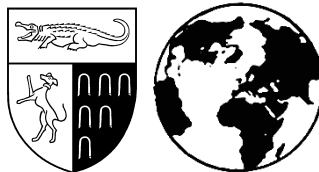


# The Yale Journal of International Law Online



## A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens

Asaf Lubin<sup>†</sup>

Frédéric Sourgens's recent article, *The Privacy Principle*,<sup>1</sup> dares to ask a provocative question: can international law regulate global surveillance programs without sacrificing national security interests? The need to strike a balance between privacy and security is of course not new.<sup>2</sup> It is perhaps as old as the second oldest profession itself.<sup>3</sup> Indeed, it was Sir Francis Welsingham, the father of modern intelligence agencies, who made the hackneyed statement on behalf of Elizabeth I of England concerning the latter's reservation towards surveillance of Catholics and Puritans on a massive scale. Welsingham noted in

---

<sup>†</sup> J.S.D. candidate at Yale Law School; Resident Fellow of the Information Society Project; Visiting Scholar, Hebrew University Cyber Security Research Center; Robert L. Bernstein International Human Rights Fellow at Privacy International. I would like to thank Frédéric Sourgens for bringing our lively exchanges over the 2016 Jessup Compromis into a forum fitting of their breadth. I would like to also thank the student editors at the Yale Journal of International Law for all of their thoughts and hard work surrounding the publication of both pieces. The arguments presented in this paper reflect my own thoughts and in no way represent the positions of any of the organizations with which I am associated.

1. Frédéric Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345 (2017).

2. In *Discourses on Livy*, Niccolò Machiavelli writes, "as far as the . . . popular desire of recovering their liberty, the prince, not being able to satisfy them, must examine what the reasons are that make them desire being free . . . . As for the rest, for whom it is enough to live securely, they are easily satisfied by making orders and laws that, along with the power of the king, comprehend everyone's security. And once a prince does this, and the people see that he never breaks such laws, they will shortly begin to live securely and contentedly." NICCOLÒ MACHIAVELLI, DISCOURSES ON LIVY (ca. 1517), reprinted in NICCOLÒ MACHIAVELLI, THE CHIEF WORKS AND OTHERS 237 (A. Gilbert trans., 1965). See also Benjamin Franklin, Letter to the Pennsylvania Assembly, Reply to the Governor (Nov. 11, 1755), in VOTES AND PROCEEDINGS OF THE HOUSE OF REPRESENTATIVES, 1755-1756, 19-21 (1756) ("Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety"); cf. Benjamin Wittes, *What Ben Franklin Really Said*, LAWFARE (July 15, 2011), <https://www.lawfareblog.com/what-ben-franklin-really-said> (noting that when read in its original context, the famous quote "does not mean what it seems to say" and suggesting that "Franklin was not describing some tension between government power and individual liberty. He was describing, rather, effective self-government in the service of security as the very liberty it would be contemptible to trade. Notwithstanding the way the quotation has come down to us, Franklin saw the liberty and security interests of Pennsylvanians as aligned").

3. Michael J. Barrett, *Honorable Espionage II*, 2 J. DEF. & DIPL. 12, 14 (1984) ("Espionage is the world's second oldest profession and just as honourable as the first.").

a letter to the Secretary of France that it was her majesty's repugnance of the "tyranny of the Church of Rome" —which used "terror and rigour" to secure obedience—that led her to not want "to make windows into men's hearts and secret thoughts." Instead, Queen Elizabeth opted to amend her laws and restrain her own supreme power to surveil, expecting that such an act of self-control would bring about "good effects" over time.<sup>4</sup>

The world has, however, changed significantly since the sixteenth century. For Welsingham, a global mass surveillance program involved "pa[y]ing off travellers in the ports of Lyon and merchant adventurers in the bazaars of Hamburg."<sup>5</sup> It meant diligently running expensive and cumbersome human spy rings across the European continent. The advancement of new forms of digital communications not only created an ever-more connected and globalized world; it also broke the conceptual and practical shackles that restricted the work of intelligence agencies. The capacity limitations of the past have been replaced by new opportunities for bulk interception, retention, and analysis of signals intelligence (SIGINT). Coupled with the emergence of contemporary global threats, ranging from the proliferation of WMDs to the rise of trans-boundary non-state terror groups, it is easy to accept Sourgens's argument that "the collection of remote electronic communications of foreign targets has become the coin of the security realm" and his prediction that intelligence gathering is thus "only going to increase. . . ."<sup>6</sup>

In this context, international human rights law (IHRL) is supposed to provide limits on the surveillance state, standing tall and sturdy, like a fortified wall, against Orwell's Big Brother. As the ICTY concluded in its famous *Tadić* decision, we have, in the course of recent decades, reoriented the purposes of the international security system to take into consideration the rise to pre-eminence of human rights.<sup>7</sup> The universal right to privacy, as one of those core rights, is therefore supposed to offer us assurance against unfettered and arbitrary interference in our private lives. The combined effect of the Universal Declaration of Human Rights, the international human rights treaties and treaty bodies, the regional human rights courts, and the Human Rights Council's special rapporteurs was supposed to be enough to prevent governments from engaging in wholesale surveillance of entire populations.

Sourgens's piece, however, offers a sobering and demystifying account of the fault lines of the privacy agenda and human rights discourse. Looking at privacy protections from both treaty and customary law perspectives, Sourgens concludes that "existing international law approaches to the protection of global

---

4. 2 GILBERT BURNET, *THE HISTORY OF THE REFORMATION OF THE CHURCH OF ENGLAND* 418-19 (1681).

5. Asaf Lubin, *Espionage as a Sovereign Right under International Law and Its Limits*, 24(3) INT'L L. STUDENTS ASS'N Q. 22, 24-25 (2016).

6. Sourgens, *supra* note 1, at 346-347.

7. *Prosecutor v. Duško Tadić*, Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 97 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995) (recognizing that the world has witnessed "significant changes in international law, notably in the approach to problems besetting the world community. A State-sovereignty-oriented approach has been gradually supplanted by a human-being-oriented approach. Gradually the maxim of Roman law *hominum causa omne jus constitutum est* (all law is created for the benefit of human beings) has gained a firm foothold in the international community as well").

privacy rights face significant hurdles when applied to the digital age of signals intelligence, leading to an apparent normative gap in the law.”<sup>8</sup> Faced with this gap he therefore calls for a paradigm shift through the introduction of a “privacy principle”—a “general principle of law protecting the right to privacy.”<sup>9</sup> The Article then attempts to prove the existence of this principle, to define its scope and nature, and to apply it in context. I wholeheartedly commend Professor Sourgens for creatively thinking beyond the conventional legal wisdom to innovatively propose a new international legal framework to enhance privacy protections in the face of foreign mass surveillance. Nonetheless, I’m afraid I do not share his optimism about the existence or value of such a principle and believe that its promotion is thus misguided.

This short response is inevitably selective. Part I offers a brief summary of Sourgens’ key arguments and his legal rationales for them. Part II pushes against the existence of a general privacy principle. This Part challenges both the methodology employed by Sourgens to identify this principle, as well as the practicality of the overall endeavor. Part III makes the case for an extraterritorial right to privacy under both treaty and customary international law. This Part further analyzes recent successes of IHRL in fighting against unwarranted surveillance, and concludes by providing counter-arguments to the concerns raised by Sourgens regarding the effectiveness of the human rights discourse in this sphere. I conclude my response in Part IV by acknowledging the real need, noted by Sourgens, for a paradigm shift in the discourse on privacy. Despite the recent accomplishments, it is nonetheless true, and worth highlighting as Sourgens persuasively does, that IHRL activists have not been able to establish sufficient privacy protections against foreign mass surveillance. This Part makes the claim that the only solution for the many deficiencies of the human right to privacy is to reform human rights thinking and advocacy. Instead of introducing a new non-enforceable general principle with identical content to that of the human right it seeks to supplant, let us reconceptualize the legal content of the human right itself. The final concluding Part thus gestures towards a paradigmatic shift *within* IHRL by suggesting a controversial, yet far more realistic way of applying tailored privacy protections to foreign surveillance, taking into consideration the justified needs of States.

