narrowly the means were tailored to achieve a given end.[482] This requires an examination of reasonably available alternative courses of conduct.[483] If a less intrusive means would have been available to achieve the same goal, the interest served must be significantly more important to make the intrusion proportionate.[484]

Second, even if no less intrusive means would have been available to achieve the goal in question, one must consider the collateral damage done by the means chosen.[485] Assume it were possible to prove that a fictional leader of a certain Eastern European Great Power had siphoned billions of dollars in public money to personal accounts, but this proof would require hacking every bank in the United Kingdom and sifting through terabytes of financial records of ordinary people.[486] The collateral damage here would almost certainly outweigh legitimate global transparency interests despite the fact that no less restrictive means is available to discover information of great public concern.[487]

The proportionality analysis has important implications. If the interests at issue in favor of publicity outweighed reasonable expectations of seclusion and the means of intrusion were reasonable, there is no violation of the Privacy Principle.[488] Public interest can trump privacy concerns.[489] In those instances, the Privacy Principle does more than tolerate intrusions upon reasonable expectations of seclusion.[490] The Privacy Principle accepts that intrusion is legitimate.[491] Intrusion is in fact desirable.

Due to the proportionality analysis, the Privacy Principle therefore becomes more than a shield against intrusive conduct. It acts as more than a liability rule deeming certain kinds of conduct wrongful.[492] It helps to establish protocols for determining when one should intrude.[493] It provides a contextually tested principled reason for gathering intelligence and for using it.[494] The

---

481. *See* Zagaris, *supra* note 477, at 123-25 (discussing the value of the Panama Papers).

482. *See* Gidron, *supra* note 366, at 289 (discussing Israeli law); Andrew Serwin, *Privacy 3.0—The Principle of Proportionality*, 42 U. MICH. J.L. REFORM 869, 875-76 (2009) (deriving a principle of proportionality for U.S. law); Suda, *supra* note 425, at 256-58 (discussing the French *Nikon* case); Vigneau, *supra* note 425, at 355-56 (same).

483. Levi, *supra* note 480, 909.

484. *See* Jackson, *supra* note 478, at 3113 (discussing this form of proportionality).

485. *See id.*

486. *See id.* at 3117 (discussing proportionality as such in Canadian public law in similar terms).

487. *See id.*

488. *See* sources cited *supra* note 466.

489. *See id.*

490. *See id.*

491. *See id.*

492. *See* REISMAN, *supra* note 165, at 21 (distinguishing a textual-rule based mode of decisionmaking from a context-policy based mode of decisionmaking); Guido Calabresi, *Torts—The Law of the Mixed Society*, 56 TEX. L. REV. 519, 521 (1978) (discussing the difference between liability rules and regulatory conduct).

493. *See* sources cited *supra* note 482.

494. *See id.*

Privacy Principle thus improves and refines *ad hoc* rationalizations for intrusive conduct.[495] It explains why some circumstances make intrusion a social good.[496]

The Privacy Principle, in other words, can guide intelligence-gathering efforts. It can assist in identifying and choosing targets for intelligence gathering. It can assist in means testing the intelligence tools used. It thus provides a legal rubric that can be used ex ante to supplement other policy tools.

B. *Integrating the Proportionality Exception into International Law*

The proportionality test developed on the basis of private law sources is fully consistent with existing human rights law as developed above. Like private law, human rights law relies upon proportionality analyses to assess potential liability for intrusions of privacy.[497] The proportionality analysis used in human rights law further functionally mirrors the understanding of proportionality in private law.[498] In fact, both private law and human rights law have already greatly enriched each other in actual adjudications of invasion of privacy claims.[499]

Integrating the Privacy Principle with its proportionality analysis in international law can greatly help appraise existing intelligence gathering efforts. Public interest in safety is certainly significant.[500] But the interest will have to be contextually tested both in terms of the threat presented and in terms of the privacy interest intruded upon.[501] Reviewing work emails and tapping work phones implies different privacy interests than snooping on a bedroom by remotely enabling a web camera.[502] Further, the concern for public safety is greater when intelligence gathering responds to specific threats as opposed to instituting a global program in case a new threat might emerge.[503]

Integrating proportional means testing highlights the need for specific targeting. In terms of least restrictive means testing, it will have to be queried whether collaborative efforts with local law enforcement officials might have been feasible.[504] If it is possible to cooperate with foreign law enforcement agencies to gather intelligence, such efforts would assure the additional due process protections for the targets.[505] The targets would have effective recourse should their privacy be wrongfully invaded; they would be immediately able to file a claim against their home government pursuant to available public law causes of action.

---

495. *See id.*

496. *See id.*

497. *Id.*

498. *Id.*

499. Phillipson, *supra* note 464, at 219 (discussing the influence of European Court of Human Rights law on English law).

500. *See* Milanovic, *supra* note 23, at 139 (discussing security interests).

501. *See* sources cited *supra* notes 466, 478-80.

502. *See* sources cited *supra* notes 466, 478-80.

