2014

Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?: Hearing Before the Subcomm. On Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce, 113th Cong., Sept. 17, 2014 (Statement of Laura K. Donohue)

Laura K. Donohue
Georgetown University Law, lkd27@georgetown.edu

HIGH TECHNOLOGY, CONSUMER PRIVACY, AND U.S. NATIONAL SECURITY

Professor Laura K. Donohue, J.D., Ph.D.*

Written Remarks
Prepared for the U.S. House of Representatives
Committee on Energy and Commerce,
Subcommittee on Commerce, Manufacturing, and Trade
" Cross border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?"
Sept. 17, 2014

I. INTRODUCTION

Documents released over the past year detailing the National Security Agency's telephony metadata collection program and interception of international content under the Foreign Intelligence Surveillance Act (FISA) directly implicated U.S. high technology companies in government surveillance.[1] The result was an immediate, and detrimental, impact on U.S. firms, the economy, and U.S. national security.

The first Snowden documents, printed June 5, 2013, revealed that the U.S. government had served orders on Verizon, directing the company to turn over telephony metadata under Section 215 of the USA PATRIOT Act.[2] The following day, *The Guardian* published classified slides detailing how the NSA had intercepted international content under Section 702 of the FISA Amendments Act.[3] The type of information obtained ranged from E-mail, video and voice chat, videos, photos, and stored data, to Voice over Internet Protocol, file transfers, video conferencing, notifications of target activity, and online social networking details.[4] The companies

---

* Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law.

[1] *See, e.g.*, Glenn Greenwald and Ewen MacAskill, *NSA Taps into Internet Giants' Systems to Mine User Data, Secret Files Reveal*, THE GUARDIAN (London), June 6, 2013; Barton Gellman and Laura Poitras, *U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013; Glenn Greenwald, *NSA collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (London), June 6, 2013; Glenn Greenwald, *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN, Jul. 11, 2013, *available at* http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data; *NSA Taps Yahoo, Google Links*, WASH. POST, Oct. 31, 2013. For statutory and constitutional analysis of the telephony metadata program and the interception of international content, *see* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37(3) HARV. J. OF L. & PUB. POL'Y, 757-900 (2014), *available at* http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2360&context=facpub; *Section 702 and the collection of International Telephone and Internet Content*, 38(1) HARV. J. OF L. & PUB. POL'Y, (2015), *available at* http://scholarship.law.georgetown.edu/facpub/1355/.

[2] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[3] Glenn Greenwald and Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google, and Others*, THE GUARDIAN, June 6, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/us-tech- giants-nsa-data.

[4] *Id.*

involved read like a who's who of U.S. Internet giants: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.[5]

More articles highlighting the extent to which the NSA had become embedded in the U.S. high tech industry followed. In September 2013 ProPublica and the *New York Times* revealed that the NSA had enjoyed considerable success in cracking commonly-used cryptography.[6] The following month the *Washington Post* reported that the NSA, without the consent of the companies involved, had obtained millions of customers' address book data: in one day alone, some 444,743 email addresses from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail, and 22,881 from other providers.[7] The extent of upstream collection stunned the public – as did slides demonstrating how the NSA had bypassed the companies' encryption, intercepting data as it transferred between the public Internet and the Google cloud.[8]

Further documents suggested that the NSA had helped to promote encryption standards for which it already held the key or whose vulnerabilities the NSA understood but not taken steps to address.[9] Beyond this, press reports indicated that the NSA had at times posed as U.S. companies—without their knowledge—in order to gain access to foreign targets. In November 2013 *Der Spiegel* reported that the NSA and the United Kingdom's Government Communications Headquarters (GCHQ) had created bogus versions of Slashdot and LinkedIn, so that when employees from the telecommunications firm Belgacom tried to access the sites from corporate computers, their requests were diverted to the replica sites that then injected malware into their machines.[10]

As a result of growing public awareness of these programs, U.S. companies have lost revenues, even as non-U.S. firms have benefited.[11] In addition, numerous

---

[5] *Id.*

[6] Nicole Perlroth, Jeff Larson, and Scott Shane, *NSA Able to Foil Basic Safeguards of Privacy on Web*, N. Y. TIMES, Sept. 5, 2013, available at http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0.

[7] Barton Gellman and Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST, Oct. 14, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

[8] Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 30, 2013, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[9] James Ball, Julian Borger, and Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN, Sept. 5, 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[10] Steven Levy, *How the US Almost Killed the Internet*, WIRED, Jan. 7, 2014, *available at* http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.

[11] *See, e.g.*, Sam Gustin, *NSA Spying Scandal Could Cost U.S. Tech Giants Billions*, TIME, Dec. 10, 2013, available at http://business.time.com/2013/12/10/nsa-spying-scandal-could-cost-u-s-tech-giants-billions/. ("The National Security Agency spying scandal could cost the top U.S. tech companies billions of dollars over the next several years, according to industry experts. In addition to consumer Internet companies, hardware and cloud-storage giants like IBM, Hewlett-Packard, and Oracle could suffer billions of dollars in losses."); Ellen Messmer, *U.S. High-Tech Industry feeling the Heat from Edward Snowden Leaks*, NETWORKWORLD, Jul. 19, 2013 ("The disclosures about the National Security Agency's massive global surveillance by Edward Snowden, the former information-technology contractor who's now wanted by the U.S. government for treason, is hitting the U.S. high-tech industry hard as it tries to explain its involvement in the NSA data-collection program."); Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N. Y. TIMES, Mar. 21, 2014, *available at* http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0 (writing, "Despite the tech companies' assertions that they provide information on

countries, concerned about consumer privacy as well as the penetration of U.S. surveillance efforts in the political sphere, have accelerated localization initiatives, begun restricting U.S. companies' access to local markets, and introduced new privacy protections—with implications for the future of Internet governance and U.S. economic growth. These effects raise attendant concerns about U.S. national security.

Congress has an opportunity to redress the current situation in at least three ways. First, and most importantly, reform of the Foreign Intelligence Surveillance Act would provide for greater restrictions on NSA surveillance. Second, new domestic legislation could extend better protections to consumer privacy. These shifts would allow U.S. industry legitimately to claim a change in circumstance, which would help them to gain competitive ground. Third, the integration of economic concerns at a programmatic level within the national security infrastructure would help to ensure that economic matters remain central to national security determinations in the future.

