On War and Peace in Cyberspace

– Security, Privacy, Jurisdiction –

by LOTHAR DETERMANN* *and* KARL T. GUTTENBERG**

The public debate surrounding Edward Snowden's revelations about NSA spying, and government surveillance in times of war and peace more generally, is passionate, persistent, utterly unfocused, and unproductive. Politicians and commentators have pursued various agendas in the course of this debate, few of which acknowledge the technological and legal realities of our world today, but rather acquiesce to a public that is frustrated and eager for action in the wake of a perceived breach of public trust. These various agendas are not all "hot air." Indulging public opinion has measurable, serious consequences that are complicating diplomatic relations and may be harmful to national and global security, economic cooperation and development, and ultimately, peace.

Asking governments to stop spying is an illusory undertaking. But, there are a few topics worthy of discussion and more within reach. The situation is sufficiently complex and warrants a closer look at the laws, facts, and myths underlying the current public debate.

---

* Lothar Determann teaches Internet, computer, and data privacy law at Freie Universität Berlin, University of California, Berkeley School of Law, and University of California, Hastings College of the Law, and practices law as a partner with Baker & McKenzie, LLP, in Palo Alto.

** Karl-Theodor zu Guttenberg, former Minister of Defense and former Minister of Economics & Technology of the Federal Republic of Germany is Chairman and Founder of Spitzberg Partners, LLC and Distinguished Statesman at the Center for Strategic and International Studies (CSIS), Washington, D.C. Opinions expressed herein reflect only the authors' views, and should not be imputed to their universities, firms, clients, or others. The authors thank Sarah Barkley, J.D. Candidate 2015, University of California, Hastings College of the Law, and Brendan Gilmartin, B.A. International Affairs, 2010, The George Washington University, for their valuable assistance.

I. NSA SNAFU

In the summer of 2013, Edward Snowden, an employee of the business and technology consulting firm Booz Allen Hamilton,[1] leaked classified information about his work on projects for the United States National Security Agency ("NSA") to various newspapers, then fled to Hong Kong, and eventually found a safe haven in Russia.[2] Newspaper reports revealed that the NSA collected vast amounts of information on Internet communications and international phone calls, including communications of foreign diplomats and government officials, most notably German chancellor Angela Merkel.[3]

Americans and those abroad reacted with outrage, politicians mobilized to respond to their constituents,[4] and foreign governments showed indignation—and some level of hypocrisy.[5] In the United States, several lawsuits against the government were filed, including a class action lawsuit brought by Senator Rand Paul against President Barack Obama.[6] In Europe, the European Parliament threatened to suspend the United States' access to key portions of the Society for Worldwide Interbank Financial Telecommunication ("SWIFT")

1. Julian Borger, *Booz Allen Hamilton: Edward Snowden's US Contracting firm*, THE GUARDIAN (June 9, 2013), http://www.theguardian.com/world/2013/jun/09/booz-allen-hamilton-edward-snowden.

2. Borger, *supra* note 1; James Risen, *Snowden Says He Took No Secret Files to Russia*, N.Y. TIMES, Oct. 17, 2013 at A1.

3. Karl T. Guttenberg, *Merkel's American Minders*, PROJECT SYNDICATE (Oct. 28, 2013), http://www.project-syndicate.org/commentary/karl-theodor-zu-guttenberg-on-the-fallout-from-us-spying-on-its-european-allies; Alison Smale, Melissa Eddy & David E. Sanger, *Data Suggests Push to Spy on Merkel Dates to '02,* N.Y. TIMES, Oct. 27, 2013, at A4. *See also* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT & ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), at 1, *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf.

4. Ewen MacAskill & Julian Borger, *New NSA Leaks show how U.S. is Bugging its European Allies*, THE GUARDIAN (June 30, 2013), http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

5. Karl-Theodor zu Guttenberg, *The American spying scandal is no ordinary diplomatic rift*, FIN. TIMES (Nov. 7 2013), http://www.ft.com/intl/cms/s/0/033a9e12-46ff-11e3-9c1b-00144feabdc0.html#axzz2vTNMOlm2.

6. James Fuller, *Rand Paul Files Suit Against Obama, NSA Wednesday*, WASH. POST (Feb. 12, 2014), http://www.washingtonpost.com/blogs/post-politics/wp/2014/02/12/rand-paul-files-suit-against-obama-nsa-today.

financial network,[7] free trade negotiations, and the transatlantic U.S.–EU Safe Harbor program.[8]

The European Commission is leading the charge to establish a "European Cloud."[9] German politicians and companies, including Deutsche Telekom, are advocating for "email made in Germany" and even a "German Internet," which would be required by German federal law to route domestic web traffic through servers located within Germany.[10] Chancellor Merkel recently called for the creation of a "European data network."[11] Pending trade agreements have been thrown into jeopardy as well: French President François Hollande demanded that the United States stop spying "immediately" and threatened to block negotiations over the ambitious Transatlantic Trade and Investment Partnership ("TTIP").[12]

Hysteria, it turns out, is not confined to Europe. Mere months after the NSA leak, the Brazilian government awarded a $4.5 billion fighter jet contract to Swedish manufacturer Saab, despite the fact

7. Stephen Gardner, *EU Draft Surveillance Resolution Might End Safe Harbor, SWIFT Data Sharing Programs,* PRIVACY & SECURITY L. REP. (Bloomberg BNA), Jan. 13, 2014, at 97. *See* Eur. Parl. Comm. on Civil Liberties, Justice & Home Affairs, DRAFT REPORT on the Electronic Mass Surveillance of EU Citizens: The Impact of US NSA Surveillance Programmes & Surveillance Bodies in Various EU Member States on EU Citizens Fundamental Rights & on EU-US Transatlantic Cooperation in Justice & Home Affairs, EUR. PARL. DOC. 2013/2188(INI) (2013) (Rapporteur: Claude Moraes).

8. *EU Threatens Suspension of Data Deal with U.S.*, EURACTIV.COM (Jan. 29, 2014), http://www.euractiv.com/infosociety/eu-threatens-suspension-data-dea-news-533093; Plenary Session Press Release, Eur. Parl., *US NSA: Stop Mass Surveillance Now or Face Consequences, MEPs Say* (Dec. 3, 2014), *available at* http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say.

9. Neelie Kroes, *Making Europe the Natural Home of Safe Cloud Computing,* NEELIE KROES'S BLOG (Nov. 14, 2011), http://ec.europa.eu/commission_2010-2014/kroes/en/content/making-europe-natural-home-safe-cloud-computing (Ms. Kroes is the Vice-President of the European Commission).

10. Leila Abboud & Peter Maushagen, *Germany wants a German Internet as Spying Scandal Rankles*, REUTERS (Oct. 25, 2013), http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025.

11. *See* Mark Scott, *EU Leaders Seek Way to Protect Individuals' Data,* N.Y. TIMES, Feb. 19, 2014, at B2.

12. Damien McElroy, Bruno Waterfield & Tom Parfitt, *François Hollande Tells the US to Stop Eavesdropping on Europe if it Wants Progress on Trade Deal,* THE TELEGRAPH (July 1, 2013), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10152478/Francois-Hollande-tells-the-US-to-stop-eavesdropping-on-Europe-if-it-wants-progress-on-trade-deal.html.

that Boeing had been the clear leader during the bid process.[13] The switch to Saab was widely reported to be a direct result of "the NSA problem," which deeply upset Brazilian President Dilma Rousseff.[14] Brazil and the European Union are developing an undersea data cable to circumvent U.S. spying and Brazil is negotiating an "Internet Constitution" titled the "Marco Civil da Internet," which will include a local data storage requirement for companies in the country.[15]

None of the foreign government reactions seem particularly rational, and each could adversely impact global cooperation and security. The ubiquitous SWIFT information-sharing network is trusted everyday by more than 10,000 financial institutions and corporations in 212 countries to exchange information in a secure and standardized manner.[16] Following the terrorist attacks of September 11, 2001, a transatlantic information-sharing agreement was struck, providing the United States Treasury Department with limited access to SWIFT data, enabling the United States to "follow the money" of suspected terrorists.[17] Strengthening and monitoring this network has been a key priority of global anti-terrorism and anti-money laundering initiatives.[18] The largely symbolic threat to suspend this arrangement, if realized, could severely jeopardize the ability of the United States and other governments to track and curb the financing of international terrorist networks.[19]

The U.S.-EU Safe Harbor framework is a unique international cooperative program that aims to facilitate the compliance of U.S. companies with EU data protection laws, and the enforcement of EU

13. Brian Winter, *Insight: How U.S. spying cost Boeing multi-billion dollar jet contract*, REUTERS (Dec. 20, 2013), http://www.reuters.com/article/2013/12/20/us-boeing-brazil-insight-idUSBRE9BJ10P20131220.