503. *Id.*

504. *Id.*

505. ICCPR, *supra* note 36, art. 19.

Even if working with local law enforcement is not feasible, intelligence-gathering conduct cannot cover every communication spanning the globe. It is at its most legitimate when it can rely upon specific information linking a person or a group of persons to a specific threat.[506] The narrower the field of surveillance targets and the more contextually sensitive the criteria for selecting targets, the stronger the claim to proportionality by the state's intelligence services.[507]

The Privacy Principle can now be put to further use in order to backstop or help design existing efforts. Thus, websites used by hostile organizations to recruit new members are presumptively public.[508] The threat posed by the hostile organization for life, safety, and prosperity of the intelligence gathering state will permit a quantification of intelligence gathering interest.[509] If that interest is great, proportionality analysis would deem it desirable to monitor the websites in question and to log visitors.[510]

The information gathered in public virtual spaces can then be used to develop specific target lists directly linked to significant threats. To the extent it is possible as a matter of foreign policy and policing efficacy to make the home state of the individual in question aware of the individual's threat posture, disclosure of the information in question would itself be desirable because it is in the public interest—i.e., the interest of the gathering state, home state of the target, and the world community at large.[511] Disclosure further would be in the interest of the target of the intelligence operation as it would immediately extend the due process protections applicable as a matter of the law of his or her home state and international law to all further investigations.[512]

To the extent that disclosure is not feasible, the target list would support the surveillance of repeat visitors.[513] The surveillance could be tiered to monitor websites used by multiple targets. If this next step yields intelligence confirming a threat, a full surveillance of the person's electronic correspondence and even home may well be warranted. This in turn would yield new targets for further intelligence gathering and so on.

The Privacy Principle thus permits the construction of intelligence gathering programs that facially protect both privacy and security interests. To the extent that threat levels measurably increase, proportionality analysis would expand permissible intelligence gathering efforts. It would also point to meaningful next steps to develop actionable intelligence rather than amassing an unmanageable sea of big data. The Privacy Principle, in other words, can

506. *See supra* Sections V.A.1-2 (discussing the scope of intelligence gathering).
507. *Id.*
508. *See* Ku, *supra* note 427, at 391.
509. *See* sources cited *supra* notes 466, 478-80.
510. *Id.*
511. *Id.*
512. *Id.*
513. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328 (2012) (noting in the context of longer term surveillance that "[t]he repeated use of nonsearch techniques has been considered an essential way to create probable cause that justifies searches rather than an unlawful search itself").

become a policy tool for the development of intelligence, rather than simply an impediment to intelligence gathering.

VI. CONCLUSION

The Privacy Principle is an international legal prescription that can be applied to signals intelligence efforts. It thus transforms signals intelligence from a space currently suffering from fragmented international legal rules at best, or a complete vacuum of legal rules at worst, into a sphere governable by general international law. The Privacy Principle does so by vindicating privacy rights in reasonable expectations of seclusion of private citizens as anchored in the private laws of leading global legal systems.

The Privacy Principle is decidedly non-occidental. It forms part of diverse legal systems inspired by Western rationalism, pragmatic policy-science, Confucianism, Islam, and Jewish tradition. This principle is accepted by key members of the intelligence community to govern their own private internal affairs. It is thus opposable to these members without risk of prescribing international rules of conduct not supported by authoritative expectations in their respective civil societies. In other words, the Privacy Principle is legitimate both as a matter of international and domestic law.

But the Privacy Principle is more than a liability rule designating certain intelligence programs as internationally wrongful. It provides guidance to intelligence officers. It can provide a means to determine intelligence priorities. It can assist in designing intelligence programs that manageably meet these priorities. It is a policy tool as well as a legal limit on state conduct.

Given the current state of global violence, the Privacy Principle is greatly needed. The near weekly reports of violent, mass casualty attacks on civilians in the West, Africa, the Middle East, and Asia present a significant temptation to spy indiscriminately on the entire world population.[514] The Privacy Principle emphatically rejects any such efforts as both illegal and unwise. Such efforts would not respect the very authoritative expectations shared by states and their citizens as to what spaces, conduct, and thoughts remained private.[515] Thwarting such expectations can be quickly perceived as repressive.[516] Repressive government conduct engenders further disaffection in the civil population in both target states and intelligence gathering states: both in equal measure perceive that law is ineffective in protecting their respective interests.[517] This in turn leads to an increased likelihood of future strife and violence.[518]

514. Cameron Glenn, *Timeline: Rise and Spread of the Islamic State*, WILSON CTR. (July 5, 2016), https://www.wilsoncenter.org/article/timeline-rise-and-spread-the-islamic-state (chronicling ISIL attacks).

515. *See* Frederic Sourgens, *The End of Law: The ISIL Case Study for a Comprehensive Theory of Lawlessness*, 39 FORDHAM INT'L L.J. 355, 369-72 (2015) (discussing the importance of authoritative expectations for lawfulness).

516. *See id.* at 407-12 (discussing the transnational transference of lawlessness).

517. *See id.*

518. *See id.*

This is not to say that the Privacy Principle condemns us to suffer violence without means of thwarting potential plots. It provides for clearly identifiable and justifiable pathways to conduct global and cooperative intelligence gathering. These pathways help narrow the field of inquiry to a manageable and digestible set of data. They extend the set of actors contributing to these efforts from one state's agency to that of a broader global community committed to stopping the mass killing of civilians. The Privacy Principle thus provides a means to carry the intelligence function of the world community discriminately and prudently. The Privacy Principle is one instance in which legal decision making processes devise sensible policy in the face of severe uncertainty and distrust.[519] In following the Privacy Principle, intelligence gathering will reduce uncertainty and engender trust in equal measure. This twin reduction of uncertainty and building of trust is the central function of legal processes in the world community.[520]

519. *See* REISMAN, *supra* note 165, at 21 (submitting that the task of legal scholars is to design lawful decisions that are contextually meaningful and realistic).

520. *See id.*