II. ECONOMIC IMPACT OF NSA PROGRAMS

Billions of dollars are on the line because of worldwide concern that the services provided by U.S. information technology companies are neither secure nor private.[12] Perhaps nowhere is this more apparent than in cloud computing. Approximately 50% of the worldwide revenues previously came from the United States.[13] The domestic market more than tripled in value 2008-2014.[14] But within weeks of the Snowden documents, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft's Azure were losing business.[15] By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information.[16] In January 2014 a survey of Canadian and British businesses found that one quarter of the respondents were moving their data outside the United States.[17] The Information Technology and Innovation Foundation estimates that declining revenues of corporations that focus on cloud computing and data storage alone could reach $35 billion over the next three years.[18] Other commentators, such as Forrester Research analyst James Staten, have put actual losses

---

their customers only when required under law – and not knowingly through a back door – the perception that they enabled the spying program has lingered.")

[12] *IT Industries Set to Lose Billions Because of Privacy Concerns*, UPI, Dec. 17, 2013, available at http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/ ("Information technology companies stand to lose billions of dollars of business because of concerns their services are neither secure nor private.").

[13] *Gartner Predict Cloud computing Spending to Increase by 100% in 2016, Says AppsCare*, PR WEB, July 19, 2012, available at http://www.prweb.com/releases/2012/7/prweb9711167.htm.

[14] *Id.*

[15] David Gilbert, *Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations*, INT'L BUSINESS TIMES, July 4, 2013, *available at* http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613.

[16] Mieke Eoyang & Gabriel Horwitz, Opinion: *NSA Snooping's Negative Impact on Business Would Have the Foundign Fathers "Aghast,"* FORBES, Dec. 20, 2013, *available at* http://snewsi.com/id/1342616710/NSA-Snoopings-Negative-Impact-On-Business-Would-Have-The-Founding-Fathers-Aghast.

[17] *NSA Scandal: UK and Canadian Business Wary of Storing Data in the US*, PEER 1 HOSTING, Jan. 8, 2014.

[18] *Id. See also* Mary DeRosa, *U.S. Cloud Services Companies Are Paying Dearly for NSA Leaks*, TECH INSIDER, Mar. 24, 2014, *available at* http://www.nextgov.com/voices/mary-derosa/8437/ (reporting estimates of losses of $22 billion over the next three years).

as high as $180 billion by 2016, unless something is done to restore confidence in data held by U.S. companies.[19]

The economic impact of the NSA programs extends beyond cloud computing to the high technology industry. Cisco, Qualcomm, IBM, Microsoft, and Hewlett-Packard have all reported declining sales as a direct result of the NSA programs.[20] Servint, a webhosting company based in Virginia, reported in June 2014 that its international clients had dropped by 50% since the leaks began.[21] Also in June, the German government announced that because of Verizon's complicity in the NSA program, it would end its contract with the company, which had previously provided services to a number of government departments.[22] As a senior analyst at the Information Technology and Innovation Foundation explained, "It's clear to every single tech company that this is affecting their bottom line."[23] The European commissioner for digital affairs, Neelie Kroes, predicts that the fallout for U.S. businesses in the EU alone will amount to billions of Euros.[24]

Not only are U.S. companies losing customers, but they have been forced to spend billions to add encryption features to their services. IBM has invested more than a billion dollars to build data centers in London, Hong Kong, Sydney, and elsewhere, in an effort to reassure consumers outside the United States that their information is protected from U.S. government surveillance.[25] Salesforce.com made a similar announcement in March 2014.[26] Google moved to encrypt terms entered into its browser.[27] And in June 2014 the company released the source code for End-to-End, its newly-developed browser plugin that allows users to encrypt email prior to it being sent across the Internet.[28] The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.[29] Together with the establishment of a Transparency Center, where foreign governments could review source code to assure themselves of the integrity of Microsoft software, the company sought to put an end to both NSA back door surveillance and doubt about the integrity of Microsoft products.[30]

---

[19] *IT Industries Set to Lose Billions Because of Privacy Concerns*, UPI, Dec. 17, 2013, available at http://www.upi.com/Business_News/Security-Industry/2013/12/17/IT-industries-set-to-lose-billions-because-of-privacy-concerns/UPI-30251387333206/. This number includes domestic customers who may go elsewhere to find greater privacy protections. *See* Gustin, *supra* note 11.

[20] Sean Gallagher, *NSA Leaks Blamed for Cisco's Falling Sales Overseas*, ARS TECHNICA, Dec. 10, 2013; Paul Taylor, *Cisco Warns Emerging Market Weakness is no Blip*, FIN. TIMES, Dec. 13, 2013; Spencer E. Ante, *Qualcomm CEO Says NSA Fallout Impacting China Business*, WALL. ST. J., Nov. 22, 2013; Miller, *supra* note 11.

[21] Julian Hattem, *Tech Takes Hit from NSA*, THE HILL, June 30, 2014.

[22] Andrea Peterson, *German Government to Drop Verizon over NSA spying Fears*, WASH. POST, June 26, 2014.

[23] *Id.*

[24] Eoyang et al, *supra* note 16.

[25] Miller, *supra* note 11.

[26] *Id.*

[27] Danny Sullivan, *Post-PRISM, Google Confirms Quietly Moving to Make All Searches Secure, Except for Ad Clicks*, SEARCH ENGINE LAND, Sept. 23, 2013, *available at* http://searchengineland.com/post-prism-google-secure-searches-172487.

[28] Klint Finley, *Google Renews Battle With the NSA by Open Sourcing Email Encryption Tool*, WIRED, June 3, 2014, *available at* http://www.wired.com/2014/06/end-to-end/.

[29] Matt Thomlinson, Vice President Trustworthy Computing Security, Microsoft, *Advancing our Encryption and Transparency Efforts*, Press Release, *available at* http://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/. *See also* Carly Page, *Microsoft Installs Tougher Outlook and Onedrive Encryption to Curb NSA Snooping*, THE INQUIRER, Jul. 1, 2014, *a* http://www.theinquirer.net/inquirer/news/2353073/microsoft-installs-better-outlook-and-onedrive-encryption-to-curb-nsa-snooping.