14. Alanos Soto & Brian Winter, *Update 3-Saab wins Brazil jet deal after NSA spying sours Boeing bid*, REUTERS (Dec. 18, 2013), http://www.reuters.com/article/2013/ 12/18/ brazil-jets-idUSL2N0JX17W20131218.

15. Angelica Mari, *Companies Brace for Brazil Local Data Storage Requirements*, ZDNET.COM (Mar. 7, 2014), http://www.zdnet.com/companies-brace-for-brazil-local-data-storage-requirements-7000027092/.

16. SWIFT.COM, *Company Information*, http://www.swift.com/about_swift/company_information/company_information?rdct=t&lang=en (last visited, Mar. 9, 2014).

17. Eric Lichtblau & James Risen, *Bank Data is Sifted by U.S. in Secret to Block Terror*, N.Y. TIMES (June 23, 2006), http://www.nytimes.com/2006/06/23/washington/ 23intel.html?hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage&_r=0.

18. *See id.*

19. *Id.*

data protection laws in the United States by the U.S. government.[20] More than 3,000 U.S. companies have voluntarily chosen to participate in the program, which offers additional legal protections for Europeans' personal data.[21] In retreating from the threat, European Union Home Affairs Commissioner Cecilia Malmström later acknowledged that improving the system was preferable to suspension, and the EU Commission ultimately reaffirmed its support for the program.[22]

A "Germany-only Internet" is technologically impractical and incompatible with EU Common Market law.[23] Similarly, "Europe-only" or "Brazil-only" clouds would constitute technological regress, restrict freedom of information and communications within and between countries, create tensions with World Trade Organization rules and various free trade agreements, and could ultimately harm the global economic recovery. These ideas embrace a position of what can be dubbed "data secessionism" and add to a "Balkanization" of the Internet.[24]

Moreover, neither initiative would reign in government surveillance. Snowden revealed that European governments operate intelligence programs similar to the NSA and regularly share

20. *See* U.S.-EU SAFE HARBOR CERTIFICATION WEBSITE, *U.S.-EU Safe Harbor Overview,* http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Mar. 18, 2014); Brian Hengesbaugh, Amy de La Lama & Michael Egan, *European Commission Reaffirms Safe Harbor & Identifies 13 Recommendations to Strengthen the Arrangement*, PRIVACY & SECURITY L. REP. (Bloomberg BNA), Dec. 16, 2013; Lothar Determann, *International Data Transfers from Europe & Beyond*, 25 REV. BANKING & FIN. SERVICES 125, 132 (2009).

21. U.S.-EU SAFE HARBOR CERTIFICATION WEBSITE, *U.S.-EU Safe Harbor Overview*, http://export.gov/safeharbor/eu/eg_main_018476.asp (last visited Mar. 18, 2014); *Id.* at *U.S.-EU Safe Harbor List,* http://safeharbor.export.gov/list.aspx (last visited Mar. 18, 2014) (listing all U.S. businesses that have voluntarily sought certification from the U.S.-EU Safe Harbor program).

22. Brian Hengesbaugh, Amy de La Lama & Michael Egan, *European Commission Reaffirms Safe Harbor & Identifies 13 Recommendations to Strengthen the Arrangement*, PRIVACY & SECURITY L. REP. (Bloomberg BNA), Dec. 16, 2013, at 2073; James Fontanella-Kahn, *Brussels Considers Option to Respond to NSA Spying Scandal*, FIN. TIMES (Nov. 26, 2013), http://www.ft.com/intl/cms/s/0/6f4bf1a8-470b-11e3-9c1b-00144feabdc0.html#axzz2wH7IOR00.

23. Article 26 of the Treaty on the Functioning of the European Union provides, "The internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisions of the Treaties." Treaty on the Functioning of the European Union, (EN) No. 26 of Oct. 2012, art. 26, 2012 O.J. (C 326) 59. *See* Abboud & Maushagen, *supra* note 13.

24. Karl-Theodor zu Guttenberg, *European Legislators Face "Data Secessionism,"* TECHONOMY EXCLUSIVE (Apr. 1, 2014), http://techonomy.com/2014/04/european-legislators-face-data-secessionism/.

intelligence with the NSA.[25] Sweden, for instance, which seems to have benefited from the NSA fallout in Brazil by winning the fighter jet contract intended for Boeing, passed a law in 2008 allowing its intelligence agency to monitor cross-border email and phone communications without any court order.[26]

Given all this outrage, one may wonder why the NSA and similar agencies around the world gather intelligence in the first place, and whether such programs might be per se illegal.

II. Why Spy?

Most people consider intelligence a good thing. Informed governments can make more cognizant decisions.[27] Foreign intelligence gathering has an ancient and storied history. Called "second-oldest profession," its roots date back thousands of years to military strategists like Sun-Tzu in China and Chanakya in India.[28] Today, most governments gather foreign intelligence by openly sending diplomats and secretly sending spies abroad.[29] Also, due to the globalization of information and communications networks, governments are increasingly able to collect intelligence with fewer agents sent across borders, relying on 'signal intelligence' and cyber espionage.[30]

Regardless of how the means of intelligence gathering evolve, the motivations behind foreign intelligence gathering largely remain the same. The United States Central Intelligence Agency ("CIA"), for example, has a mission to "preempt threats and further U.S. national security objectives by collecting intelligence that matters, producing objective all-source analysis, conducting effective covert action as directed by the President, and safeguarding the secrets that

25. Julian Borger, *GCHQ & European spy agencies worked together on mass surveillance: Edward Snowden papers unmask close technical cooperation and loose alliance between British, German, French, Spanish & Swedish spy agencies*, THE GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden; Hubert Gude, Laura Poitras & Marcel Rosenbach, *Mass Data: Transfers from Germany Aid U.S. Surveillance*, SPIEGEL ONLINE INTERNATIONAL (Aug. 5, 2013), http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

26. Borger, *supra* note 25.

27. *See* John Radsan, *The Unresolved Equation of Espionage and International law*, 28 MICH. J. INT'L L. 595, 613 (2007).

28. Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071, 1072 (2006).

29. John Radsan, *supra* note 27, at 613.

30. *See* Borger, *supra* note 25.

help keep our Nation safe."[31] The NSA's "core missions are to protect U.S. national security systems and to produce foreign signals intelligence information."[32]

Germany has an integrated foreign intelligence service, called the *Bundesnachrichtendienst*, or ("*BND*"), while the German armed forces *Bundeswehr* maintains its own intelligence service, *Amt für den Militärischen Abschirmdienst* ("*MAD*"), which is responsible for military counterintelligence.[33] The *BND* describes its mission as compiling economic, political, and military foreign intelligence on behalf of the German government, operating in secret and clandestine ways, but always in compliance with applicable law and in the interest of Germany's security.[34] The British "Secret Intelligence Service ("SIS"), often known as MI6, collects Britain's foreign intelligence. . . . SIS provides Her Majesty's Government with a global covert capability to promote and defend the national security and economic well-being of the United Kingdom."[35]

Less is known about the foreign intelligence-gathering agencies and activities of countries whose political systems tend to be less transparent. However, the People's Republic of China and Russia, for example, are very active in foreign intelligence gathering—particularly with respect to cyberspying.[36]

So, everybody is doing it—but, is it *legal*?

---

31. CENTRAL INTELLIGENCE AGENCY, https://www.cia.gov (last visited Feb. 21, 2014).

32. NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, https://www.nsa.gov (last visited Feb. 23, 2014).

33. DIE DIENSTSTELLEN DER STREITKRÄFTEBASIS, AMT FÜR DEN MILITÄRISCHEN ABSCHIRMDIENST, http://www.kommando.streitkraeftebasis.de/portal/a/kdoskb/!ut/p/c4/04_SB8K8xLLM9MSSzPy8xBz9CP3I5EyrpHK94uyk-OyUfL3y1MySlOKS4hK93MQU_YJsR0UABos3fg!!/ (last visited Mar. 21, 2014) (Office of Military Counterintelligence website [all text in German]).