#### I. A NEW GENERAL PRINCIPLE IS BORN: ALL HAIL THE PRIVACY PRINCIPLE

While Sourgens’s Article is comprised of five Parts, I wish to focus my response only on the first three, as they lay the foundation and set the narrative of the entire piece. In Part I, titled “The Privacy Problem in International Law,” Sourgens focuses predominately on the asserted territorial limitations of IHRL treaties to prove the inaptitude of the privacy-as-a-right approach. As Sourgens notes,

[o]ne core challenge for the human rights treaty paradigm is the objection lodged by the United States that human rights instruments have purely territorial application . . . . Contemporary global signals intelligence programs can operate entirely outside

---

8. Sourgens, *supra* note 1, at 348.

9. *Id.* at 349.

of the territory of the signatory state. Due to the nature of the internet, this is true even for surveillance of a state's own nationals. Some are therefore concerned that such signals intelligence is beyond the reach of the privacy principle codified in the [International Covenant on Civil and Political Rights (ICCPR)].<sup>10</sup>

Sourgens continues by suggesting that “the United States appears to be leading a movement of state practice away from a more robust understanding of human rights [to] privacy.”<sup>11</sup> To establish this claim, he looks to three of the four additional permanent members of the United Nations Security Council (China, Russia, and France).<sup>12</sup> Focusing on their recent state practice, Sourgens shows that all three are adopting both domestic and foreign surveillance legislation and policies that challenge global privacy protections.<sup>13</sup> On these grounds, Sourgens concludes that

[i]n 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. 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 rights exists.<sup>14</sup>

Parts II and III introduce the privacy principle to fill this regulatory gap. To fully grasp the novelty of Sourgens's claims, it is worth clarifying the distinction between international human rights law and general principles of international law.<sup>15</sup> Whereas international human rights law is predominantly grounded in treaties and the interpretation of treaty bodies and courts, general principles are a “co-equal source of international law” that do not require an explicit international enactment,<sup>16</sup> but instead arise from deep and widespread custom and practice in both national and international law. As such, Sourgens correctly notes, they can be used to “fill gaps within the fabric of international law.”<sup>17</sup> In other words, Sourgens contends that the privacy-as-a-right approach suffers from the limitations of conflicting interpretations, inadmissibility, and a lack of uniform adoption, thus leaving a gap in control. Once recognized, privacy-as-a-principle would automatically become part of international law proper and could therefore offer a globally binding solution.

Part II, titled “Proving General Principles of Law” establishes the theoretical framework for verifying the existence of general principles. Relying on the

---

10. *Id.* at 353-54.

11. *Id.* at 358.

12. Oddly, Sourgens ignores the United Kingdom, the final P5 member, despite the fact that, on its face, its recent state practice seems to bolster his claim even further. The United Kingdom adopted the Investigatory Powers Act this past December – rancorously referred to by digital rights activists as the “Snooper’s Charter,” as it is one of the most robust and expansive pieces of surveillance legislation in the western world. For further reading, see Asaf Lubin, *The Investigatory Powers Act and International Law: Part I*, UCL J. L. & JURIS. BLOG (Dec. 26, 2016), <https://blogs.ucl.ac.uk/law-journal/2016/12/26/the-investigatory-powers-act-and-international-law-part-i/>.

13. Sourgens, *supra* note 1, at 358.

14. *Id.* at 359.

15. The question of whether each of the human rights enshrined in the corpus of IHRL also reflects custom, and within it whether the full content of each right is customary, is a matter of controversy. I believe the right to privacy reflects custom, an argument that Sourgens ignores. This issue is discussed further in Section III.B, *infra*.

16. Sourgens, *supra* note 1, at 349.

17. *Id.* at 367.

jurisprudence of both the Permanent Court of International Justice (PCIJ) and the International Court of Justice (ICJ), the Part introduces a two-phased test for determining the existence of a general principle: (1) whether a “comparative legal analysis of relevant legal systems establish[es] a requisite degree of convergence to formulate a common, shared legal principle of domestic laws”<sup>18</sup>; and (2) whether this shared principle of domestic law “is compatible with existing norms of general international law.”<sup>19</sup> In essence, Sourgens embraces a “comparativist approach” to establishing the existence of a critical mass of convergence amongst domestic legislation, examining “the amount of resource, but also of the density, and purity of that resource.”<sup>20</sup>

Finally, in Part III, titled “The Privacy Principle,” Sourgens applies this theoretical model to prove the existence of his principle. This Part looks at six legal systems (those of the United States, France, China, Russia, Iran, and Israel), which Sourgens claims represent geographical and cultural diversity as well as significant capacities in signals intelligence.<sup>21</sup> Sourgens shows that a critical mass of these jurisdictions recognize, in their civil law, that any unconsented-to collection or use of “private information is an independent wrongful act in violation of the right to privacy. . . .”<sup>22</sup> To establish that the principle is also compatible with existing international law norms, Sourgens relies on IHRL, claiming that the principle is “entirely consistent with existing human rights law and jurisprudence. The privacy protections extended by the [p]rivacy [p]rinciple are analogous to the interpretation of the right to privacy included in human rights treaties.”<sup>23</sup> The Article concludes with Parts IV and V, which adopt a working definition of privacy under the principle, and apply the principle to the design of international surveillance programs, using standards of proportionality.

## II. THE PRIVACY PRINCIPLE: THE PRINCIPLE THAT DIED IN ITS CRIB

I do not share Sourgens’s position that a privacy principle exists, for three primary reasons. First, the privacy principle does not meet the “indispensability requirement” under the jurisprudence of the PCIJ and ICJ (Section II.A *infra*). Second, Sourgens erroneously bases his privacy principle on a comparative analysis of private law in each of the surveyed States while completely ignoring public law exceptions (Section II.B *infra*). Finally, there exists a circular fallacy at the stage where Sourgens deems the privacy principle compatible with international law (Section II.C *infra*).

---

18. *Id.* at 368.

19. *Id.*

20. *Id.* at 372 (quoting Adeno Addis, *The Concept of Critical Mass in Legal Discourse*, 29 CARDOZO L. REV. 97, 104 (2007)).

21. *Id.* at 375-376 (“These jurisdictions capture a reasonable diversity in legal traditions, cover a broad geographic range, and encompass a significant cultural diversity. 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. An agreement between these global leaders is going to carry the greatest authority vis-à-vis possible repeat offenders against the principle in question. 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.”).

22. *Id.* at 388.

23. *Id.* at 390.

However, and this is perhaps most important, even if we were to accept the existence of the privacy principle, it is, as far as I can see, much ado about nothing, as it is unlikely to achieve any of Sourgens' purported goals.

#### A. *The Forgotten Indispensability Requirement*

While Sourgens posits a two-phased test for determining the existence of a general principle, scholars have identified a third requirement in the jurisprudence of the International Court, the requirement of "indispensability." As noted by Jalet, "it is not because rules or legal principles exist in most, or even in every, legal system that they constitute general principles, but because they are so basic and fundamental as to compose the substratum from which positive rules may be derived."<sup>24</sup> Professor Hersch Lauterpacht defined general principles as "obvious maxims of jurisprudence of a general and fundamental character."<sup>25</sup> Baron Descamps, President of the Advisory Committee that drafted the PCIJ Statute, stated that general principles are "the fundamental law of justice and injustice deeply engraved on the heart of every human being and which is given its highest and most authoritative expression in the legal conscience of civilized nations."<sup>26</sup> Professor Gordon Christenson referred to general principles as "foundational ordering norms in a global interdependent community."<sup>27</sup> Even Bin Cheng, whom Sourgens cites extensively throughout his piece, recognized that general principles are "juridical concept[s]" that lie "in the very nature of law."<sup>28</sup>

This short literary review suggests that for a general principle to exist, it must be indispensable for the functioning of a legal system. General principles are cardinal ideas, a core of legal foundational norms. Bassiouni cites, as examples, the principles of "justice, fairness, equality, and good faith," as well as the notion of "territorial criminal jurisdiction" and the requirement that treaty and contract interpretations "be based first on the plain meaning of the words."<sup>29</sup> Bassiouni then proceeds to survey the jurisprudence of the PCIJ and ICJ to identify even more established general principles, including *inter alia*, the principle of competence-competence,<sup>30</sup> the doctrine of *nullus commodum*

24. Frances T. Freeman Jalet, *The Quest for the General Principles of Law Recognized by Civilized Nations - A Study*, 10 UCLA L. REV. 1041, 1085-86 (1963); see also Alfred Verdross, *Les Principes Généraux du Droit dans la Jurisprudence Internationale*, 52 COLLECTED COURSES OF THE HAGUE ACADEMY OF INTERNATIONAL LAW 191, 203 (1935) (noting that identifying general principles can be achieved without conducting a comparative survey, simply by studying whether a principle is indeed indispensable to the existence of a legal system).