[30] *Id.*

Foreign technology companies, in turn, are seeing revenues increase.[31] Runbox, for instance, an email service based in Norway and a direct competitor to Gmail and Yahoo, almost immediately made it publicly clear that it does not comply with foreign court requests for its customers' personal information.[32] Its customer base increased 34% in the aftermath of the Snowden revelations.[33] Mateo Meier, CEO of Artmotion (Switzerland's biggest offshore data hosting company), reported that within the first month of the Snowden releases, the company saw a 45% rise in revenue.[34] Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is as a result of an official court order demonstrating guilt or liability; there are no exceptions for the United States.[35] In April 2014, Brazil and the European Union, which previously used U.S. firms to supply undersea cables for transoceanic communications, decided to build their own cables between Brazil and Portugal, using Spanish and Brazilian companies in the process.[36] OpenText, Canada's largest software company, now guarantees customers that their data remains outside the United States. Deutsche Telekom, a cloud computing provider, is similarly gaining more customers.[37] In sum, numerous foreign companies are marketing their products as "NSA proof" or "safer alternatives" to those offered by U.S. firms, gaining market share in the process.[38]

III. FOREIGN GOVERNMENT RESPONSES

The Snowden documents revealed not just the extent to which high technology companies had become coopted, but that the targets of NSA surveillance include both allied and non-allied countries.[39] The resulting backlash has led some commentators to raise concern that "the Internet will never be the same."[40] Jurisdictional questions and national borders previously marked the worldwide Internet discussions.[41] Countries, however, are now using the disclosures to restrict data storage to national borders, making it more difficult for the United States to gain access.[42] As risk is the balkanization of the Internet, undermining its traditional culture of open access, and increasing the cost of doing business.[43]

---

[31] *Id.*
[32] Miller, *supra* note 11.
[33] *Id.*
[34] Gilbert, *supra* note 15.
[35] *Id.*
[36] Miller, *supra* note 11.
[37] *Id.*
[38] Mark Scott, *European Firms Turn Privacy into Sales Pitch*, N. Y. TIMES, June 11, 2014.
[39] *See, e.g.*, Laura Poitras, Marcel Rosenbach, Fidelius Schmid and Holger Stark, *NSA Spied on European Union Offices*, DER SPIEGEL, June 29, 2013; Laura Poitras, Marcel Rosenbach, and Holger Stark, *Codename "Apalachee": How America Spies on Europe and the UN*, DER SPEIGEL ONLINE, Aug. 26, 2013, *available at* http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html; *EXCUSIVE: US spies on Chinese Mobile Phone Companies, Steals SMS Data: Edward Snowden*, SOUTH CHINA MORNING POST, June 22, 2013, *available at* http://www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden; Lana Lam, *US Hacked Pacnet, Asia Pacific Fibre-Optic Network Operator, in 2009*, SOUTH CHINA MORNING POST (HONG KONG), June 23, 2013; Ewen MacAskill, Julian Borger, NEW NSA LEAKS SHOW HOW US IS BUGGING ITS EUROPEAN ALLIES, THE GUARDIAN (LONDON), June 30, 2013.
[40] Levy, *supra* note 10.
[41] *See, e.g.*, Kristina Irion, *Government Cloud Computing and National Data Sovereignty*, SOCIAL SCIENCE RESEARCH NETWORK, June 2012.
[42] Levy, *supra* note 10.
[43] *Id.*

A. Data Localization and Data Protection

Countries around the world are increasingly adopting data localization laws, restricting the storage, analysis, and transfer of digital information to national borders.[44] To some extent, the use of barriers to trade as a means of incubating tech-based industries predated the Snowden releases.[45] However, in the aftermath of the leaks, the dialogue has accelerated. The asserted purpose is to protect both government data and consumer privacy.

As of the time of writing, China, Greece, Malaysia, Russia, South Korea, Venezuela, Vietnam, and others have already implemented local data server requirements.[46] Turkey has introduced new privacy regulations preventing the transfer of personal data (particularly locational data) overseas.[47] Others, such as Argentina, India, and Indonesia are actively considering new laws, even as Brazilian president, Dilma Rousseff, has been promoting a law that would require citizens' personal data to be stored within domestic bounds.[48] Germany and France are considering a Schengen routing system, retaining as much online data in the European Union as possible.[49]

As a regional matter, the EU Commission's Vice President, Viviane Reding, is pushing for Europe to adopt more expansive privacy laws.[50] And in March 2014 the European Parliament passed the Data Protection Regulation and Directive, imposing strict limits on the handling of EU citizens' data. Regardless of where the information is based, those handling the data must obtain the consent of the data subjects to having their personal information processed. They also retain the right to later withdraw consent. Those violating the directive face steep fines, including up to five percent of revenues.

In addition, the Civil Liberties, Justice, and Home Affairs Committee of the European Parliament passed a resolution calling for the end of the US/EU Safe Harbor agreement.[51] Some 3000 U.S. companies rely on this framework to conduct business with the EU.[52]

---

[44] Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders*, 2(3) LAWFARE RESEARCH PAPER SERIES, Jul. 21, 2014.

[45] *See, e.g.,* Stephen J. Ezell, Robert D. Atkinson, and Michaelle A. Wein, *Localization Barriers to Trade: Threat to the Global Innovation Economy, The Information Technology & Innovation Foundation*, Sept. 2013, *available at* http://copyrightalliance.org/sites/default/files/resources/2013-localization-barriers-to-trade.pdf.

[46] Sidley Austin, LLP., *Privacy, Data Security and Information Law Update*, Dec. 30, 2013, available at http://www.sidley.com/files/News/1ce5014c-9236-41cb-87ba-32dee9163fed/Presentation/NewsAttachment/6d72f3e3-6b28-4d23-bc9a-5493071c9b13/12.30.2013%20Privacy%20Update.pdf.

[47] Richard Chirgwin, *USA Opposes "Schengen Cloud" Eurocentric Routing Plan*, THE REGISTER (United Kingdom), Apr. 7, 2014, *available at* http://www.theregister.co.uk/2014/04/07/keeping_data_away_from_the_us_not_on_ustr/.

[48] Levy, *supra* note 10.

[49] *See, e.g., Weighing a Schengen Zone for Europe's Internet Data*, DEUTSCHE WELL, Feb. 20, 2014, *available at* http://www.dw.de/weighing-a-schengen-zone-for-europes-internet-data/a-17443482 ; *Deutsche Telekom: "Internet Data Made in Germany should Stay in Germany,"* DEUTSCHE WELLE, Oct. 18, 2013, *available at* http://www.dw.de/about-dw/who-we-are/s-3325.

[50] Mike Eoyang & Gabriel Horwitz, *Opinion*: *NSA Snooping's Negative Impact on Business Would have the Founding Fathers "Aghast,"* FORBES, Dec. 20, 2013.

[51] *NSA Snooping; MEPS TABLE PROPOSALS TO PROTECT EU CITIZENS' PRIVACY*, EUROPEAN PARLIAMENT, Feb. 12, 2014.

[52] Alex Byers, *Tech Safe Harbor Under Fire in Europe*, POLITICO MORNING TECH, Nov. 6, 2013.

In May 2014 the EU Court of Justice ruled that users have a "right to be forgotten" in their use of online search engines. The case derived from a complaint lodged against a Spanish newspaper, as well as Google Spain and Google Inc., claiming that notice of the plaintiff's repossessed home on Google's search engine infringed his right to privacy because the incident had been fully addressed years before. He requested that the newspaper be required to remove or alter the pages in question to excise data related to him, and that Google Spain or Google Inc. be required to remove the information. The EU court found that even where the physical server of a company processing information is not located in Europe, as long as the company has a branch or subsidiary and is doing business in a Member state, the 1995 Data Protection Directive applies.[53] Because search engines contain personal data, they are subject to such data protection laws. The Court recognized that, under certain conditions, individuals have the "right to be forgotten"—i.e., the right to request that search engines remove links containing personal information. Data that is inaccurate, inadequate, irrelevant, or excessive may be removed. Not absolute, the right to be forgotten must be weighed against competing rights, such as freedom of expression and the media.