34. *See* BUNDESNACHRICHTENDIENST, *arbeitsfelder*, www.bnd.de (last visited Feb. 23, 2014) (German federal intelligence website [all text in German]).

35. SECRET INTELLIGENCE SERVICE M16, https://www.sis.gov.uk/about-us.html (last visited Feb. 23, 2014).

36. In May 2013, the U.S. Department of Defense published a report about Chinese cyber espionage. Ann. Rep. to Cong.: Military & Security Developments Involving China (Sec'y of Defense 2013), http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf. This followed shortly after a report was issued by private security firm Mandiant Corporation, which documented a sustained campaign of cyberattacks against over 100 U.S. companies in twenty industries; every one of these attacks emanated from a run-down office building on the outskirts of Shanghai. *See also* APT1 – Exposing One of China's Cyber Espionage Units, Mandiant (2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. *See also* Radsan, *supra* note 27, at 613.

III. Spying and Punishment of Spies Under International Versus National Law

The legality of government actions can be scrutinized based on international and national laws.

Public international law—the law of nations—governs rights and obligations between countries.[37] Generally, sovereign nations retain the powers of self-governance and do not submit to supranational authorities that can impose laws on them.[38] Instead, public international law is created through contracts between countries (also known as "treaties") and customary international law.[39] Countries create customary international law through consistent practice in recognition of a legal obligation to follow the practice.[40] As a matter of custom, countries have not accepted any meaningful geographical limitations on their own jurisdiction to prescribe laws.[41] Many nations frequently legislate extraterritorially.[42] Still, countries tend to acknowledge that their jurisdiction to execute and adjudicate is generally limited to their own territory.[43]

37. *See* JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 3–4 (8th ed. 2012); LOTHAR DETERMANN, FREEDOM OF COMMUNICATIONS ON THE INTERNET – CIVIL RIGHTS & STATUTORY LIMITATIONS 133–71 (1999) (German with English summary).

38. There are exceptions to this general rule. Many nations submit jurisdiction over specific trade matters to the World Trade Organization. Similarly many countries cede jurisdiction to the International Court of Justice over international human rights matters. Finally, the most striking example of an existing supranational legislative body is the European Union; its twenty-eight member states have ceded jurisdiction in a variety of broadly defined areas. *See* Treaty on the Functioning of the European Union, (EN) No. 26 of Oct. 2012, art. 1, 2012 O.J. (C 326) 47. *See also*, The Council of Europe Cybercrime Convention, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (last visited Apr. 5, 2014); Ian Walden, *Law Enforcement Access to Data in Clouds* (forthcoming, 2014).

39. The Case of the S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7); CRAWFORD, *supra* note 37, at 6.

40. *See* CRAWFORD, *supra* note 37, at 23–24.

41. *See id.* at 456–57 (discussing the move away from the territorial theory of jurisdiction in international law); *id.* at ch. 21 (discussing prescriptive, enforcement, and adjudicative jurisdiction).

42. For example, jurisdiction under conspiracy and antitrust law is often independent from territorial boundaries, as are violations of immigration law. Additionally, many European countries retain jurisdiction over criminal matters if an element of the offense is committed within the state's borders. CRAWFORD, *supra* note 37 at 458–59, nn.15–18. Moreover, many countries have enacted expansive embargoes and extraterritorial trade sanctions laws. Determann, *supra* note 40, at 162.

43. The Permanent Court of International Justice stated in the 1927 Lotus case, "[T]he first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in

As an exception to the general limitation of executive powers to a country's own territory, governments have been sending spies to foreign territories for centuries, and spying has become an accepted practice as a matter of customary public international law.[44] Most countries conduct foreign intelligence programs and spy on each other.[45] In this context, the hyped outrage of some governments in the wake of the NSA revelations does not fall short of a certain irony.

At the same time, most countries have national laws against espionage, treason, and other acts affecting national security, that prohibit foreign surveillance against themselves.[46] International law does not prohibit countries from spying abroad or punishing spies at home.[47]

Spying in cyberspace does not necessarily require intruding on foreign territorial sovereignty by sending agents across borders. Cyberspies typically stay on their home territories. Thus, the impact of remote espionage on territorial sovereignty is less tangible than that of sending covert agents across borders. Given that even sending spies abroad does not violate international law, spying in cyberspace can hardly raise any international law concerns.[48]

Just as the act of sending a spy is typically permissible under the sending nation's domestic laws and illegal under the spied-upon country's domestic laws, intercepting foreign communications and accessing foreign computers is usually strictly prohibited under the

any form in the territory of another State." The Case of the S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

44. Chesterman, *supra* note 28, at 1078, quoting HUGO GROTIUS, DE JURE BELLI AC PACIS LIBRI TRES 655 (Francis W. Kelsey trans., 1925) (1646) (sending spies in war is "beyond doubt permitted by the law of nations"). Only a few countries are known to have entered into treaties regarding spying and hardly any universally relevant rules on spying can be found in treaties: In 1947 the United States and Britain signed the United Kingdom–USA Intelligence Agreement (UKUSA), which was joined by Australia, Canada, and New Zealand in 1948 to form a "five eyes" alliance on intelligence sharing. In the 1970s, the USA and the Soviet Union acknowledged intelligence gathering practices and agreed on limitations regarding counter-intelligence measures. Radsan, *supra* note 27, at 595. *But see, e.g.*, Ingrid Delupis, *Foreign Warships & Immunity for Espionage*, 78 AM J. INTL'L L. 53, 67 (1984).

45. Chesterman, *supra* note 28, at 1072.

46. Radsan, *supra* note 27, at 604.

47. *Id.* at 601.

48. Wolfgang Ewer & Tobias Thiene, *Völker-, unions- und verfassungsrechtliche Aspekte des NSA-Datenskandals*, NEUE JURISTISCHE WOCHENSCHRIFT 30, 32 (2014) (German law journal article).

spied-upon country's domestic laws.[49] But, simply because one country's foreign intelligence gathering programs may violate another country's domestic telecommunications and computer interference laws, this does not mean these programs are illegal under international law or the domestic law of the cyberspying country. Every country's international espionage programs regularly violate other countries' domestic laws.[50]

Equally normal is the fact that a captured spy or traitor can be severely punished as an enemy of the spied-upon state and celebrated as a hero abroad.[51] "Spies are generally condemned to capital punishment, and not unjustly; there being scarcely any other way of preventing the mischief they may do."[52]

This apparent contradiction—allowing one state to send spies abroad and another to kill them—is simply a function of the fact that the spying and spied-upon country's interests are diametrically opposed and no treaty or benevolent supranational legislature has resolved the conflict with a rule of law protecting the individuals in the crossfire.[53] It is no surprise then, that Edward Snowden and Chelsea Manning (born Bradley Manning) are celebrated abroad yet face harsh punishments under United States law. Public sentiment or sympathy in their favor should not be mistaken as proof or even an indication that the U.S. government acted inappropriately by international standards with respect to U.S. intelligence gathering.

49. For example, unauthorized access to computers on U.S. territory is punishable by serious prison terms under the U.S. Computer Fraud & Abuse Act. Lothar Determann, *Internet Freedom & Computer Abuse*, 35 HASTINGS COMM. & ENT. L.J. 429 (2013).

50. Chesterman, *supra* note 28, at 1078, quoting *U.S. Intelligence Agencies & Activities: Risks & Control of Foreign Intelligence*, *Part V*, 94th Cong. 1767 (1975) (Mitchell Rogovin, Special Counsel to CIA Director ("Espionage is nothing but the violation of someone else's laws.")).

51. For definitions and distinctions on "spy" and "traitor," *see* Geoffrey B. Demarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 332 (1996); Radsan, *supra* note 27, at 607.

52. *See* Chesterman, *supra* note 28, at 1078 (*quoting* H. W. HALLECK, INTERNATIONAL LAW; OR, RULES REGULATING THE INTERCOURSE OF STATES IN PEACE & WAR 406 (1st ed. 1861)).

53. *See id.*

IV. Do European Data Protection Laws Offer Protection Against Spying?

Conceptually, yes. Practically, no.[54]

European data protection laws originate from a German data protection law in the state of Hessen that became effective 1970[55] and was intended to protect data privacy against the Orwellian vision of 1984.[56] From the outset, European data protection laws were intended to curtail government surveillance.