25. 1 INTERNATIONAL LAW: BEING THE COLLECTED PAPERS OF HERSCH LAUTERPACHT 69, 74 (E. Lauterpacht ed., 1970).

26. MAARTEN BOS, A METHODOLOGY OF INTERNATIONAL LAW 70 (1984) (quoting Descamps).

27. Gordon A. Christenson, *Jus Cogens: Guarding Interests Fundamental to International Society*, 28 VA. J. INT'L L. 585, 587 (1988).

28. BIN CHENG, GENERAL PRINCIPLES OF LAW AS APPLIED BY INTERNATIONAL COURTS AND TRIBUNALS 392-94 (1953).

29. M. Cherif Bassiouni, *A Functional Approach to "General Principles of International Law"*, 11 MICH. J. INT'L L. 768, 772 (1989-1990).

30. The general rule that "a body possessing jurisdictional powers has the right in the first place itself to determine the extent of its jurisdiction", reaffirmed by the PCIJ in the Interpretation of the Greco-Turkish Agreement of Dec. 1, 1926, 1928 P.C.I.J. (ser. B) No 16, at 20 (Aug. 28).

*capere (potest) de sua iniuria propria*,<sup>31</sup> the principle of reparations derived from wrongful acts,<sup>32</sup> and the blue pencil doctrine.<sup>33</sup> All of these general principles are indeed maxims and foundational ordering norms.<sup>34</sup>

Now compare these principles with the right to privacy, and in fact any of the human rights enumerated in the corpus of IHRL. What you will find is that human rights are not suitable candidates for consideration as general principles. They are subject to a high level of political scrutiny, debate, and nuanced interpretation. The fact that these unalienable rights can be limited and balanced against each other, that they can be derogated from in times of emergency, or be interpreted differently depending on the particular customs of a geographical region, or in the light of the parallel application of the laws of armed conflict, all seem to suggest that they cannot be deemed indispensable generalized maxims of foundational law.

Accepting Sourgens's interpretation would lead to an over-expansion of general principles to spheres of legal activity which they were never intended to cover, filling gaps which they were never intended to fill. It would mean that any human right could now resurface as its own "co-equal source of international law" by simply rebranding itself as a general principle. Struggling to abolish the death penalty in the U.S., China, and Russia? Try the "life principle" on for size. Having issues with CIA "black sites" in Poland and prolonged administrative detention in the U.K. and France? Don't worry! Take the "liberty principle" for a spin. Human rights obligations cannot simply be reintroduced through general principles. Rather, they must be interpreted within the bounds of their own natural habitat, examined internationally through the lenses of constitutional, domestic, and human rights law.

### B. *A Comparative Review of Private Law in Isolation*

I have no immediate qualms with Sourgens's selection of the six jurisdictions that he chose for his review,<sup>35</sup> but I do challenge aspects of the methodol-

---

31. The maxim that no advantage may be gained from one's own wrong was recognized by the PCIJ as a general principle in *Factory at Chorzów (Ger. v. Pol.)*, Judgment, 1927 P.C.I.J. (ser. A) No. 9 (July 26) (where the Court concluded that it is a "principle generally accepted in the jurisprudence of international arbitration, as well as by municipal courts, that one Party cannot avail himself of the fact that the other has not fulfilled some obligation or has not had recourse to some means of redress, if the former Party, by some illegal act, prevented the latter from fulfilling the obligation in question, or from having recourse to the tribunal which would have been open to him.").

32. *Factory at Chorzów (Ger. v. Pol.)*, Claim for Indemnity, 1927 P.C.I.J. (ser. A) No. 17 (Sept. 13) (The Court stated that the "essential principle contained in the actual notion of an illegal act – a principle which seems to be established by international practice and in particular decisions of arbitral tribunals – is that reparation must, as far as possible, wipe out all the consequences of the illegal act and reestablish the situation which would in all probability, have existed if that act had not been committed.").

33. The "separateness" of treaty provisions as a principle which may be resorted to when a treaty provision has become inoperable was employed by Judge Jessup in the *South West Africa Cases (Ethiopia v. S. Afr.; Liberia v. S. Afr.)*, 1962 I.C.J. 319, 408 (Dec. 21).

34. For a complete list of general principles, see Bassiouni, *supra* note 29, at 791-801.

35. One can, however, raise the question of why Sourgens deemed the United States, France, Israel, Iran, China, and Russia to be "the key stakeholders' jurisdictions affected by the principle to be proved." Sourgens, *supra* note 1 at 370. Are the key stakeholders only those countries that engage in significant SIGINT collection? Shouldn't the primary victims (namely those countries in the global

ogy of analysis employed throughout the piece. In his survey of privacy protections in the domestic laws of each of the six examined countries, Sourgens looks only to private law, from the Restatement (Second) of Torts, to the Civil Codes of France, Iran, and Russia, to the Chinese Torts Liability Law, and the Israeli Protection of Privacy Law.<sup>36</sup> However, Hersch Lauterpacht argues that in identifying general principles one must engage in “comparison, generalization, and synthesis of rules of law in its various branches – private and public, constitutional, administrative, and procedural.”<sup>37</sup> One cannot simply engage in cherry-picking, reading a single private law statute in a vacuum separate from the general system. This is of specific importance in light of the fact that the subject of review is governmental espionage, an area inherently governed by public law and public policy. To look at the private law conceptualization of privacy in each of these systems, in isolation from the public law exceptions enshrined therein, would be “doing violence to the fundamental concepts of any of those systems.”<sup>38</sup>

Take as an example the Israeli case study. Sourgens correctly cites to Article 2 of the Protection of Privacy Law of 1981, and accurately finds that the law “makes infringement of privacy a civil wrong.”<sup>39</sup> However, he ignores two key points. First, the law (as is true for all the other civil laws examined by Sourgens) only applies territorially. The privacy protections enumerated therein do not apply to a non-national in a foreign country, let alone in cases where the infringing party is an agency of the State operating under statutory authorization. Second, and relatedly, Sourgens’s analysis stops before introducing the readers to Article 19 of the same law titled “Exemption.” That Article reads, in relevant part:

“19. . . . (b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of performance thereof.

(c) security authority, for purpose of this section – [includes] any of the following:

(1) the Israel Police;

(2) the Intelligence Branch of the General Staff of the Israel Defense Forces, and the Military Police;

(3) the General Security Services;

(4) the Institute for Intelligence and Special Assignments . . . .”<sup>40</sup>

---

south – in Africa, South America, and the Arab world), those countries with weaker cyber security capacities, and therefore the ones most affected by surveillance programs, be better represented?

36. Sourgens, *supra* note 1, at 379-82.

37. LAUTERPACHT, *supra* note 25, at 74.

38. H. C. GUTTERIDGE, *COMPARATIVE LAW* 65 (2d ed. 1949) (“If any real meaning is to be given to the words ‘general’ or ‘universal’ and the like, the correct test would seem to be an international judge before taking over a principle from private law must satisfy himself that it is recognised in substance by all the main systems of law, and that in applying it he will not be doing violence to the fundamental concepts of any of those systems.”).

39. Sourgens, *supra* note 1, at 380.

40. Protection of Privacy Law, 5741-1981 SH No. 1011 p. 128 (Isr.). For an English translation, see *Israel Protection of Privacy Law 5471-1981*, WIPO (2014), [http://www.wipo.int/wipolex/en/text.jsp?file\\_id=347462](http://www.wipo.int/wipolex/en/text.jsp?file_id=347462).