Various country-specific privacy laws are similarly poised to be introduced. Their potential economic impact is not insubstantial: the Information Technology and Innovation Fund estimates that data privacy rules could retard the growth of the technology industry by up to four percent, impacting U.S. companies' ability to expand and forcing them out of existing markets.[54]

The current dialogue is merely the latest in a series of growing concerns about the absent of effective privacy protections within the U.S. legal regime. High tech companies appear to see this as a potential step forward. As Representative Justin Amash (MI-R), has explained, "Businesses increasingly recognize that our government's out-of-control surveillance hurts their bottom line and costs American jobs. It violates the privacy of their customers and it erodes American businesses' competitive edge."[55]

It is with concern about the impact of lack of privacy controls on U.S. competitiveness in mind that in December 2013 some of the largest U.S. Internet companies launched a campaign to pressure the government to reform the NSA surveillance programs. Microsoft General Counsel Brad Smith explained: "People won't use technology they don't trust." He added, "Governments have put this trust at risk, and governments need to help restore it." Numerous high technology CEOs supported the initiative, such Google's Larry Page, Yahoo's Marissa Mayer, and Facebook's Mark Zuckerberg.[56] The aim is to limit government authority to collect user data, to institute better oversight and accountability, to ensure greater transparency about what the government is requesting (and obtaining), to increase respect for the free flow of data across borders, and to avoid political clashes on a global scale. Mayer, explained, "Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world."[57]

---

[53] Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[54] Michael Hickens, AMERICAN SPYING STYMIES TECH FIRMS, WALL STREET J., Feb. 18, 2014.
[55] Gustin, *supra* note 11
[56] *Id.*
[57] *Id.*

B. Global Initiatives Regarding Internet Governance

Apart from economic considerations, the backlash raises question about the future of Internet governance. From the inception of the Internet, the U.S.-based Internet Corporation for Assigned Names and Numbers (ICANN) has governed the web. As time has progressed, and the Internet has become part of the global infrastructure, there have been calls from several nations to end U.S. dominance and to have the International Telecommunication Union (ITU), an entity within the UN, become the governing body. The revelations have not only contributed further to such calls, but they have spurred increased discussion of the need for regional Internet control.

Over the past decade, three main groups have emerged to vie for control of the Internet. The first is centered on states, who consider the question in light of national sovereignty. It is comprised of developing countries as well as large, emerging economies like China, Russia, Brazil, and South Africa.[58] It overlaps significantly with the Group of 77 (consisting of more than 100 countries which emerged from the non-aligned movement in the Cold War). These states are critical of the United States and its dominant role in Internet governance and oppose private sector preeminence, on the grounds that they are pawns of the United States. Emphasis instead is placed on the UN and the ITU as potential repositories of Internet authority.

The second group is civil society. The third is the private sector. These groups both tend to support what is referred to as a "multistakeholder model:" i.e., native Internet governance institutions that are generally nonprofit entities in the private sector.[59] Membership includes both technical experts (e.g., ICANN and Regional Internet Registries), as well as multinational corporations (e.g., Microsoft, Facebook, and AT&T). Prior to the Snowden releases, Japan, the EU, and the US found themselves in this camp. Civil society organizations emphasize Internet freedom, consumer privacy, and user rights—often bringing them into conflict with the states who comprise the G77-type group.[60]

As one commentator explains, "This alignment of actors has been in place since the 2003 World Summit on the Information Society (WSIS) meetings. But the Snowden NSA revelations seem to have destabilized this settled political alignment."[61]

In brief, ICANN and Brazil have formed an alliance, condemning U.S. actions. Concern about the latest revelations spurred a major conference in April 2014: i.e., the *Global Multistakeholder Conference on the Future of Internet Governance*. The purpose of the meeting, which was held in Sao Paulo, was "to produce universal internet principles and an institutional framework for multistakeholder Internet governance."[62]

It is not clear how the newest shifts will be resolved—either temporarily or in the future. But significant, and enormously important, questions have been raised by the Snowden revelations: How should the Internet governance be structured to ensure legitimacy and compliance? Who gets to make the decision about what such governance looks like? Which bodies have the authority to establish future rules and procedures? How are such bodies constituted and who selects their membership?

---

[58] Milton Mueller and Ben Wagner, *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance*, (2013), p. 3, *available at* http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final.pdf.
[59] *Id.*
[60] *Id.*
[61] *Id.*, at 4.
[62] *Id.*, at 1.

These questions are fundamentally at odds with the decentralization tendencies in the Internet—tendencies that have been exaggerated post-Snowden as a result of regional efforts to expand the local sphere of influence and to protect consumer and state privacy from U.S. surveillance.

The U.S. government's failure to address the situation domestically has undermined the tech industry. Despite calls from the companies for legislative reform to address the breadth of the NSA programs,[63] there has been no significant shift that would allow companies to approach their customers to say, with truth, that the situation has changed. Resultantly, American companies are losing not just customers, but the opportunity to submit proposals for contracts for which they previously would have been allowed to compete.[64] And the future of Internet governance hangs in the balance.

IV. ECONOMIC SECURITY AS NATIONAL SECURITY

The NSA programs illustrate lawmakers' failure to recognize the degree to which economic strength is central to national security, as well as the importance of the high technology industry to the U.S. economy. The concept of economic security as national security is not new: the Framers and the generations that followed acknowledged the importance of economic strength as central to national security. Our more recent understandings, however, have gotten away from the concept, in the process cleaving important interests out of the calculations required to accurately understand the implications of government actions. Unintended consequences have resulted: the NSA revelations, for instance, may have driven bad actors to seek non-U.S. companies for ISP services, creating gaps in insight into their operations. They have also undermined U.S. efforts to call other countries to heel for their exploitation of international communications to gain advantages over U.S. industry. In sum, the expansive nature of the programs may well have acted to undermine U.S. national security in myriad ways linked to the country's economic interests.