In line with European integration, European Union data protection laws have increasingly taken center stage and dwarfed similar national laws. Still, EU law does not impose any meaningful limitations on government surveillance because the EU has limited jurisdiction over the foreign intelligence activities of its member states.[57] Each EU member state maintains its own policies and laws on domestic intelligence gathering, with varying degrees of privacy protection afforded to their own citizens.[58] All have enacted

54. *See* Lothar Determann, *Data Privacy in the Cloud: A Dozen Myths & Facts*, 28 COMPUTER & INTERNET LAW 1, 2 (2011).

55. Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions & Procedures*, 126 HARV. L. REV. 1966, 1969 (2013).

56. LOTHAR DETERMANN, DETERMANN'S FIELD GUIDE TO INTERNATIONAL DATA PRIVACY LAW COMPLIANCE 8 (1st ed. 2012).

57. *See, e.g.*, Treaty on European Union, art. 4, 5, Feb. 7, 1992, O.J. C 191. Article 4.2 provides:

> The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.

Id. at art. 4.2. *See* Armin von Bogdandy & Stephan W. Schill, *Art. 4 EUV*, in E. Grabitz, M. Hilf & M. Nettesheim, DAS RECHT DER EURPÄISCHEN UNION cmt. 34 (1st ed. 2010) (commentary on Article Four of the Treaty on the European Union) (German). The EU has published various declarations relating to the limited cooperation in connection with national security interests. *See, e.g.*, Treaty on the Functioning of the European Union, art. 72, 276, 346, Oct. 26, 2012, O.J. C. 326; *id.* art. 26, PROTOCOL (NO. 21) ON THE POSITION OF THE UK AND IRELAND IN RESPECT OF THE AREA OF FREEDOM, SECURITY AND JUSTICE.

58. *See* Paul Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, 2 INT'L DATA PRIVACY L. 289 (2012), Ian Walden, Law Enforcement Access to Data in Clouds (forthcoming, 2014); *and see* Ian Brown, *Government Access to Private-Sector Data in the United Kingdom*, 2 INT'L DATA PRIVACY L. 230 (2012). *See also* Fred H. Cate, James X. Dempsey & Ira S. Rubinstein, *Systematic Government Access to Private-Sector Data*, 2 INT'L DATA PRIVACY L. 195 (2012); Council of Europe Cybercrime

legislation to protect their own citizens against foreign espionage by other countries, including cyberspying. Yet, states can only enforce these laws within their own territory,[59] which foreign cyberspies do not typically visit. Consequently, European data protection laws and other laws cannot offer meaningful protection from foreign cyberespionage.

While European outrage over a perceived breach of trust is currently directed at the United States generally and the NSA specifically, a more appropriate focus of public scrutiny would be the domestic intelligence services that facilitate the information collection and sharing privacy advocates so denounce. As long as this cooperation remains as it has been, existing proposals to create a more secure method of transmitting electronic communications in Europe will do little to fill the gaps in existing law.

For instance, European politicians have suggested that the "European cloud initiative" will offer more robust privacy protection for their citizens.[60] In reality, data stored and transmitted exclusively on European territory would not be safer from U.S. cyberspying than it is in the United States, given the close cooperation between secret service agencies in the UK (as a member of the so called "Five Eyes" alliance)[61] and other member states with the U.S. government.[62] Also, the United States devotes far greater resources towards military, intelligence, and counter-intelligence activities than European governments[63] and thus, data in a "European cloud" could be more susceptible to cyberspying and other threats than data on U.S. servers.

Convention, http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp (last visited Apr. 5, 2014).

59. The Case of the S.S. "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

60. Danny Hakim, *Europe Aims to Regulate the Cloud,* N.Y. TIMES, Oct. 7, 2013, at B1.

61. This group was originally formed in 1946 to foster joint cooperation between Britain and the United States in radio transmission intelligence gathering during World War II. Today the group is comprised of the United States, the United Kingdom, Australia, New Zealand, and Canada; the three additional countries formally joined the alliance in 1955. This alliance was formed under the United Kingdom–United States of America Communication Agreement of 1946 ("UKUSA"), which continues to be the basis for cooperation between the NSA and the GCHQ. Paul Farrell, *History of 5-Eyes–Explainer*, THE GUARDIAN (Dec. 2, 2013), http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

62. Borger, *supra* note 25; Gude, *supra* note 25.

63. Laicie Heeley, *U.S. Defense Spending vs. Global Defense Spending*, THE CENTER FOR ARMS CONTROL & NON-PROLIFERATION (Apr. 24, 2013), http://armscontrolcenter.org/issues/securityspending/articles/2012_topline_global_defense_spending.

Similarly, the much-hyped (and necessary[64]) EU data protection regulation cannot be expected to address the issue either. It is focused primarily on private sector data processing practices and most drafts continue to carve out EU, EU member states', and foreign surveillance programs.[65] Moreover, reports suggest the regulation may probably not be implemented before 2020.[66]

The ongoing and vocal criticism of the U.S.–EU Safe Harbor program also needs to be put into perspective. The EU and U.S. delegations that negotiated the program specifically agreed at the outset to carve-outs for law enforcement and government data processing.[67] Neither the EU nor individual EU member states seem

64. Current EU data protection law is based on Directive 95/46/EC - from 1995! Council Directive 95/46, 1995 O.J. (L 281) 31 (EC). *See* Guttenberg, *supra*, note 24.

65. *See Commission Proposal for a Regulation of the European Parliament & of the Counsel on the Protection of Individuals with Regard to the Processing of Personal Data & on the Free Movement of Such Data* § 3.4, COM(2012) 11 final (Jan. 1, 2012) (providing a detailed explanation of the proposed regulation). Art. 2(2) defines the contemplated scope of the draft regulation's applicability:

> This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security; (b) by the Union institutions, bodies, offices and agencies; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Id. at 40. The EU Parliament proposed to remove the carve-out but does not seem to contain any Articles specifically geared towards covering surveillance by secret service organizations. *See Inofficial Consolidate Version After Libre Committee Vote Provided by the Rapporeur*, EUR. PARL. & COUNCIL OF THE EU (Oct. 22, 2013), *available at* http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf). *See also* LONDON ECONOMICS, FINAL REPORT TO THE INFORMATION COMMISSIONER'S OFFICE, *Implications of the European Commission's Proposal for a General Data Protection Regulation for Business*, 2013, *available at* http://ico.org.uk/~/media/documents/library/Data_Protection/Research_and_reports/implications-european-commissions-proposal-general-data-protection-regulation-for-business.ashx.

66. Privacy Laws & Business – Data Protection & Privacy Information Worldwide, *Delay with EU DP Draft Regulation – Lack of Political Will or Tricky Technical Issue?* (Jan. 23, 2014), http://www.privacylaws.com/Publications/enews/International-E-news/Dates/2014/1/Delay-with-EU-DP-draft-Regulation—-lack-of-political-will-or-tricky-technical-issues/ (quoting head of the Polish Data Protection Authority, Dr. Wojciech Wiewiorowski, with an assessment that "not having a new framework until 2020, is looking more and more likely"). For a critical assessment, see LONDON ECONOMICS, *supra* note 65.

67. Brian Hengesbaugh, Amy de La Lama & Michael Egan, *European Commission Reaffirms Safe Harbor & Identifies 13 Recommendations to Strengthen the Arrangement*,

able or willing to regulate their own intelligence services in the manner they propose that the NSA be regulated.[68] If privacy advocates amongst European politicians truly want reform, they should first focus on their own country's intelligence gathering and sharing practices and laws. In this context, they will have to make tough choices regarding inevitable trade-offs.[69]

V. Do, Can, Should U.S. Law Offer Protection Against Spying?

For many of the same reasons laid out with respect to European data protection laws, it is unrealistic to expect meaningful legal protection from foreign cyberspying under U.S. law. Like European laws, U.S. law does not impose significant limitations on foreign intelligence gathering by the U.S. government on foreign territory.[70] But, U.S. law can—and is intended to—protect U.S. citizens against domestic spying by their own government.

The Fourth Amendment to the United States Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[71] Federal and state laws further protect electronic communications privacy.[72] If law enforcement officers violate applicable laws or infringe upon an individual's civil liberties, the government cannot use the illegally gathered evidence in a criminal proceeding.[73] Similarly, the fruits of the poisonous tree doctrine bars

PRIVACY & SECURITY L. REP. (Bloomberg BNA), Dec. 16, 2013, at 2073, 2078; Determann, *supra* note 59, at 17.