Each of the countries surveyed by Sourgens, and in fact any country that engages in covert surveillance for purposes of preventing serious crime or foiling terrorist threats, has similar exemptions in law. If the purpose of Sourgens's review was to determine whether privacy protections exist in each of the jurisdictions examined, he cannot simply read these statutes outside of the regulatory environment in which they are situated. In other words, yes, Sourgens is correct in concluding that "the legal systems studied conceive of privacy as a right" and that the "right to privacy has support from a diversity of legal traditions."<sup>41</sup> However, this right is not extended extraterritorially by any of the statutes that he cites, nor do the countries surveyed see this right as a hindrance to either their domestic or foreign surveillance practices (quite the opposite—there is a convergence of national security exemptions for surveillance purposes).

To justify his isolated review of private law, Sourgens confusingly relies on the extraterritorial nature of the operations in question,<sup>42</sup> making the following argument:

"[W]hen 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. Extraterritorial conduct of the state is thus not a priori permissible as sovereign prerogative, but nor is it a priori impermissible as interference in the internal affairs of its neighbors. 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."<sup>43</sup>

One of Edward Snowden's many revelations was that the United States used its embassy in Berlin as a listening station to monitor the communications of German government officials working nearby the embassy in the Regierungsviertel (the Government District).<sup>44</sup> According to Sourgens, we should treat the United States in this scenario as an "everyman," subject to the German domestic private law regulations of privacy, thus justifying an isolated review of private law. But nothing is further from the truth. The United States enjoyed state immunity from criminal and civil prosecution and enforcement, and the NSA and CIA employees who engaged in the alleged surveillance activities were equally immune under the Vienna Conventions on Diplomatic and Consular Relations. The most that Germany could do, as it eventually did, is kick those spymasters out of the country as *persona non grata*.<sup>45</sup> To equate the United States in this scenario to a jealous husband spying on his ex-wife, or to an incredulous boss spying on his employees, is unreasonable. This episode in U.S.-German foreign relations was never seen, by any of the parties, as a pri-

---

41. Sourgens, *supra* note 1, at 382.

42. This is already an unpersuasive argument, as the privacy principle is presumably supposed to apply equally to both domestic and foreign surveillance, so it is unclear why it can only be justified through foreign surveillance rationales.

43. Sourgens, *supra* note 1, at 377.

44. *The NSA Secret Spy Hub in Berlin*, SPIEGEL ONLINE INT'L (Oct. 27, 2013), <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>.

45. Michael B. Kelley, *Germany Just Kicked Out the CIA's Berlin Station Chief*, BUS. INSIDER (July 10, 2014), <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>.

vate law matter. It was solely an issue of public law, resolved using political and diplomatic tools.

Moreover, at the heart of Sourgens's analysis stands the unfortunately prevalent and common mischaracterization of espionage, within international legal literature, as not constituting a "regulatory right" subject to the "sovereign prerogative" of states.<sup>46</sup> The literature has a blind spot when it comes to spying. In actuality, one can identify a plethora of legal sources that recognize, what I have termed the *jus ad explorationem*, a derivative, liberty right of the State to peacetime intelligence gathering.<sup>47</sup> These sources include the right of states to survival, recognized by the ICJ in the *Nuclear Weapons* advisory opinion (and the related collective right of self-determination of peoples); the laws on the use of force (and their recognition of a customary right for anticipatory self-

---

46. Sourgens, *supra* note 1, at 377. I acknowledge in this regard that Sourgens is merely citing back to a mountain of works that have been produced on espionage in international law, all of which seem to suggest that espionage is neither legal nor illegal, operating beyond the realm of the law. This is, I argue, a classic case of *argumentum ad populum*, each scholar piggybacking on the shoulders of his predecessor. They all suggest that the international law of espionage is unstated, because none of them are creative or daring enough to state it. Thus everyone seems to believe that espionage and international law are strangers, simply because no one has said otherwise before. See, e.g., Human Rights Council, Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Martin Scheinin, at 9, U.N. Doc. A/HRC/10/3 (2009) ("[N]o general norm exists in international law expressly prohibiting or limiting acts of intelligence gathering . . . ."); Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L. L. REV. 1091, 1091 (2004) ("Espionage is curiously ill-defined under international law, even though all developed nations, as well as many lesser-developed ones, conduct spying and eavesdropping operations against their neighbors."); Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115, 116 (2014) ("[T]here is a long-standing (and cynically named) 'gentleman's agreement' between nations to ignore espionage in international law."); Richard Falk, *Foreword*, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW v, v (Roland J. Stranger ed., 1962) ("[T]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture"); David Silver, *Intelligence and Counterintelligence*, in NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005) ("There is something almost oxymoronic about addressing the legality of espionage under international law . . . despite the ambiguous state of espionage under international law, it is not specifically prohibited by treaty or other international legal mechanism."); W. Hays Parks, *The International Law of Intelligence Collection*, in NATIONAL SECURITY LAW 433, 433-34 (John Norton Moore et al. eds., 1st ed. 1990) ("No serious proposal ever has been made within the international community to prohibit intelligence collection as a violation of international law because of the tacit acknowledgement by nations that it is important to all, and practiced by each."); Simon Chesterman, *The Spy Who Came In From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L. L. 1071, 1072 (2006) ("Despite its relative importance in the conduct of international affairs, there are few treaties that deal with it directly. Academic literature typically omits the subject entirely, or includes a paragraph or two defining espionage and describing the unhappy fate of captured spies. For the most part, only special regimes such as the laws of war address intelligence explicitly. Beyond this, it looms large but almost silently in the legal regimes dealing with diplomatic protection and arms control."); Geoffrey Demarest, *Espionage in International Law*, 24 DENV. J. INT'L. L. & POL'Y 321, 321 (1996) ("International Law regarding peacetime espionage is virtually unstated, and thus international law has been an inappropriate and inadequate reference for either condemnation or justification of actions involving intelligence gathering."); Jeffrey H. Smith, *Keynote Address: State Intelligence Gathering and International Law*, 28 MICH. J. INT'L. L. 543, 544 (2007) ("[M]ost lawyers would likely scoff at the notion that espionage activities are constrained in any meaningful way by international law. Indeed most probably believe that international law's only influence on espionage is that in wartime, spies caught behind the lines out of uniform can be shot. Hardly a sophisticated or, to intelligence services, comforting notion."). Most recently, the international group of experts who worked at the invitation of the NATO Cooperation Cyber Defence Centre of Excellence agreed "there is no prohibition of espionage *per se*" under international law. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 168 (2d ed. 2017) (concluding that peacetime espionage is not *per se* regulated by international law).

47. See Lubin, *supra* note 5, at 23-24.

defense); international human rights law (and the obligation of states to respect and ensure the right to life, liberty, and security of all persons subject to their jurisdiction); international humanitarian law (and the obligation of States to develop effective intelligence systems in preparation for war); collective security under U.N. Law (and the obligations of States under both treaty law and United Nations Security Council Resolutions to participate in the maintenance of international peace and security including through the sharing of intelligence to counter terrorism and the proliferation of WMDs, and to ensure the success of sanctions regimes); international disaster response laws and international environmental laws (which mandate cooperation in intelligence-gathering); and international accountability regimes (which depend on effective factual determinations that, in some cases, can only be achieved through continuous monitoring).<sup>48</sup>

In this short response piece, I am unable to fully engage in an analysis of each of these sources of law. Let me just focus on the right to anticipatory self-defense, as an example. Dating back to the Caroline incident of 1837, the right of a State to engage in pre-emptive self-defense in order to avert an attack that is “instant, overwhelming, leaving no choice of means, and moment of deliberation”<sup>49</sup> has been extensively analyzed.<sup>50</sup> Even those who still maintain, based on the wording of U.N. Charter Article 51, that a right of self-defense applies only “if an armed attack occurs,” cannot ignore diverse and robust subsequent practice by states.<sup>51</sup> The 2004 High-level Panel on Threats, Challenges, and Change established by the U.N. Secretary-General thus recognized that “a threatened State, according to long established international law, can take military action as long as the threatened attack is imminent, no other means would deflect it and the action is proportionate.”<sup>52</sup> Regardless of what interpretation of “imminence” one adopts, from a classically restrictive “Pearl Harbor”-type position to a highly permissive “Bush doctrine”-type position,<sup>53</sup> both ends of the spectrum, and everything in between, will embrace a State’s derivative right to

---

48. The prescriptive evidence is further backed by the function that intelligence plays in maintaining our public world order. See generally Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMP. L.Q. 365 (1973); Baker, *supra* note 46, at 1102-11.