A. Economic Security from the Founding

Despite its appearance throughout U.S. history, the term "national security" is rarely defined.[65] The 1947 National Security Act, for instance, which, *inter alia*, constituted the National Military Establishment (later the Department of Defense), and the National Security Council, refers to "national security" more than 100 times; yet it does not define the term.[66] The Foreign Intelligence Surveillance Act of 1978 employs the term nearly a dozen times, to ascertain what matters fall within the Foreign Intelligence Surveillance Court's (FISC) purview, who can certify an application to FISC, and under what conditions *in camera* and *ex parte* proceedings can be held.[67] Where the Attorney General ascertains that a national security threat exists, officials may secretly search and seize property—waiting notice otherwise required under the Fourth Amendment.[68] But no definition is provided in FISA. Nor

[63] *See, e.g.*, Gustin, *supra* note 11 (reporting that the nation's largest Internet companies are calling for Congress and the Administration to reform the secret surveillance programs).
[64] Miller, *supra* note 11.
[65] *See* Laura K. Donohue, *The Limits of National Security*, 48 AM. CRIM. L. REV., 1579 (2011).
[66] National Security Act of 1947, Pub. L. No. 80-235, 61 Stat. 495 (current version at 50 U.S.C. §401 (2006)).
[67] 50 U.S.C. §§1803(e), 1804(a), 1806(f), and 1845(f).
[68] 50 USC §1825(b).

does the USA PATRIOT Act prove more illuminating—despite referring to national security more than two dozen times.[69]

Where we do find definitions in the U.S. Code, they tend to limit consideration to foreign affairs and matters related to military strength. Thus, under the Classified Information Procedures Act, "national security" is understood as involving matters related to the "national defense and foreign relations of the United States."[70] Nowhere does the definition reference U.S. economic security.

In the amended National Security Act, while the term could potentially be understood to encompass U.S. economic security, the actual definition does not specify a precise link to economic vitality. Instead, "intelligence related to national security" refers to:

> all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that
> (A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and
> (B) that involves—
> (i) threats to the United States, its people, property, or interests;
> (ii) the development, proliferation, or use of weapons of mass destruction; or
> (iii) any other matter bearing on United States national or homeland security.[71]

The Federal Information Security management Act of 2002 (providing rules for government-wide information security) similarly fails to consider the economic underpinnings of national security, instead, understanding national security systems as any system:

> (i) the function, operation, or use of which
> (I) involves intelligence activities;
> (II) involves cryptologic activities related to national security;
> (III) involves command and control of military forces;
> (IV) involves equipment that is an integral part of a weapon or weapons system; or
> (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or
> (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.[72]

While there may be room in the definition for economic considerations, they are not front and center.

Executive Branch articulations prove little better. President George W. Bush's five-page National Security Presidential Directive 1 referred to "national security"

[69] *See, e.g.*, Pub. L. No. 107-56, §505.
[70] Classified Information Procedures Act §1(b), 18 U.S.C. app. 3 (2006).
[71] 50 U.S.C.A. § 401a(5) (2012).
[72] Federal Information Security Management Act of 2002, Pub. L. 107-347, § 201, 116 Stat. 2947 (2002) (codified at 44 U.S.C. § 3542(b)(2)(A)).

thirty-three times, without any definition.[73] President Barak Obama's Presidential Policy Directive 1 (PPD-1), in turn, addressing the National Security Council, referred to "national security" thirty-three times—without ever defining it.[74] And like the Executive Branch, Courts tend to look to the military and diplomatic aspects of national security, instead of their economic concomitant.[75]

Despite the lack of emphasis on economic strength, the Founders were well aware of the importance of the economy in fostering international independence. The Articles of Confederation failed in significant part because the national government lacked the resources, and the country the economic strength, to protect the Union. For Alexander Hamilton, absent military might, diplomatic stature, and commercial success, the country would cease to exist.[76]

One of the first expansions of the executive, accordingly, was to include a Secretary of the Treasury, which, along with the Secretary of War and the establishment of the office of Attorney General, reflected the purposes for which Union had been sought: foreign relations, military strength, economic growth, and the rule of law. In his *Farewell Address*, President George Washington called for U.S. energies to be directed towards strengthening the U.S. economy: "[T]he great rule of conduct for us in regard to foreign nations is in extending our commercial relations, to have with them as little political connection as possible."[77]

The federal government was willing, from a very early date, to act in support of its commercial interests with whatever diplomatic, legal, and military power it could muster.[78] The Monroe Doctrine was premised largely on this approach. In 1837 President Martin Van Buren came to office determined to continue Washington's legacy, underscoring the importance of avoiding entangling alliances while pursuing America's economic interests abroad.[79] President Zachary Taylor came to office in 1849 determined to continue the course, emphasizing the importance of bolstering trade as a means of securing the country.[80] The 1950 Clayton-Bulwer Treaty ensured that future canal access through Central America would be open to international trade.[81] As Millard Fillmore succeeded Taylor, he considered commerce central to U.S. interests abroad—for this reason, the Navy would require further resources to protect trade along the Pacific Coast.[82] Upon taking office, President Franklin Pierce reiterated the same policies: of the complicated European tumults and anxieties, the

---

[73] George W. Bush, NSPD-1, National Security Presidential Directive 1: Organization of the National Security Council System (2001).

[74] *See* Barack Obama, PSD-1, Presidential Study Directive 1: Organizing for Homeland Security and Counterterrorism 1-2 (2009), *available at* http://www.fas.org/irp/offdocs/psd/psd-1.pdf ("[C]onceptually and functionally, [national security and homeland security] should be thought of together rather than separately.").

[75] *See, e.g.*, *See N.Y. Times Co.*, 403 U.S. at 719 (Black, J., concurring).

[76] FEDERALIST No. 1, (Alexander Hamilton).

[77] President George Washington, Farewell Address to the People of the United States (Sept. 19, 1796), *reprinted in* S. Doc. No. 106-21, at 6 (2d Sess. 2000) [hereinafter Washington, Farewell Address], http://www. access.gpo.gov/congress/senate/farewell/sd106-21.pdf.

[78] For a catalog of every military intervention in support of U.S. commercial interests, *see* WILLIAM APPLEMAN WILLIAMS, EMPIRE AS A WAY OF LIFE: AN ESSAY ON THE CAUSES AND CHARACTER OF AMERICA'S PRESENT PREDICAMENT ALONG WITH A FEW THOUGHTS ABOUT AN ALTERNATIVE (1st ed. 1980).

[79] President Martin Van Buren, Inaugural Address (Mar. 4, 1837).

[80] President Zachary Taylor, Inaugural Address (Mar. 5, 1849).

[81] Convention Between the United States of America and Her Britannic Majesty (Clayton-Bulwer Treaty), U.S.-Gr. Brit., Apr. 19, 1850, 9 Stat. 995.

[82] President Millard Fillmore, First Annual Message to Congress (Dec. 2, 1850), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=29491&st=fillmore&st1=#axzz1Wo2idoeG.