68. Stewart Baker, *Last Chance to Vote for the 2014 Privies–Plus* Sebelius v. Reding *for Privacy Hypocrite of the Year*, SKATING ON STILTS (Dec. 31, 2013), http://www.skatingonstilts.com/skating-on-stilts/2013/12/last-chance-to-vote-for-the-2014-privies-plus-sebelius-v-reding-for-privacy-hypocrite-of-the-year.html.

69. *See infra.* § 5.A.

70. Radsan, *supra* note 27, at 616.

71. U.S. CONST. amend. IV. *See also* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007).

72. *See, e.g.*, Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2014); Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2014). *See, e.g.*, Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 1–14 (2004) (discussing the Wiretap Act of 1968 and its role in ensuring that electronic surveillance by law enforcement officers is conducted in accord with the law).

73. Weeks v. United States, 232 U.S. 383 (1914) (establishing the Exclusionary Rule as applicable to federal law enforcement officers); Mapp v. Ohio, 367 U.S. 643 (1961) (extending the Exclusionary Rule as binding on the states); U.S. v. Warshak, 631 F.3d 266, 274, 283–89 (6th Cir. 2010) (holding that warrantless government seizure of defendant's email messages during criminal investigation violated his Fourth Amendment rights).

the admission of any evidence gathered as a result of such violations.[74] In the wake of the controversies surrounding NSA programs, some are questioning whether the current laws are sufficient and more importantly, whether they are being observed.[75] A number of possible changes are worth considering.

A. Trading Privacy for Security

The most direct response to outrage over government surveillance would be to demand that governments discontinue or limit surveillance. Privacy advocates are demanding this, and the U.S. government is looking at options to make surveillance operations more targeted.[76] However, at this juncture, we must remember that we still live in a dangerous world. And because few in the United States want to completely give up on security or embrace a total surveillance state, privacy, civil liberties, and security must be balanced to safeguard the nation. There is no guarantee that even *if* the United States limits or stops surveillance, other countries will automatically follow its lead. To the contrary, many are likely trying to bolster their activities in an effort to match the United States. Thus, limiting U.S. surveillance may well reduce the security of people in the United States and its allied countries, increase their exposure to surveillance by other countries, and not increase anyone's net privacy protections. Further, surveillance and privacy discussions cannot remain limited to the public sector, as tech companies increasingly acquire vast amounts of data. In a discussion about the proper balance between these competing interests, we need to be honest about the trade-offs.[77]

74. Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920) (applying the exclusionary rule to "fruits of the poisonous tree," or evidence recovered as the result of a violation of constitutional rights or applicable law).

75. PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 3. U.S. courts are split *Compare* Jewel v. NSA, No. 08-CV-04373, (N.D. Cal. Sept. 18, 2008), *with* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *and* Klayman v. Obama, 957 F. Supp. 2d 1 (D.C. Cir. 2013). *See, e.g.*, Michelle Richardson, *The Nine Things You Should Know About the NSA Recommendations From the President's Review Group*, ACLU FREE FUTURE BLOG (Dec. 20, 2013, 12:00 AM), www.aclu.org/blog/national-security-technology-and-liberty/10-things-you-should-know-about-nsa-recommendations.

76. Richardson, *supra* note 75; PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 3; Bill Blum, *Reining in the NSA*, CALIFORNIA LAWYER (Feb. 2014), at 10, *available at* http://www.callawyer.com/clstory.cfm?eid=933196&wteid=933196_Reining_in_the_NSA.

77. On the trade-offs, *see* Susan Freiwald, *Nothing to Fear or Nowhere to Hide: Competing Visions of the Harm from National Security Surveillance*, COLO. TECH. L.J. (forthcoming 2014).

B. Transparent Espionage

Some commentators suggest that increased government transparency should be the basis of further discussion and cost-benefit analyses regarding intelligence-gathering program reform.[78] The probability of achieving this goal seems limited given the potential adverse impact transparency could have on successful intelligence gathering and on diplomatic relations among nations, due to the sensitive nature of intelligence gathering. While transparency is easier to communicate from a political standpoint, it bears the risk of populism. Instead, a turn in the opposite direction may be more promising. Secret services should be kept more secret.

C. Keeping Secret Services More Secret

To a large degree, the foreign government outrage in the wake of disclosures like Snowden's appear to be stirred up by embarrassment rather than genuine surprise or concern of the surveillance itself. Similarly, ordinary citizens would likely be less concerned by foreign intelligence gathering if the information were kept secret, safe, and secure. It is alarming that the United States government has been unable to keep the massive amounts of sensitive information it collects secure and secret.

Manning, a low-level intelligence analyst in the U.S. Army,[79] and Snowden, a civilian computer technician at a private government contractor leaked Top Secret information to the media for publication.[80] If any one of their thousands of colleagues have been secretly revealing information to foreign governments, companies, or others, for financial gain or otherwise, there is cause for serious concern for individual and national security, as well as for individual privacy.

In recent years, the United States government has outsourced an increasing portion of intelligence gathering and analysis duties to private corporations.[81] The practice of outsourcing national security has been the subject of criticism and many are skeptical about the

78. Richardson, *supra* note 75; PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 3, at 18.

79. Charlie Savage & Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, N.Y. TIMES, Aug. 21, 2013, at A1.

80. Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES, June 9, 2013, at A1.

81. R.J. Hillhouse, *Outsourcing Intelligence*, THE NATION (July 30, 2007), http://www.thenation.com/article/outsourcing-intelligence#.

security risks associated with such an approach.[82] The security of information stored in the NSA's new data centers has also been publicly questioned.[83] The fact that since the terrorist attacks of September 11, 2001, the U.S. government has increased spending on intelligence while simultaneously issuing significant cutbacks in government agencies, raises concerns regarding increased security risks created by the security services' insufficiently secure data handling practices.[84]

Proponents of intelligence outsourcing point out that security clearance requirements remain the same in the private sectors as they are in NSA- and CIA-operated facilities.[85] At the same time, computers, networks, and other technology operated by intelligence agencies have repeatedly fallen victim to insider leaks and hacks by outsiders, exposing the vulnerability of internally managed government systems.[86] Better data security measures and restrictions on use and access are needed[87] to ensure that secure intelligence and surveillance information is properly protected, but it is not clear whether insourcing or outsourcing is the right answer.

D. Fences in Cyberspace

Under U.S. law, the CIA is supposed to be focused on *foreign* intelligence gathering, whereas the FBI the Department of Homeland Security and law enforcement authorities are tasked with *domestic* security.[88] Increasingly however, the concepts of "foreign" and

82. *Id.* (identifying potential vulnerabilities created by outsourcing intelligence to private corporations); Robert O'Harrow, Jr., *The Outsourcing of U.S. Intelligence Raises Risks Among Benefits*, WASH. POST (June 9, 2013), http://www.washingtonpost.com/world/national-security/the-outsourcing-of-us-intelligence-raises-risks-among-the-benefits/2013/06/09/eba2\d314-d14c-11e2-9f1a-1a7cdee20287_story.html (suggesting that increased access to top-secret intelligence information increases the risk of national security leaks); Tim Shorrock, Op-Ed, *Put the Spies Back Under One Roof*, N.Y. TIMES, June 17, 2013, at A25; N.Y. Times Editorial Board, *Prying Private Eyes*, June 20, 2013, at A26; Simon Chesterman, *'We Can't Spy . . . If We Can't Buy!': The Privatization of Intelligence & the Limits of Outsourcing 'Inherently Governmental Functions'*, 19 THE EUR. J. INT'L L. 1055 (2008).

83. *See, e.g.*, Richardson, *supra* note 75. THE NSA UNCHAINED, https://www.aclu.org/files/pages/fisainfographic3.pdf (last visited March 21, 2014).

84. O'Harrow, Jr., *supra* note 82.

85. Binyamin Appelbaum & Eric Lipton, *Leaker's Employer is Paid to Maintain Government Secrets*, N.Y. TIMES, June 9, 2013, at A12.

86. O'Harrow, Jr., *supra* note 82.

87. Lothar Determann & Jesse Hwang, *Data Security Requirements Evolve: From Reasonableness to Specifics*, 26 COMPUTER & INTERNET LAW. 6, 7 (2009).