49. See generally R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AM. J. INT’L. L. 82 (1938).

50. For a summary of the literature, see Christopher Greenwood, *Self-Defence*, MAX PLANCK ENCYCLOPEDIA PUB. INT’L L. (Apr. 2011), <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401?prd=EPIL>. For a more recent review of the literature, see Monica Hakimi, *North Korea and the Law on Anticipatory Self-Defense*, EJIL: TALK! (Mar. 28, 2017), <https://www.ejiltalk.org/north-korea-and-the-law-on-anticipatory-self-defense/>.

51. W. Michael Reisman & Andrea Armstrong, *The Past and Future of the Claim of Pre-emptive Self-Defense*, 100 AM. J. INT’L. L. 525, 526 (2006) (noting that anticipatory self-defense was not, in their view, “in the contemplation of drafters of the Charter, though claimed by many to have been grafted thereon by subsequent practice,” followed by a showing of such practice through case studies).

52. Sec’y Gen.’s High-Level Panel on Threats, Challenges, and Change, *A More Secure World: Our Shared Responsibility*, UNITED NATIONS 63 (2004), [http://www.un.org/en/peacebuilding/pdf/historical/hlp\\_more\\_secure\\_world.pdf](http://www.un.org/en/peacebuilding/pdf/historical/hlp_more_secure_world.pdf).

53. For more moderate interpretations, see Daniel Bethlehem, *Principles Relevant to the Scope of a State’s Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT’L. L. 769 (2012); Jeremy Wright, *The Modern Law of Self-Defense*, EJIL: TALK! (Jan. 11, 2017), <https://www.ejiltalk.org/the-modern-law-of-self-defence/>.

engage in peacetime intelligence gathering. For how else will a State know when a threat reaches whatever level of imminence is deemed sufficient to justify military action? If a State is entitled to retaliate against imminent threats to its survival, by definition it must be allowed to engage in peacetime espionage to gather the information necessary to reach that very conclusion. Even were we to adopt the formalistic and anachronistic approach that only Article 51 applies (and therefore that a State may only react to an imminent threat by seeking Security Council authorization) there would still be a derivative right for States to engage in peacetime espionage. For how else will a Delegation be able to prove to the Security Council that a threat is mounting, so to convince its members to vote in favor of an authorization of the use of force? To the extent that the United Nations does not have its own intelligence capacities, the Security Council must rely on Member States in order to fulfill its mandate of maintaining peace and security.<sup>54</sup> We can and should debate under what circumstances, or by what means, the right to spy might be abused or disproportionately extended, but to claim that espionage is not “*a priori* permissible as a sovereign prerogative” seems inconceivable in our public world order, and it certainly ignores the realities of state practice.

### C. *The Circular Fallacy in Determining Compatibility*

Sourgens’s compatibility analysis, the second test he lays out to prove the existence of a general principle, suffers from circular reasoning. Consider for example the classic circular reasoning fallacy:

Person A: God exists.

Person B: Why should I believe that?

Person A: Because the Bible says God exists.

Person B: Why should I believe anything the Bible says?

Person A: Because the Bible is the inspired word of God.

In this example God is true because of the Bible, and the Bible is true because of God. Put differently, the proposition is supported by the premise, which in turn is supported by the proposition, creating a circle in reasoning in which no real authority is being cited. Compare this to Sourgens’s analysis of the compatibility of the privacy principle with international law.

Sourgens: A general privacy principle, distinct from the ICCPR privacy right, exists.

Lubin: Why should I believe that?

---

54. In fact, even if one does not recognize the existence of a right of anticipatory self defense (a position held by a number of States, namely China, India, and members of the Non-Aligned Movement), one must still recognize the derivative right of States’ for peacetime intelligence gathering. That is because, at a minimum, all States recognize the Security Council’s role in carefully assessing the immanency of threats to international peace and security. With the U.N. lacking any intelligence producing powers, how is the Security Council to exercise this function, if not through the review of intelligence gathered, analyzed, and disseminated to it by its members? See TOM RUYSS, ‘ARMED ATTACK’ AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY INTERNATIONAL LAW AND PRACTICE 341 (2010) (identifying the states which do not recognize a right of anticipatory self defense).

Sourgens: Because all examined legal systems “expressly recognize a right to privacy as a matter of their private law.”<sup>55</sup>

Lubin: Why should I believe that anything these countries legislate, as a matter of their private law, is a general principle of international law?

Sourgens: Because it is compatible with the ICCPR privacy right.

To establish the existence of the principle, Sourgens looks at domestic civil legislation in six jurisdictions that have adopted the right to privacy.<sup>56</sup> Once the principle is identified, Sourgens attempts to prove its compatibility with international law, by analogizing it back to the ICCPR privacy right.<sup>57</sup> The proposition (that a privacy principle separate from a privacy right exists) is supported by the premise (that the domestic legislation of states is converging to recognize privacy as a principle compatible with international law). However, that premise is then supported by the proposition (as any compatibility could only be drawn from relying back on the very international human right to privacy which was deemed inoperable and which launched our quest to find this principle in the first place).

“Good faith,” for example, is a general principle of international law because it is compatible across different international legal fields. One can find good faith in treaty negotiation and interpretation, as well as in the admission of a state to the United Nations. One can find good faith in international environmental law, as well as in the law of international adjudication.<sup>58</sup> On the other hand, one can find Sourgens’s privacy principle only in the privacy right, making his reliance on that human right to prove a general principle distinct from human rights a circular fallacy.

It should therefore come as no surprise that the content of the principle itself merely echoes the content of the right. It is the same king wearing a different tunic. Sourgens spends significant time in Parts IV and V analyzing different privacy definitions and applying standards of proportionality to the newly found principle—but in essence the definitions and standards put forward are all part and parcel of the human right to privacy discourse. The privacy principle did not replace, or supplant that discourse, as Sourgens had intended it to; it simply reproduced it.

But even were we to ignore all of this, and assume the existence of a privacy principle under international law, what would it all mean? If the human right to privacy is nothing more than a normative hope without means of ready legal enforcement, as Sourgens believes, what is to be said about the privacy principle? How is it, in any way, more enforceable? Why are the P5 more likely to follow this principle than they are the human right to privacy? What mechanisms does this principle provide that were lacking within our existing frameworks? These questions must be answered, as general principles of internation-

---

55. Sourgens, *supra* note 1, at 378.

56. *Id.* at 379-82.

57. *Id.* at 388-391.

58. See generally Steven Reinhold, *Good Faith in International Law*, 2 UCL J. L. & JURIS. 40 (2013).

al law tend to inspire more literature than practical use.<sup>59</sup> Sourgens promises that privacy-as-a-principle would allow us to overcome the treaty-based limitations that hinder the effectiveness of the privacy right.<sup>60</sup> However, he ignores the fact that once we stop using human rights law as our grounds for finding a violation, we can no longer rely on human rights mechanisms and institutions to demand accountability (such as the human rights treaty bodies, the regional human rights courts, and the Human Rights Council and its Special Procedures). Note in this regard that the introduction of a privacy principle (on top of the treaty and customary individual rights to privacy) could potentially cause further fragmentation in international law, with different layers of legal protections and obligations colliding. Such fragmentation is likely to lead to less, rather than more, protection of privacy in the long haul. Sourgens therefore bears the burden of proving that the introduction of a privacy principle will lead to an overall increase in privacy protection. A burden he has not met.