United States was to be exempt, "But the vast interests of commerce are common to all mankind, and the advantages of trade and international intercourse must always present a noble field for the moral influence of a great people." The United States went on to emphasize its dealings with Asia and to sign an historic trade agreement with Japan.[83] Expansionism, and the economic benefits it brought, similarly proved central to U.S. national security. "Should [new possessions] be obtained," Pierce asserted during his *Inaugural Address*, "it will be through no grasping spirit, *but with a view to obvious national interest and security*, and in a manner entirely consistent with the strictest observance of national faith." From the 1898 Spanish-American War forward, the country promoted its national interests through formative political, military, and economic engagement in the international arena.

2. National Security Infrastructure

The National Security Council (NSC) is "the principal forum for consideration of national security policy issues requiring Presidential determination."[84] The President looks to the forum for advice and assistance in matters ranging from domestic, foreign and military, to intelligence and economic.[85] It is thus somewhat surprising that the 1947 National Security Act includes neither the Secretary of the Treasury, nor the Secretary of Commerce, as permanent (statutory) members of the NSC.

Instead, the entity is chaired by the President, with formal membership extended to the Vice President, the Secretary of State, and the Secretary of Defense. The Chair of the Joint Chiefs of Staff acts as the statutory military advisor, the Director of National Intelligence the statutory intelligence advisor, and the Director of National Drug Control Policy as the statutory drug control policy advisor.

Under PDD-1, the NSC includes the Secretary of Treasury, and "When international economic issues are on the agenda of the NSC, the NSC's regular attendees will include the Secretary of Commerce, the United States Trade Representative, the Assistant to the President for Economic Policy, and the Chair of the Council of Economic Advisers."[86]

When the emphasis, however, is not international economic issues, the structure does not cement economic concerns into the discussion. Nor does it contemplate the inclusion of Treasury or Commerce as an operational matter—i.e., when the intelligence community is deciding whether to develop a surveillance program. Such matters are not brought directly to the NSC.[87]

To the extent that the failure to include these members at the most basic level reflects a perspective that potentially sidelines economic concerns, the continued failure to build in strong representation at a programmatic level underscores the concern. Economic concerns may be treated with seriousness, but they are not meaningfully integrated into the national security infrastructure.

3. Unintended Consequences

There are various ways in which the failure to fully take account of the impact of the programs on U.S. industry may have acted to undermine U.S. security beyond weakening the economy. The revelations, for instance, may well have driven enemies

[83] Treaty of Amity and Commerce, U.S.-Japan, July 29, 1858, 12 Stat. 1051.
[84] PPD-1, *Organization of the National Security Council System*, Feb. 13, 2009.
[85] *Id.*
[86] PDD-1, at 2.
[87] DeRosa, *supra* note 18.

of the United States to use other countries' Internet Service Providers, thus creating a gap in our insight into their operations. They may similarly spur the initiation of encryption techniques that the NSA will have no means to address—making the country less secure because of the perceived overreach of the agency. The revelations have also undermined U.S. credibility in challenging other countries' efforts to obtain trade secrets and other information through state surveillance. China provides one of the strongest examples.

Online warfare between China and the United States has simmered in the background, until in early 2013 the Obama Administration began to make it center stage. In January 2013 the *New York Times* reported that Chinese hackers had infiltrated its computers following a threat that if the paper insisted on publishing a story about its prime minister, consequences would follow.[88] The following month a security firm, Mandiant, revealed that the Chinese military unit 61398 had stolen data from U.S. companies and agencies.[89] In March 2013 President Obama's national security advisor publicly urged China to reduce its surveillance efforts—following which classified documents leaked to the public demonstrated the extent to which China had infiltrated U.S. government servers.[90] In May 2013 the National Security Advisor flew to China to lay the groundwork for a summit, in which cyber surveillance would prove center stage.[91] Two days before the Obama-Xi meeting was scheduled to take place, *The Guardian* ran the first story on the NSA programs.[92] On June 7, when Obama raised the question of Chinese espionage, Xi responded by quoting the Guardian and suggesting that the U.S. should not be lecturing the Chinese about surveillance.[93]

Although differences may mark the two countries approaches to surveillance (e.g., in one case for economic advantage, in the other for political or security advantage), the broader translation for the global community has been one in which the United States has lost high ground to try to restrict cybersurveillance by other countries.

V. STEPS REQUIRED TO REDRESS THE CURRENT SITUATION

Numerous steps could be taken by Congress to address the situation in which U.S. industry currently finds itself. The most effective and influential decision that legislators could take would be to curb the NSA's authorities under the Foreign Intelligence Surveillance Act. This action has two components: first, ending the telephony metadata collection program and, second, restricting the use of to/from, or about collection under upstream interceptions. Both programs would further benefit from greater transparency, to make it clear that their aim is to prevent foreign aggression and to prevent threats to U.S. national security—not to engage in the interception of trade secrets or to build dossiers on other countries' populations.

The second most effective change that could be undertaken would be to introduce stricter privacy controls on U.S. companies, in the process bringing the United States into closer line with the principles that dominate in the European Union. The two entities are not as far apart as the dialogue might have one assume, and so changes required in this sphere would be minimal. Together, these two alterations—curbing the NSA surveillance programs and providing increased consumer protections for

[88] Kurt Eichenwald, *How Edward Snowden Escalated Cyber War*, NEWSWEEK, Nov. 1, 2013.
[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Id.*
[93] *Id.*

privacy—would allow U.S. industry to argue changed circumstance to allow companies to again become competitive for contracts and markets to which they seek access.

A third alteration that would make a substantial difference over the longer term relates to the national security infrastructure. The current failure of the United States to integrate economic concerns creates a vulnerability for the country in terms of the breadth and depth of programs subsequently adopted. New thought needs to be given to how to take on board—and mitigate—potentially devastating economic consequences of government surveillance efforts.

A. FISA Alterations

In addition to the economic impact of NSA telephony metadata collection (discussed, *infra*), the program runs contrary to Congressional intent in introducing the Foreign Intelligence Surveillance Act, contradicts the statutory language, and violates the Fourth Amendment.[94] In 2014 the Privacy and Civil Liberties Oversight Board came to a similar conclusion,[95] as did the President's own appointed Review Group, charged with considering the telephony metadata collection program, in 2013.[96]

Accordingly, the President announced on January 17, 2014 that he was "ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk metadata."[97] The alternative approach was to be developed by March 28, 2014. Nine months later, on September 13, 2014, the Foreign Intelligence Surveillance Court approved DOJ's request to extend the program for another 90 days—without any transition program in place.

Although the President issued a new presidential directive in January 2014 for U.S. signals intelligence activities both at home and abroad, the classified nature of parts of the document, international skepticism about the Administration's commitment to privacy, and the failure of the Administration to make good on its promise of transition to a new program meant that the global community, with good reason, has questioned whether anything has really changed. No new legislation is in place that would provide limits on the Executive Branch beyond those that operated for the duration of the bulk collection program.