88. Radsan, *supra* note 27, at 612. On its home page, the CIA states that the "CIA's primary mission is to collect, analyze, evaluate, and disseminate foreign intelligence to

"domestic" are both meaningless and impossible to separate within cyberspace and within our globalized economy and information society. The Internet was conceived to be borderless and global from the outset.[89] An email sent to a neighbor across the street could be routed through foreign countries. Thus, any attempt to define or uphold geographical borders in Cyberspace are futile.[90] U.S. citizens would not enjoy more privacy if the NSA moved its surveillance equipment abroad to honor the current statutory distinction between surveillance on domestic versus foreign territory. Conversely, German citizens would not be better protected if they limited themselves to a "Germany-only Internet" while the German secret service continues its surveillance activities and sharing. Besides, more and more emails and other communications must be sent abroad due to necessities in today's global economy. In addition, any fragmentation into "parallel internets" would lead to enormous opportunity costs for the private and public sector.

E. Walls Between Defense and Law Enforcement

While public support for NSA surveillance programs continues to wane,[91] most U.S. citizens accept the idea that some form of government surveillance is necessary in thwarting terrorism, provided that meaningful limits are placed on programs to protect individual civil liberties.[92] Most notably these limits include restriction on information and evidence sharing between intelligence agencies and law enforcement agencies.

In recent history, information sharing between federal intelligence agents and federal law enforcement officers was limited.[93]

---

assist the President and senior US government policymakers in making decisions relating to national security." https://www.cia.gov/about-cia/todays-cia/what-we-do (last visited Apr. 5, 2014).

89. *See* Barry M. Leiner et al., *Brief History of the Internet*, INTERNET SOCIETY, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#JCRL62 (last visited Mar. 17, 2014).

90. DETERMANN, *supra* note 37, at 41–44, 170–71.

91. Susan Page, *Poll: Most Americans now Oppose the NSA Program*, USA TODAY (Jan. 20, 2014), http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/.

92. Pew Research Center for the People & the Press, *Few See Adequate Limits on NSA Surveillance Program: But More Approve than Disapprove* (July 26, 2013), *available at* http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/.

93. Michael P. Robotti, *Grasping the Pendulum: Coordination Between Law Enforcement & Intelligence Officer Within The Department of Justice in a Post-"Wall" Era*, 64 N.Y.U. ANN. SURV. AM. L. 751, 776 (2009).

A proverbial wall between federal agencies was erected under the Foreign Intelligence Surveillance Act ("FISA")—a U.S. statute that prescribes the ways in which physical and electronic foreign intelligence gathering and surveillance efforts are conducted.[94] Law enforcement agencies restricted information sharing due to concerns that evidence resulting from data collection for intelligence purposes could be tainted and thus, inadmissible in criminal proceedings.[95]

Many within the United States Department of Justice ("DOJ") expressed frustration when their investigations were thwarted by the presence of what became known as the "FISA wall."[96] Perhaps the most striking example of the negative impact of the FISA wall can be seen in the 2004 DOJ report, "A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks."[97]

The wall was specifically cited as one factor that hindered the FBI's ability to prevent the September 11 attacks.[98] In the months leading up to the attacks, FBI criminal investigators and intelligence agents were focused on a number of the same targets.[99] In August of 2001, intelligence agents were aware that three suspected terrorists—two of whom ultimately participated in the September 11 attacks—had entered the United States.[100] Intelligence operatives opened an intelligence investigation but did not share surveillance information with criminal investigators for fear of violating the wall procedures.[101]

---

94. *See* 50 U.S.C. §§ 1801–1812 (2014).

95. *See* Robotti, *supra* note 96, at 764–66.

96. In a 2006 opinion piece in the Wall Street Journal, Victoria Toensing, a Deputy Assistant Attorney General related her experience working for the DOJ while the wall was in place:

> I experienced the pain of terminating a FISA wiretap when to do defied common sense and thwarted the possibility of gaining information about American hostages. [During the TWA 847 hijacking] [w]e had a previously placed tap in the U.S. and thought there was a possibility we could learn the hostages' location. But [DOJ] career lawyers told me that the FISA statute defined its 'primary purpose' as foreign intelligence gathering. Because crimes were taking place, the FBI had to shut down the wire.

Victoria Toensing, Opinion, *Terrorists on Tap*, WALL ST. J., Jan. 22, 2006, at A14, *available at* http://online.wsj.com/news/articles/SB113763551855150439.

97. Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks 21 (2004), *available at* http://www.fas.org/irp/agency/doj/oig/fbi-911/ [hereinafter DOJ 9/11 Report].

98. *Id*. at 21.

99. *Id.* at 223–25.

100. *Id*. at 349.

101. *Id*. at 350.

The FBI's criminal investigation went unresolved and just one month later the September 11 terrorist attacks were carried out.[102]

In the wake of these revelations and the publication of the 9/11 Commission Report, efforts to tear down the wall intensified.[103] In 2002, the government brought a case before the Foreign Intelligence Surveillance Court of Review ("FISCR") challenging the wall.[104] FISCR had never before been convened.[105] FISCR held that FISA allows coordination between intelligence and law enforcement officers, so long as the primary purpose of communication is to obtain evidence to prosecute foreign spies or terrorists.[106]

Revelations during the past year, however, suggest that such communications are in fact used to prosecute U.S. citizens for crimes unrelated to espionage: The FBI routinely receives information from the NSA, and so do other domestic law enforcement agencies.[107] In August 2013, a special report by Reuters uncovered a secret unit within the U.S. Drug Enforcement Agency known as the Special Operations Division ("SOD").[108] Comprised of representatives from approximately twenty-five partner agencies, including the FBI, CIA, NSA, IRS, and Homeland Security, the SOD allegedly funnels information from intelligence intercepts, wiretaps, informants, and a massive database of telephone records to authorities across the nation to aid criminal investigations of U.S. citizens.[109]

In an internal document obtained by Reuters, agents are instructed to use "normal investigative techniques to recreate the information provided by SOD" and to specifically omit any mention of the SOD in investigative reports, affidavits, discussions with prosecutors and courtroom testimony.[110] In a subsequent revelation in October 2013, the *New York Times* reported that DEA officials had routine access to an enormous AT&T database containing

102. *Id*.

103. Radsan, *supra* note 27, at 612.

104. Robotti, *supra* note 96, at 789.

105. DOJ 9/11 Report, *supra* note 97, at 350.

106. *Id*. at 790.

107. Stewart Baker, *Breaking News from August 2013: NSA Is Providing 2–3 Tips a Day to the FBI?*, SKATING ON STILTS (Jan. 21, 2014), http://www.skatingonstilts.com/ skating-on-stilts/2014/01/breaking-news-from-august-2013-nsa-is-providing-2-3-tips-a-day-to-the-fbi .html.

108. John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), http://www.reuters.com/ article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

109. *Id.*

110. *Id.*

information on every call passing through an AT&T switch in the last twenty-six years. "The scale and longevity of the data storage appears to be unmatched by other government programs, including the NSA's gathering of phone call logs under the Patriot Act."[111] These reports raise concerns regarding disturbing abridgements of the Fourth and Fifth Amendments to the U.S. Constitution. A careful look at the wall is warranted.

Re-erecting the wall could have adverse impacts on security. Yet, it may be one of the few practical ways with a decent chance of success to protect U.S. citizens' civil liberties against one of the primary threats to their privacy: namely, the concern that illegally obtained evidence may be used to prosecute government critics or otherwise disfavored persons for minor offenses.[112]

To be effective, the rules regarding the wall need to be simple and enforced primarily through audits and supervision of law enforcement authorities, which tend to be more susceptible to supervision than the intelligence agencies. A pragmatic solution to the inherent problems in re-erecting the wall could be to include an enumerated short list of offenses that warrant information sharing "through the wall." Like any other statute, such a law would ultimately be subject to scrutiny under the Fourth Amendment. Therefore, the statute must be carefully and narrowly designed, for example, by providing that only if U.S. intelligence agents intercept information that indicates a massive and immediate threat to domestic security, in the form of mass murder or deployment of weapons of mass destruction, the intelligence agents could share information with the FBI or other law enforcement agencies as necessary to prevent the harm or punish the murderers. Intercepted information pertaining to drug dealing operations, money laundering and tax evasion, however, would not be included on such a list and thus, could not be shared with law enforcement. This approach could allow the NSA to continue pursuing information gathering programs, while imposing limitations on the use of intelligence for law enforcement purposes. This would provide protection for civil liberties, while preserving the government's ability to protect national

111. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. TIMES, Sept. 2, 2013, at A1.