### III. THE RIGHT TO PRIVACY: THE ONE TRUE HEIR TO THE THRONE

International human rights law is certainly not a panacea for all the world's ills and misfortunes. As William Burke-White has noted, "promotion of human rights has long been viewed as a luxury, to be pursued when the Government has spare diplomatic capacity and national security is not being jeopardized."<sup>61</sup> Sourgens's account of the limited effectiveness of the human right to privacy must be considered within this context. I will argue that discounting the many milestones and success stories of recent years does a disservice to the privacy agenda. It is also unhelpful to overplay archaic arguments about the application of human rights treaties' extraterritorially, or to overemphasize the refusal of certain superpowers to ratify fundamental human rights treaties. I address each of these points in turn.

#### A. *The Evolution of the International Privacy Agenda*

The international community has taken significant steps to enhance privacy protections since the signing of the ICCPR in 1966 and the Human Rights Committee's adoption of General Comment No. 16 on the right to privacy in 1988.<sup>62</sup> These accomplishments include, since 1999, a significant body of work on human rights and surveillance practices by the U.N. High Commissioner for

---

59. MANLEY OTTMER HUDSON, *THE PERMANENT COURT OF INTERNATIONAL JUSTICE 1920-1942: A TREATISE* 609 (1943) (noting that general principles in practice have loomed "less large" than in the literature which they have inspired and suggesting that this could be owed to "a sense of caution" taken by the PCIJ in their application).

60. Sourgens, *supra* note 1, at 406 ("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").

61. William W. Burke-White, *Human Rights and National Security: The Strategic Correlation*, 17 *HARV. HUM. RTS. J.* 249, 251 (2004).

62. Human Rights Comm., General Comment 16, Twenty-second session, 1988, p.21 U.N. Doc. HRI/GEN/1/Rev.1 (1994) U.N. Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1, at 21 (Apr. 8, 1988).

Human Rights and the U.N. Special Rapporteurs on Freedom of Expression and Counter-Terrorism.<sup>63</sup> The repeated adoption of both U.N. General Assembly Resolutions and U.N. Human Rights Council Resolutions, by consensus, on the right to privacy in the digital age also marks a significant step forward.<sup>64</sup> The 2015 creation of a U.N. Special Rapporteur on the Right to Privacy is itself a reaffirmation of the international privacy agenda, and his reports to the Council further signify the importance of his new role as an international intelligence watchdog.<sup>65</sup> The U.N. Human Rights Committee has begun to routinely address surveillance legislation and practices in its Concluding Observations to States, beginning in 2014.<sup>66</sup> On the regional level, the European Court of Human

---

63. See, e.g., Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009); Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/17/27 (May 16, 2011); Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/20/17 (June 4, 2012); Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013); Rep. of the Office of the United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014); Rep. of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (Sept. 23, 2014); Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/29/32 (May 22, 2015); Rep. of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/32/38 (May 11, 2016); Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/HRC/34/61 (Feb. 21, 2017).

64. U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/69/166 (Dec. 18, 2014); U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/28/L.27 (Mar. 24, 2015); U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/71/199 (Dec. 19, 2016); U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/L.7/Rev.1. See also U.N. Human Rights Council Resolution on the Safety of Journalists, U.N. Doc. A/HRC/33/L.6 (Sept. 26, 2016).

65. See, e.g., Rep. of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/HRC/31/64 (Mar. 8, 2016); Rep. of the Special Rapporteur on the Right to Privacy, U.N. Doc. A/71368 (Aug. 30, 2016). For a critique of the work of the Special Rapporteur to date, see Marc Rotenberg, *Urgent Mandate, Unhurried Response: An Evaluation of the UN Special Rapporteur on the Right to Privacy*, 3 EUR. DATA PROTECTION L. REV. 47 (2017).

66. See, e.g., Concluding Observations of the Fourth Periodic Rep. of the United States of America, Human Rights Committee, U.N. Doc. CCPR/C/USA/CO/4 (Apr. 23, 2014); Concluding Observations on the Initial Periodic Rep. of Malawi, Human Rights Committee, U.N. Doc. CCPR/C/MWI/CO/1/Add.1 (Aug. 19, 2014); Concluding Observations on the Fifth Periodic Rep. of Sri Lanka, Human Rights Committee, U.N. Doc. CCPR/C/LKA/CO/5 (Nov. 21, 2014); Concluding Observations on the Seventh Periodic Rep. of the Russian Federation, Human Rights Committee, U.N. Doc. CCPR/C/RUS/CO/7 (Apr. 28, 2015); Concluding Observations on the Sixth Periodic Rep. of Canada, Human Rights Committee, U.N. Doc. CCPR/C/CAN/CO/6 (Aug. 13, 2015); Concluding Observations on the Third Periodic Rep. of the Former Yugoslav Republic of Macedonia, Human Rights Committee, U.N. Doc. CCPR/C/MKD/CO/3 (Aug. 17, 2015); Concluding Observations on the Fifth Periodic Rep. of France, Human Rights Committee, U.N. Doc. CCPR/C/FRA/CO/5 (Aug. 17, 2015); Concluding Observations on the Seventh Periodic Rep. of the United Kingdom of Great Britain and Northern Ireland, Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7 (Aug. 17, 2015); Concluding Observations on the Fourth Periodic Rep. of the Republic of Korea, Human Rights Committee, U.N. Doc. CCPR/C/KOR/CO/4 (Dec. 3, 2015); Concluding Observations on the Second Periodic Rep. of Namibia, Human Rights Committee, U.N. Doc. CCPR/C/NAM/CO/2 (Apr. 22, 2016); Concluding Observations on the Initial Rep. of South Africa, Human Rights Committee, U.N. Doc. CCPR/C/ZAF/CO/1 (Apr. 27, 2016); Concluding Observations on the Seventh Periodic Rep. of Sweden, Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7 (Apr. 28, 2016); Concluding Observations on the Sixth Periodic Rep. of New Zealand, Human Rights Committee, U.N. Doc. CCPR/C/NZL/CO/6 (Apr. 28, 2016); Concluding Observations on the Fourth Periodic Rep. of Rwanda, Human Rights Committee, U.N. Doc. CCPR/C/RWA/CO/4 (May 2, 2016); Concluding Observations on the Sixth Periodic Rep. of Denmark, Human Rights Committee, U.N. Doc. CCPR/C/DNK/CO/6 (Aug. 15, 2016); Concluding Observations

Rights, the Court of Justice of the European Union, and the Inter-American Commission and Court on Human Rights have developed considerable and authoritative jurisprudence on surveillance and privacy.<sup>67</sup>

For a legal positivist, these advancements might seem insignificant, as most of the above are soft law or regional instruments without the binding effect of black-letter texts. Nonetheless, they have had profound impacts on the practice of intelligence agencies. Consider the following anecdotal examples: Canada's 2016 decision to temporarily halt intelligence sharing with its Five Eyes partners following revelations of unlawful surveillance of Canadians;<sup>68</sup> the launch in 2014 of the German Parliamentary Committee investigating the NSA spying scandal (the final report of which is currently being written) which has already led to a reduction in BND-NSA cooperation,<sup>69</sup> as well as to various

---

on the Seventh Periodic Rep. of Colombia, Human Rights Committee, U.N. Doc. CCPR/AZE/CO/4 (Nov. 4, 2016); Concluding Observations on the Sixth Periodic Rep. of Morocco, Human Rights Committee, U.N. Doc. CCPR/C/MAR/CO/6 (Nov. 4, 2016); Concluding Observations on the Seventh Periodic Rep. of Poland, Human Rights Committee, U.N. Doc. CCPR/C/POL/CO/7 (Nov. 4, 2016); Concluding Observations on the Sixth Periodic Rep. of Italy, Human Rights Committee, U.N. Doc. CCPR/C/ITA/CO/6 (Mar. 28, 2017); Concluding Observations on the Second Periodic Rep. of Turkmenistan, Human Rights Committee, U.N. Doc. CCPR/C/TKM/CO/2 (Mar. 28, 2017). For further reading see Yuval Shany, *On-Line Surveillance in the Case-law of the UN Human Rights Committee*, Hebrew University Cyber Security Research Center (July 2017), <http://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee> (noting that “whereas questions relating to [surveillance] were raised with respect to two states between 2007-2014, since 2014 they have been addressed with respect to 15 different states (representing more than 25% of the states reviewed by the Committee during this period). This sharp rise is suggestive both of the growing resort to on-line surveillance powers by governments due to advances in available technology, and of growing awareness to their human rights implications by the Committee.”).