As a matter of Section 702 and the interception of international content, both PRISM and upstream collection present global concerns—neither of which have been addressed through any legislative change. The existence of these programs, while perhaps statutorily consistent with the FISA Amendments Act, as well as constitutionally sufficient with regard to the interception of non-U.S. persons

---

[94] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37(3) HARV. J. OF L. & PUB. POL'Y, 757-900 (2014), *available at* http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2360&context=facpub

[95] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, Jan. 23, 2014, *available at* https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf.

[96] PRESIDENT'S REVIEW GROUP, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, Dec. 12, 2013, available at http://apps.washingtonpost.com/g/page/world/nsa-review-boards-report/674/.

[97] *Remarks by the President on Review of Signals Intelligence*, Jan. 17, 2014, *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

communications, where the individual is reasonably believed to be located outside the United States, as a policy matter, goes some way towards undermining international confidence in U.S. companies.

The Fourth Amendment does not reach non-U.S. persons based overseas who lack a substantial connection to the United States.[98] Writing for the Court in *United States v. Verdugo-Urquidez*, Chief Justice Rehnquist concluded that "the people" referred to in the Fourth Amendment indicate a particular group—not merely people *qua* people.[99] His reading stems from a deeply Aristotelian approach: i.e., one that emphasizes membership in the polis (πόλις), or political community, as a concomitant of forming a structure of government.[100] As members of the polis, U.S. persons, both distributively and collectively, obtain the protections of the constitution.

Looked at in this regard, the Constitution itself embodies the collective organization of "the people" into one entity. "U.S. persons" and "the people" are therefore one and the same. The "right of the people" thus refers to a collective group of individuals "who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[101]

Very few cases address precisely what constitutes sufficient contact with the United States to satisfy the "substantial connections" aspect of the majority's decision. Those that do point in seemingly different directions.[102] At a minimum, however, it would be extraordinary to assume that simply because an individual uses a U.S. company, he or she thereby gains the protections of the Fourth Amendment. This was the basic argument underlying the "modernization" of FISA in the first place, to take account of bad actors, communicating overseas, who would suddenly fall within the more protective FISA regime merely because their communications happened to come within U.S. territory by nature of the carrier in question.

Even recognizing, however, that few constitutional barriers may apply to the programmatic use of Section 702 insofar as it is applied to non-U.S. persons (leaving aside the questions that accompany the incidental collection of U.S. persons' information, as well as entirely domestic conversations), as a matter of policy, certainly both PRISM and the use of to/from or about collection in upstream gathering has dramatically undermined U.S. industry. As a matter of policy, therefore, greater restrictions, more transparency, and more effective oversight of the international collection of content may help to alter the situation with regard to the skepticism expressed towards U.S. companies.

B. Privacy Law Harmonization

Much ink has been spilled on the cultural and practical differences between the U.S. and EU with regard to data protection and privacy law. These differences have been over-blown.

---

[98] *Section 702 and the collection of International Telephone and Internet Content*, 38(1) HARV. J. OF L. & PUB. POL'Y, (2015), *available at* http://scholarship.law.georgetown.edu/facpub/1355/.
[99] United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990) (per curiam).
[100] ARISTOTLE, POLITICS, BOOK I (350 BC), trans. by Benjamin Jowett, *available at* http://classics.mit.edu/Aristotle/politics.1.one.html; also *available at* http://www.perseus.tufts.edu/hopper/text;jsessionid=91A85450747C74DF609D266E0A8DF8E5?doc=Perseus%3atext%3a1999.01.0057 (in the original Greek).
[101] 494 U.S. at 265 (per curiam).
[102] Orin Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. (forthcoming 2015), at 8-9.

There are myriad ways in which the two regions reflect a similar approach. Just as the United States' Fourth Amendment protects the right to privacy, for instance, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms embraces the same.[103] These documents constitutionally ground two fundamental liberty interests in the respective regions' governing frameworks: (a) the right to privacy, and (b) freedom from arbitrary invasion of one's private sphere. In the European Union, these liberties are supported by EU-wide directives, such as the 1995 European Data Protection Directive and the EU Internet Privacy Law of 2002. Further, in both the EU and the U.S. such liberty interests are protected through national legislation, in which a judicial remedy is provided for a breach of the right to privacy.[104] The manner in which these rights are treated is similarly consistent. In both spheres, these rights are offset against the obligations owed by the data holder to the individual to whom the information relates.[105]

As a substantive matter, the two regions have adopted similar provisions. In both the EU and the U.S., for instance, heightened protections are provided for what is known as personally-identifiable information.[106] A series of exceptions to the dominant structure is provided in two central areas: security (including, e.g., criminal law, public security, defense, and national security) and freedom of expression (such as with regard to journalism, literary pursuits, artistic expression, and political opinions).[107] To ensure that the substantive measures reflect the underlying constitutional principles, both regions insist on minimization—i.e., that the information collected on individuals be limited to what is strictly necessary for the purposes delineated by statute.[108]

Both the U.S. and the EU have established a set of substantive requirements related to individuals' knowledge that data about them is being collected, stored, and possibly shared with others. Consent, for instance, is central to both systems.[109] Much has been made in regard to the distinction between the opt-in (European approach) versus the opt-out (American approach). What has been lost, however, is that both approaches rely on the consent of the subject (subject to specific exceptions, above), in order to proceed with data gathering, analysis, and distribution. To

---

[103] *Compare* "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST., 4th Amend., and "Everyone has the right to respect for his private and family life, his home and his correspondence." Eur. Conv. H.R. & F. F., Art. 8.

[104] *Compare* EU Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Recitations No. 55 [hereinafter 1995 EU Directive], and U.S. statutory provisions related to privacy (including, *inter alia*: the Americans with Disabilities Act, the Cable Communications Policy Act of 1984, the Children's Internet Protection Act of 2001, Children's Online Privacy Protection Act of 1998, Fair Credit Reporting Act, Driver's Privacy Protection Act of 1994, Electronic Communications Privacy Act of 1986, Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Privacy Act of 1974, Privacy Protection Act of 1980, Right to Financial Privacy Act of 1978, Telephone Consumer Protection Act of 1991, Video Privacy Protection Act of 1988, and the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936, Aug. 21, 1996).

[105] *Compare* 1995 EU Directive, Recitation No. 25, and U.S. laws, *supra* note 5.

[106] *Compare, e.g.*, 1995 EU Directive, Recitation No. 26, and the Systems of Records Notice requirement in the U.S. Privacy Act of 1974.

[107] *Compare, e.g.*, 1995 EU Directive, Recitation No. 16 (national security), 17 (written and artistic expressions), and 36 (political opinions), and 1978 Foreign Intelligence Surveillance Act (national security exceptions and singling out of otherwise protected First Amendment activity). *See also* EU 2006 Data Retention Directive (creating exceptions for criminal law).