112. Radsan, *supra* note 27, at 612 ("What we fear is something far worse than Richard Nixon's "enemies list" of those who were to receive extra attention from the Internal Revenue Service. We fear the dirtiest tricks." *Id.*); Blum, *supra* note 79, at 16 (referring to "widespread unauthorized wiretapping and other illegal activity committed by the FBI as part of its Cointelpro campaign, intended to disrupt left-wing political groups").

security in situations where threats of mass destruction and murder are imminent.

F. Borders Between War Powers and Civil Liberties in Peace

Since the terrorist attacks of September 11, 2001, the U.S. government has been suggesting to its citizens that the country is in a constant state of war.[113] War powers have been invoked against terrorists and other perceived threats to national security.[114] The U.S. has engaged in various semi-official wars and carried out drone strikes killing U.S. citizens without trials, warrants, or other judicial proceedings.[115] In a classified memo that was leaked in February 2013, the U.S. Department of Justice approves killings by drone strikes in cases of "imminent threats," explaining that "[t]he condition that an operational leader present an 'imminent' threat of violent attack against the United States does not require the United States to have clear evidence that a specific attack on U.S. persons and interests will take place in the immediate future."[116] This seems difficult to reconcile with the U.S. Constitution's Due Process Clause,

113. *See* President George W. Bush, Address to a Joint Session of Congress & the Nation (Sept. 20, 2001) full text *available at* WASHINGTONPOST.COM, http://www.washingtonpost.com/wp-srv/nation/specials/attacked/transcripts/bushaddress_ 092001.html (last visited Mar. 22, 2014); Letter from Barack Obama, U.S. President, to John Boehner, Speaker of the House of Representatives, (Sept. 28, 2012) full text with attachments *available at* WHITEHOUSE.GOV, http://www.whitehouse.gov/sites/default/files/omb/assets/budget_amendments/oco_designation_09282012.pdf (last visited Mar. 22, 2014). *See* Michael Hirsh & James Oliphant, *Obama Will Never End the War on Terror*, NATIONAL JOURNAL (Feb. 27, 2014), http://www.nationaljournal.com/magazine/obama-will-never-end-the-war-on-terror-20140227; John O'Rourke, *The World, Post 9/11 BU Faculty & Staff on What's Changed in Decade Since,* BU TODAY (Sept. 2011), http://www.bu.edu/bostonia/web/post-9-11/. U.S. presidents have used the term "war " loosely for decades. *See, e.g.*, *A Brief History of the Drug War,* DRUG POLICY ALLIANCE (last visited Apr. 2, 2014), www.drugpolicy.org/new-solutions-drug-policy/brief-history-drug-war (discussing the "war on drugs"); *Obama War on Poverty*, HUFFINGTON POST (last visited Apr. 2, 2014), www.huffingtonpost.com/tag/obama-war-on-poverty (compilation of articles regarding the "war on poverty"); Dave Gilson, *109 Things Obama Has Declared War On*, MOTHER JONES (Feb. 8, 2012), www.motherjones.com/mixed-media/2012/02/obama-war-xmas-christians-cheerios (listing various other ideological wars).

114. Louis Fisher, *Judicial Review of the War Power*, 35 PRES. STUD. Q. 446, 492 (2005).

115. Mark Mazzetti & Eric Schmitt, *U.S. Debates Drone Strike on American Terrorism Suspect in Pakistan*, N.Y. TIMES, Feb. 10, 2014, at A1.

116. Michael Isikoff, *Justice Department memo reveals legal case for drone strikes against Americans*, NBC NEWS (Feb. 4, 2014), http://investigations.nbcnews.com/_news/2013/02/04/16843014-justice-department-memo-reveals-legal-case-for-drone-strikes-on-americans?lite&preview=true.

which states that no person shall "be deprived of life, liberty, or property, without due process of law."[117]

The limitations on government powers and processes in war versus peace must be updated to respond to a new threat landscape where security risks emanate more from non-state actors, and less from national governments. At the same time, government war powers need to remain confined to situations of war-like imminent threats. This is indispensable to preserve civil liberties.[118]

G. Privacy Officers for Spies

Under various data privacy laws, organizations are required to appoint an internal or external data protection officer, an "ombudsman," who is tasked with monitoring the organization's compliance with data privacy laws.[119] In the wake of 9/11, the U.S. government recognized the need to create an oversight role focused specifically on government surveillance programs. To that end, the Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent, bipartisan agency, was established to analyze and review actions the executive branch takes to protect the United States from terrorism.[120] The goal is to ensure that the need for such actions is balanced with the need to protect privacy and civil liberties, and to ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to national security and anti-terrorism efforts.[121] The PCLOB recently published a report on the two NSA programs revealed by Snowden and found them largely illegal.[122] Moreover, the PCLOB suggested the involvement of special privacy advocates in court proceedings about foreign intelligence programs.[123] In January 2013, the NSA appointed their first Civil Liberties and Privacy Officer,

117. U.S. CONST. amend. V; U.S. CONST. amend. XIV.

118. Fisher, *supra* note 114, at 482, 496; Mazzetti *supra* note 115, at A1. *See* Declan McCullagh, *Why Liberty Duffers in Wartime*, WIRED (Sept. 24, 2001), http://www.wired.com/politics/law/news/2001/09/47051?currentPage=all; Rachel Maddow, DRIFT (Crown Publishers, 1st ed. 2012); GENE HEALY, THE CULT OF THE AMERICAN PRESIDENCY (Cato Institute, 1st ed. 2008).

119. Lothar Determann & Christoph Rittweger, *German Data Protection Officers & Global Privacy Chiefs*, PRIVACY & SECURITY L. REP. 1 (Bloomberg BNA), April 2011, 1.

120. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 3. *See also* 42 U.S.C. § 2000ee (2014).

121. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 3.

122. *Id.*

123. *Id.* at 14.

whose job will be "to directly enhance decision making and to ensure that civil liberties and privacy protections continue to be baked into NSA's future operations, technologies, tradecraft, and policies."[124]

H. Defend or Adjust Privacy Expectations

In the wake of the recent NSA disclosures, privacy advocates have characterized government surveillance programs as an intrusion on individual privacy and a breach of public trust. Yet anyone who takes a close, honest look at the situation will see the NSA is hardly to blame for Scott McNealy's assessment in 1999 that you have "zero privacy" on the Internet.[125]

Any discussion about reforming intelligence collection in the twenty-first century will need to account for the exponential surge in influence and resources being accumulated by the private sector.[126] Companies have an unprecedented ability to gather, store, aggregate, and analyze vast amounts of personal data. This shift in power raises questions regarding what supposedly inherent government functions will remain strictly within the public domain, including intelligence collection. Companies and governments will need to find ways to maintain public trust in the world of big data and disruptive innovation, as well as develop a new social contract between themselves and their constituents.[127]

It would be shortsighted, however, to blame companies that are caught between shareholder mandates, consumer preferences, privacy laws, and government requests for access to data. As consumers, we must reconsider our privacy expectations and relative priorities. While we enjoy free "all-you-can-eat" online services (with cookies), we cannot reasonably expect, or demand, that law enforcement and intelligence agencies stay out of cyberspace.

Web 2.0 creates familiarity and strong social interactions that many missed in the first generation Internet. Online, we are

124. Al Kamen, *The NSA has a new, first time ever, privacy officer*, WASH. POST (Jan. 28, 2014), http://www.washingtonpost.com/blogs/in-the-loop/wp/2014/01/28/the-nsa-has-a-new-first-time-ever-privacy-officer/.

125. Polly Sprenger, *Sun on Privacy: 'Get Over It'*, WIRED NEWS (Jan. 26, 1999), http://www. http://archive.wired.com/politics/law/news/1999/01/17538 (quoting the CEO of Sun Microsystems, "You have zero privacy anyway . . . Get over it."); Helen A. S. Popkin, *Privacy is Dead on Facebook. Get Over It.*, MSNBC (Jan. 13, 2010), http://www.nbcnews.com/id/34825225/ns/technology_and_science-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.Uz8AAq1dWfV.