67. See, e.g., *Klass & Others v. Germany*, App. No. 5029/71, European Court of Human Rights, Judgment (Sept. 6, 1978); *Kopp v. Switzerland*, App. No. 23224/94, European Court of Human Rights, Judgment (Mar. 25, 1998); *Weber & Saravia v. Germany*, App. No. 54934/00, European Court of Human Rights, Decision on Admissibility (June 29, 2006); *Liberty and Others v. The United Kingdom*, App. No. 58243/00, European Court of Human Rights, Judgment (July 1, 2008); *Kennedy v. United Kingdom*, App. No. 26839/05, European Court of Human Rights, Judgment (May 18, 2010); *Uzun v. Germany*, App. No. 35623/05, European Court of Human Rights, Judgment (Sept. 2, 2010); *Szabó & Vissy v. Hungary*, App. No. 37138/14, European Court of Human Rights, Judgment (Jan. 12, 2016); *Digital Rights Ireland Ltd v. Minister of Communications, Marine & Natural Resources et al.* (C-293/12); *Kärntner Landesregierung and others* (C-594/12), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (Apr. 8, 2014); *Maximilian Schrems v. Data Protection Commissioner*, Case C-362/14, Court of Justice of the European Union, Grand Chamber, Judgment (Oct. 6, 2015); *Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14, Court of Justice of the European Union, Second Chamber, Judgment (Oct. 19, 2016); *Tele2 Sverige AB v. Post- Och telestyrelsen* (C-203/15); *Secretary of State for the Home Department v. Tom Watson et al.* (C-698/16), Joined Cases, Court of Justice of the European Union, Grand Chamber, Judgment (Dec. 21, 2016); *Opinion on the Agreement Envisaged between the European Union and Canada on the Transfer of Passenger Name Record Data*, Case C-1/15, Court of Justice of the European Union, Grand Chamber (26 July 2017); *Garcia v. Peru*, Inter-American Court of Human Rights, Case 11.006, Report No. 1/95, OEA/Ser.L/V/II.88 (Feb. 17, 1995); *Tristán Donoso v. Panamá*, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No. 193 (Jan. 27, 2009); *Escher et al. v. Brazil*, Inter-American Court of Human Rights, Judgment (on Preliminary Objection, Merits, Reparations, and Costs), Series C No. 200 (July 6, 2009); *Ms. X & Y v. Argentina*, Inter-American Commission on Human Rights, Case 10.506, Report No. 38/96 (Oct. 15, 1996).

68. AFP in Ottawa, *Canada Spy Agency Stops Sharing Intelligence With International Partners*, *GUARDIAN* (Jan. 28, 2016), <https://www.theguardian.com/world/2016/jan/28/canada-spy-agency-broke-law-by-passing-citizens-metadata-to-foreign-partners>.

69. *Germany Spying Scandal: BND 'Reduces NSA Co-operation'*, *BBC NEWS* (May 7, 2015), <http://www.bbc.co.uk/news/world-europe-32625808>.



cases being brought in German Courts;<sup>70</sup> the U.S. ruling finding Section 215 on bulk metadata collection illegal;<sup>71</sup> and recent amendments to Section 702 policies.<sup>72</sup>

Just imagine you could go back in time to the middle of the Cold War and suggest to a KGB agent that in 2015 the European Court of Human Rights would rule that Russian surveillance policies constituted an unnecessary and disproportionate interference with privacy rights. That KGB agent would have probably thought you were mad. Those were different times, as David Cornwell writes. It was a time when individuals

were being shadowed, their phones were being tapped, their cars and houses bugged, neighbors suborned. Their letters were arriving a day late, their husbands, wives, and lovers were reporting on them, they couldn't park their cars without getting a ticket. The taxman was after them and there were men who didn't look at all like real workmen doing something to the drains outside the house, they'd be loitering there all week and achieved nothing.<sup>73</sup>

It was a world in which spying was conducted without statutory limitations or parliamentary oversight, without minimization procedures or structured safeguards, without transparency mandates or notification obligations, without *ex ante* independent authorizations or *ex post* effective review. We have human rights defenders and digital rights activists to thank for their relentless hard work in changing our entire conceptualization of the practice of intelligence agencies and their public legal relationship with the people who they purport to serve.

Human rights advocacy is not for the fainthearted. The tools at the disposal of advocates are limited to different forms of agitation and the application of pressure through strategic litigation, investigative reporting, shaming campaigns, public awareness initiatives, and network building. It is a slow and painstaking process. The impact is gradual and often feels miniscule. Political events might turn years of hard work on its head. Recent ISIS-inspired terrorist attacks across the European continent have brought with them a new wave of mass surveillance legislation across EU member states, which stands in stark contradiction to the human rights protections laid down by the regional courts.<sup>74</sup> But this setback should not be a reason to give up on the human rights agenda. The great Louis Henkin wrote that “human rights” is not a single idea, but rather, it is “the sum of pairs of ideas in tension.”<sup>75</sup> Privacy and security are one of those pairings, and in this ultimate tug of war, there are continuous un-

---

70. *German Constitutional Court Rules Out Access to NSA's 'Selectors' List*, DEUTSCH WELLE (Nov. 15, 2016), <http://www.dw.com/en/german-constitutional-court-rules-out-access-to-nsas-selectors-list/a-36396385>.

71. Charlie Savage & Jonathan Weisman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. TIMES (May 7, 2015), <https://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html>.

72. Jennifer Granick, *Today's ODNI and Section 702 News*, JUST SECURITY (Apr. 28, 2017), <https://www.justsecurity.org/40391/todays-odni-section-702-news/>. Section 702 is scheduled to sunset on December 31, 2017 unless Congress passes legislation to remove or extend the sunset provision.

73. JOHN LE CARRÉ, *THE PIGEON TUNNEL: STORIES FROM MY LIFE* 165-166 (2016).

74. See Asaf Lubin, *A New Era of Mass Surveillance is Emerging Across Europe*, JUST SECURITY (Jan. 9, 2017), <https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/>.

75. Louis Henkin, *Rights: Here and There*, 81 COLUM. L. REV. 1582, 1610 (1981).

dercurrences and dynamics at play. One should not be tempted to forego the cause, simply because at any specific moment in time one of the dyads seems to be pushing stronger in a specific direction.

*B. The Extraterritorial Applicability of the Right to Privacy*

Arguments about extraterritoriality are at the heart of Sourgens's disenchantment with IHRL. These arguments must not be overplayed and should all be taken with a grain of salt. Rather than surrender, we must vehemently oppose the *teatro de la comedia* that surrounds the anarchic arguments, still being raised by a number of countries<sup>76</sup> and scholars,<sup>77</sup> in support of a territorially constrained conception of human rights. It has now been firmly established that states must respect and ensure human rights to all individuals subject to their jurisdiction, regardless of whether those individuals are situated within that state's territory.<sup>78</sup> As Marko Milanovic has framed it, this is indeed a fundamental element of the "moral logic of human rights law,"<sup>79</sup> which triggers states' human rights obligations wherever they purport to exercise a certain degree of control. In this regard, most foreign surveillance programs involve actions by public authorities of the State within its own territory and subject to its effective control. Consider for example the PRISM program, which involves the collection of internet communications under Section 702 from at least nine major U.S. internet companies.<sup>80</sup> The collection, retention, analysis, and later dissemination of information are all conducted by U.S. government officials, in U.S. Government facilities, subject to the U.S. Government's effective control. The fact that the targets are foreign nationals residing in foreign territory cannot

---

76. See, e.g., Eric A. Posner, Univ. of Chi., Statement to the Privacy & Civil Liberties Oversight Board (Mar. 14, 2014), <https://www.pclob.gov/library/20140319-Testimony-Posner.pdf>.

77. See, e.g., Michael Dennis, *Non-Application of Civil and Political Rights Treaties Extraterritorially During Times of International Armed Conflict*, 40 ISR. L. REV. 453, 461-481 (2007); Michael Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflicts and Military Occupation*, 99 AM. J. INT'L L. 119, 122-127 (2005); Dietrich Schindler, *Human Rights and Humanitarian Law: Interrelationship of the Laws*, 31 AM. U. L. REV. 935 (1982).

78. See, e.g., U.N. Human Rights Committee, General Comment 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) ("States Parties are required by Article 2, paragraph 1, to respect and to ensure the Covenant rights to all persons who may be within their territory and to all persons subject to their jurisdiction. This means that a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party. . . This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained"); *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. Rep. 136, ¶¶ 107-113 (July 9) ("The Court would observe that, while the jurisdiction of States is primarily territorial, it may sometimes be exercised outside the national territory. Considering 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. . . . The travaux préparatoires of the Covenant confirm the drafters of the Covenant did not intend to allow States to escape from their obligations when they exercise jurisdiction outside their national territory.") See generally MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011).

79. Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L.J. 81, 100 (2015).

80. See REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 7 (July 2, 2014).

serve as the basis for claiming that the individuals have not come within U.S. jurisdiction for the purposes of IHRL application in the context of this program.

Moreover, contrary to Sourgens's portrayal, the fact is that the United States has never expressly stated its position as to whether the human rights treaties apply to its foreign surveillance programs. The Privacy and Civil Liberties Oversight Board left this matter unresolved.<sup>81</sup> If anything, Presidential Policy Directive 28, seems to point in the direction of recognition of (some) privacy obligations.<sup>82</sup> Regardless of the U.S. position on this matter, the U.N. General Assembly,<sup>83</sup> the Human Rights Committee,<sup>84</sup> the Venice Commission,<sup>85</sup> and the Court of Justice of the European Union<sup>86</sup> have all recognized the applicability of human rights obligations to foreign surveillance programs (albeit not always explicitly).

More interestingly, and perhaps unsurprisingly, in the *10 Human Rights NGOs v. United Kingdom* case, currently pending before the European Court of Human Rights (which directly concerns the legality of global mass surveillance programs, including Tempora, PRISM, and Upstream), the U.K. Government did not even challenge the extraterritorial applicability of the ECHR. Instead, both the Applicants and the Respondent ignored the issue altogether, tacitly accepting that the obligation to respect and ensure the right to privacy was triggered by the nature and scope of the disputed programs.

But even if foreign surveillance programs do not trigger the ICCPR's applicability, the right to privacy is additionally part of customary international law, and its applicability to foreign surveillance programs can be derived from customary law. As Rengel notes:

[g]iven the extensive amount of recognition in international instruments of the right to privacy, the prominent place that the topic of privacy continues to occupy in writings and commentary, and the treatment as binding norm that the right to privacy

---

81. *Id.*, at 100.

82. Presidential Policy Directive 28, Signals Intelligence Activities, OFFICE OF THE PRESS SECRETARY (Jan. 17, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> (“[O]ur signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or whether they might reside, and that all persons have legitimate privacy interests in the handling of their personal information . . . . U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.”).

83. See list of UNGA Resolutions, *supra* note 64.

84. See list of HRC Concluding Observations, *supra* note 66.

85. European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, CDL-AD(2015)006, Study No. 719/2013, ¶ 6 (Apr. 7, 2015) (“The collection of signals intelligence may legitimately take place on the territory of another state with its consent, but might still fall under the jurisdiction of the collecting state from the view point of human rights obligations under the ECHR. At any rate, the processing, analysis and communication of this material clearly falls under the jurisdiction of the collecting State and is governed by both national law and the applicable human rights standards. There may be competition or even incompatibility between obligations imposed on telecommunications companies by the collecting state and data protection obligations in the territorial state; minimum international standards on privacy protection appear all the more necessary.”).

86. Case C-362/14, Maximilian Schrems v. Data Protection Commissioner, ¶ 94 (Ct. Justice EU Oct. 6, 2015) (“[L]egislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter.”).

has received in both national and international legal systems, it can be concluded that there is a general fundamental right to privacy under customary international law. Although the need for protection of the right to privacy continues to expand, it appears that in certain contexts there is widespread recognition that the right to privacy protects individuals from the actions of the state and third parties infringing on that right.<sup>87</sup>

For this reason alone, there is no need to revert to a general principle of international law. Even in a country like China, which is not party to the ICCPR, the customary protections of privacy would mean that any state action “must be reviewed with the presumption that the state’s interference is only permitted in situations where there are compelling governmental interests at stake,”<sup>88</sup> applying general standards of necessity, reasonableness and proportionality.

#### IV. PRIVACY AND MASS SURVEILLANCE: A KINGDOM IN SEARCH OF A PARADIGM SHIFT

Standing at the heart of Sourgens’s piece is a claim that I am very sympathetic to—there is a need for a “paradigm shift” in the discourse surrounding foreign mass surveillance and the right to privacy. In other words, there is a need to ensure that the human rights frameworks developed by treaty bodies, regional courts, and special rapporteurs are not only normatively compelling but also offer a realistic means of protecting global privacy rights while taking into account the legitimate security needs of States. While I raised concerns about the solution proposed by Sourgens, I am grateful for his effort to advocate for creative thinking around this problem.

In a recent Article, I too recognized the growing and troubling gap “between the practice of State surveillance agencies and the deep-seated commitments of human rights experts.”<sup>89</sup> The way to bridge this gap, in my opinion, is not through the introduction of an external privacy principle, but rather through a shift in thinking within the human rights community on privacy protections in the foreign surveillance context: *not a Privacy Principle, but a Principled Privacy Right*.

While human rights experts continue to adamantly uphold the myth of a universal right to privacy, in actuality a different operational code has already emerged in which “our” right to privacy is routinely distinguished from “theirs.” There is one set of privacy protections for those within the State’s territory, and another set of lower protections (if any) for those outside the territory. “This distinction is a common feature in the wording of electronic communications surveillance laws and the practice of signals intelligence collection agencies, and it is further legitimized . . . by the steadfast support of the laymen general public.”<sup>90</sup>

---

87. ALEXANDER RENGEL, *PRIVACY IN THE 21<sup>ST</sup> CENTURY* 108 (2013).

88. *Id.*

89. Asaf Lubin, “*We Only Spy on Foreigners*”: *The Myth of a Universal Right to Privacy and the Practice of Mass Extraterritorial Surveillance*, CHI. J. INT’L L. (forthcoming 2018).

90. *Id.*

In the article, I contend that there are justifications for the distinction. Discrepancies in jurisdictional reach and technological capacities make it necessary to allow Governments greater leniency in adopting certain foreign surveillance policies. In the name of an absolutist battle for universality, human rights defenders are losing the far bigger war. Stepping outside the shouting matches and binary splits that characterize so much of the privacy versus security discourse, I suggest that we focus our attention not on one-size-fits-all regulation of domestic and foreign surveillance, but rather expand our thinking to take into account the needs of intelligence agencies as they engage in extraterritorial surveillance for national security purposes.<sup>91</sup> This regulatory shift is more likely to bring States into the fold and ultimately serve what Sourgens identifies as a need for developing “a policy tool as well as a legal limit on state conduct” in the sphere of foreign intelligence gathering.<sup>92</sup> It will offer a mediating remedy to the data-obsessed surveillance state in an age where “politics are subordinated to a kind of algorithmic authoritarianism.”<sup>93</sup>

---

91. Asaf Lubin, Foreign Surveillance and Anti-Discrimination: The Justifications for Applying Different Safeguards for Extraterritorial Surveillance, Hebrew University Cyber Security Research Center Blog (Aug. 19, 2017), [http://csrcl.huji.ac.il/people/foreign-surveillance-and-anti-discrimination-justifications-applying-different?ref\\_tid=3718](http://csrcl.huji.ac.il/people/foreign-surveillance-and-anti-discrimination-justifications-applying-different?ref_tid=3718).

92. Sourgens, *supra* note 1, at 406.

93. HENRY A. GIROUX, DANGEROUS THINKING IN THE AGE OF THE NEW AUTHORITARIANISM 39 (2015).