126. Guttenberg, *supra* note 5.

127. *Id.*

becoming accustomed to merchants who know us like the village shopkeeper knew our grandparents. Companies create elaborate user profiles to customize searches, services, information, and advertisements.[128] As we engage with these services, expand our online lives, and share personal information in cyberspace, we need protection from fraudsters, hackers, identity thieves, and terrorists.[129] In essence, we need the same security and government protection online as we do offline.[130]

Just as we need protection online, we want privacy. But, how much? Many leading providers tell us—in their service terms, privacy policies, and in court—that we should not hold privacy expectations.[131] When we use "free" (that is, advertising-funded) online services, including email and social media accounts, we routinely consent that providers may use and share our personal information "as permitted by applicable law."[132] Also, employees accept intrusive monitoring and surveillance by employers on a regular basis, particularly in the United States.[133] When we agree to waive privacy rights and expectations, we act more like shouting information in a crowded market place than whispering behind closed doors at home—and government officials may be justified if they view such online

128. Lothar Determann, *Social Media @ Work 2014*, PRIVACY & SECURITY L. REP. 1–2 (Bloomberg BNA), Dec. 17, 2013.

129. Lothar Determann, *Social Media Privacy – 12 Myths & Facts*, 2012 STAN. TECH. L. REV. 7, 1, 8 (2012).

130. Determann, *supra* note 49, at 429.

131. Braden Goyette, *Google: Email Users Can't Legitimately Expect Privacy When Emailing Someone On Gmail*, HUFFINGTON POST (Aug. 13, 2013), http://www.huffingtonpost.com/2013/08/13/gmail-privacy_n_3751971.html.

132. *See* Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy & Data Control in Cloud Computing: Consumers, Privacy Preferences & Market Efficiency*, 70 WASH & LEE L. REV. 341, 414–16 (2013); Aditi A. Prabhu, *Contracting for Financial Privacy: The Rights of Banks & Customers Under the Reauthorized Patriot Act*, 39 LOY. U. CHI. L.J. 51, 84 (2007). Some companies are strengthening commitments to guard consumer privacy in response to criticism and perceived market preferences while others are moving in the opposite direction. *See* WHO HAS YOUR BACK? 2013 ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/who-has-your-back-2013 (last visited Mar. 24, 2014). *But see* Andy Greenberg, *The World's Worst Privacy Policy*, FORBES (Jan. 25, 2012), www.forbes.com/sites/andygreenberg/2012/01/25/the-worlds-worst-privacy-policy/, *and* Mike Masnick, *To Read All Of The Privacy Policies You Encounter, You'd Need To Take A Month Off From Work Each Year*, TECHDIRT (Apr. 23, 2012), www.techdirt.com/articles/20120420/10560418585/to-read-all-privacy-policies-you-encounter-youd-need-to-take-month-off-work-each-year.shtml.

133. Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1016 (2011).

communications like discussions in public spaces or evidence in plain view.[134]

In the United States, telephone users have never enjoyed much privacy protection with respect to phone connection information (e.g., who talked to whom, and when).[135] Thus, it might not have occurred to NSA officials that email users should have much higher privacy expectations in email metadata (who emailed whom, and when), particularly given the prevalence of service terms that disclaim privacy expectations.[136]

If consumers value their privacy and demand that it be respected, the market can be expected to respond with paid online services that promise increased security. In turn, government officials may then have to treat private online communications more like confidential speech in the sanctity of one's home.

Privacy advocates continue to press the issue. In 2011, a consumer watchdog group sent mimes to Capitol Hill to illustrate to U.S. politicians how online tracking could compare to surveillance offline.[137] Online tracking has not stopped, however, and consumers seem to accept it more readily.[138] As long as this trend continues, government agencies will see little reason for self-restraint and will continue to freely gather intelligence and evidence in cyberspace, in war and peace.

134. *See* Robert C. Power, *Criminal Law: Technology & the Fourth Amendment: A Proposed Formulation for Visual Searches*, 80 J. CRIM. L. & CRIMINOLOGY 1, 93 (1989) (on the impact of privacy notices and new technologies on privacy expectations and 4th amendment protection).

135. *See* Susan Freiwald, *Uncertain Privacy: Communication Attribute After The Digital Telephony Act*, 69 S. CALIF. L. REV. 949, 950 (1996), *see also* Smith v. Maryland, 442 U.S. 735 (1979).

136. *See In re* Application of Fed. Bureau of Investigations for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573 (Foreign Intelligence Surveillance Court Aug. 29, 2013).

137. In 2011, a consumer watchdog group sent mimes to Capitol Hill to illustrate to U.S. politicians how online tracking could compare to surveillance offline. Greg Sandoval, *Mimes Aren't Silent in Capitol Hill Attack on Google. Consumer Watchdog Dispatches a Group of mimes to Playfully Spy on Government Workers to Illustrate What They Say is Google's Antiprivacy Behavior*, CNET (Sept. 21, 2011), http://news.cnet.com/8301-31001_3-20109685-261/mimes-arent-silent-in-capitol-hill-attack-on-google/.

138. *See* Elizabeth Dwoskin, Yahoo Won't Honor 'Do Not Track' Requests From Users, WALL ST. J. (May 5, 2014), http://blogs.wsj.com/digits/2014/05/02/yahoo-wont-honor-do-not-track-requests-from-users/; Determann, *supra* note 129, at 1, 13.

VI. *Quo Vadis*, NSA, War and Peace in Cyberspace?

In conclusion, it seems the NSA does not break any international law by operating the massive surveillance programs that Edward Snowden revealed. No treaties or customary international law have developed to impose meaningful limitations on spying. Countries routinely spy on each other in war and peace, in embassies, in covert operations, and in cyberspace.

The NSA is probably violating myriad foreign countries' laws, because all countries prohibit foreign spying against themselves. Yet, this hardly justifies the current outrage abroad. The complaining countries are running similar programs. Moreover, many actually actively collaborate with the NSA and other U.S. authorities in the interest of getting help to protect their own national security. Threats to suspend free trade negotiations, individual cross-border transactions, or cooperative programs like SWIFT or the U.S.–EU Safe Harbor program have counterproductive effects for national security and privacy. Proposals to nationalize or regionalize email, the Internet, or cloud computing are technologically impractical and would be ineffective so long as the various national secret services collaborate and share information.

EU data protection law does not and cannot protect EU residents any better from foreign cybersurveillance than U.S. law can (or does). The great hopes that European politicians are publicly placing on the EU data protection regulation in this respect are misplaced not only because current drafts of the regulation do not even try to regulate surveillance for national security purposes, but also because each country's laws can only offer meaningful protection from its own government agencies. That is where those who want reform should focus—and consider the trade-offs.

Assessing the trade-offs is not a simple task, because much is and will remain unknown regarding the effects and effectiveness of surveillance programs, and because there is hardly any evidence supporting simple correlations like "less surveillance means more privacy." Most assume that less government surveillance, intelligence gathering and law enforcement may result in less security. But, less government surveillance, intelligence gathering and law enforcement could also result in a loss of net privacy if one takes into account the fact that surveillance by foreign governments and cybercriminals will increase. Less surveillance does not automatically result in more privacy. Conversely, more surveillance does not automatically

guarantee more security—as recent security breaches and data leaks demonstrate.

Security interests and civil liberties must be carefully balanced. In this context, it is worth noting that to date the public has been largely embracing or tolerating charge-free online services, big data, and tracking; evidence is the rampant success of Web 2.0, social media, and the Internet of Things. Consumers and employees agree every day to share massive amounts of personal data via various forms of tracking and surveillance technologies with companies that notify consumers and employees they should not expect privacy. In such open, limited-privacy segments of cyberspace, the government seems justified to emphasize security and patrol virtual worlds like city roads and public places. If and when individuals take steps to protect their privacy online to similar degrees as traditionally in the sanctity of their homes—for example, with paid, secure services—the government may become more pressed to respect this and give privacy a greater weight in the balancing act with security interests.

Trying to differentiate between foreign and domestic spying in cyberspace seems impractical, given the technological and social realities in today's connected global world. Even differentiating between war and peacetime has become difficult lately. Reform in this regard seems necessary to re-establish the boundaries of the rules of engagement for cyberintelligence gathering based upon war powers. In the meantime, more easily achievable goals could be to (1) focus on enhancing the government's data security measures to reduce data leaks, security concerns, and diplomatic tensions caused by public embarrassment; (2) bolster procedural and organizational safeguards at government agencies tasked with surveillance, as with the recent appointment of a privacy officer at the NSA; (3) redraw the rules for cooperation between intelligence and law enforcement agencies, permitting information sharing only in clearly enumerated cases of extreme and immediate threats to national security; and (4) closely monitor law enforcement agencies' compliance with data privacy laws—while accepting that spies will be spies in war and peace and cyberspace.