[108] *Compare* 1995 EU Directive, Recitation No. 28 and 1978 Foreign Intelligence Surveillance Act.

[109] *Compare* 1995 EU Directive, Recitation No. 30 and U.S. laws, *supra* note 5.

facilitate this structure, both regions also require that notice be provided to targets and that individuals have the right to access information that is held about them.[110] Individuals, in both systems, have the right to object to particular information, and in both systems, the data holder has a duty to ensure that the information is accurate and kept up to date.[111]

Keeping in mind the consistencies between the two systems, and the benefits to be gained for U.S. industry from emphasizing harmony, there are two areas where the two regions depart could be addressed through legislative reform: namely, recognition of residual rights in third party data, and the creation of a comprehensive, privacy-protective regime, as opposed to the piecemeal approach that currently marks U.S. law.

1. Residual Rights in Third Party Data

One central question that divides the United States from numerous other countries and regions—including the European Union—centers on who owns an individual's data. In the United States, since *Smith v. Maryland* (addressing pen registers and trap and trace devices), and *U.S. v. Miller* (focusing on financial records), all three branches have treated information held by third parties as lacking an individual right to privacy.[112]

In contrast, the European Union considers that the individual who has provided data to a third party to still have a privacy interest in the information.[113] The recent European Court decision, recognizing the right to anonymity, necessarily presupposes a continued interest in data, even once it is obtained by a third party.

The difference between the approaches is central to understanding how new technologies, such as social network analysis, cloud computing, and data mining, have deepened the privacy interests implicated in third party handling of data. New technologies allow information to be generated about which even those to whom the data relates are unaware. To say that individuals do not have a reasonable expectation of privacy in this information rather flies in the face of common sense.

The Supreme Court appears to be coming to this conclusion as well. In *United States v. Jones*, the Court considered a case involving 28-day surveillance involving the placement of a GPS chip on a vehicle.[114] Although ultimately decided on grounds of trespass, a shadow majority expressed strong concern about the implications of long-term surveillance. Justice Alito, joined by Justice Ginsburg, Justice Breyer, and Justice Kagan, suggested that in most criminal investigations, long-term monitoring "impinges on expectations of privacy."[115] The nature of new technologies mattered:

> Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of their convenience. Many motorists purchase cars

[110] *Compare, e.g.*, 1995 EU Directive, Recitation No. 38 (notice) and 41 (right of access), and U.S. laws, *supra* note 5.
[111] *Compare, e.g.*, 1995 EU Directive, Art. 14 (right to object) and Art. 6 (accurate data); and U.S. laws, *supra* note 5.
[112] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).
[113] *See, e.g.*, 1995 EU Directive, Recitation No. 47.
[114] United States v. Jones, 132 S.Ct. 945 (2012).
[115] *Id.* at 964 (Alito, J., concurring).

> that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.[116]

Justice Sotomayor went one step further, calling into question the entire basis for third party doctrine. Specifically, in light of the level of intrusiveness represented by modern technology, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[117] Sotomayor pointed out:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to the cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[118]

She continued, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[119]

Congress has an opportunity to take the lead by recognizing the right to privacy still held by data holders when information is collected by third parties. It can then craft statutes accordingly, ensuring that U.S. companies offer greater protections for consumers, in the process allowing industry to offset the claims of its overseas competitors.

2. Legal Framework

Thus far, U.S. high technology companies have been subject to a very different statutory and regulatory structure than that which prevails in the European Union. In the United States, privacy rights have largely been protected via a series of vertical statutes dealing with specific areas, such as children using the Internet, driver-related information, and medical data.

In the EU, in contrast, privacy has been protected by a more omnibus-type approach, which horizontally reaches across a number of areas. This approach is reflected in the 1995 Directive as well as the national legislation implementing the directive on a country-by-country basis.[120]

The vertical statutory scheme has been successful in addressing particular, discreet areas where privacy interests reside. However, outside of these narrow exceptions, in the interests of encouraging innovation, the high technology sector has been left largely unregulated by federal statute. The assumption has been that market forces would adjust to protect privacy interests.

---

116. *Id.* at 963.
117. *Id*. at 957 (Sotomayor, J., concurring).
118. *Id.*
119. *Id.*
120 *See, e.g.*, U.K. Data Protection Act of 1998, Germany's Federal Data Protection Act of 2001, France's Data Protection Act of 1978 (revised in 2004), Finland's Act on the Amendment of the Personal Data Act (986) 2000; Denmark's Act on Processing of Personal Data, Act No. 429, May 2000; Greece's Law No. 2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.

The advantage of this approach has been to give high tech companies a significant amount of flexibility, allowing them to independently gauge the appropriate level of privacy protections to give to consumers.

The drawback has been that privacy itself has become commoditized, with companies actually making money off of selling consumers' privacy interests.

Consider Google and its email service, Gmail, for instance. The company reads and analyzes all of its customers' emails, it watches what people read, it looks at web sites people visit, and it records what people purchase. The company then sells access to customers' private lives to companies who want to advertise. Thus, the mother who sends an email to her son raising concern about depression may receive an ad within hours for psychiatric services, even as a pregnant woman merely looking at cribs, may within days receive mail through the U.S. post, advertising sales at Babies R'Us.

In September 2013 Google lost an effort in the 9th Circuit Court of Appeals for judicial review of a lower court's refusal to dismiss multiple class action lawsuits accusing Google of violating the Wiretap Act. U.S. District Judge Lucy Koh determined that the case is too far along to suffer delays. Koh's interpretation of the Electronic communications Privacy Act limits the "ordinary course of business" exception—not least because Google's practice violates its own policies.[121] The lawsuits, filed in California, Florida, Illinois, Maryland, and Pennsylvania, at great expense, are proceeding.

Capitalizing on private data represents a significant breach of the right to privacy. Instead of protecting privacy, the market has exploited it for monetary gain. In the United States and overseas, individuals are concerned about the lack of protections afforded. Congressional legislation could fix this problem by bringing high technology within the broader statutory framework and thus closing a gap in the existing law.

3. Safe Harbor Considerations

In the wake of the Snowden documents, the EU Commission issued a report recommending the retention of Safe Harbor, but recommending significant changes, including required disclosure of cloud computing and other service provider contracts used by Safe Harbor members.

The Safe Harbor provisions, developed 1999-2000 by the U.S. Commerce Department, the Article 31 Committee on Data Privacy, and the European Union, created a narrow bridge between the United States and EU. At the time, the European Parliament, which did not bind the European Commission, *rejected* the Safe Harbor provisions by a vote of 279 to 259, with twenty-two abstentions. Chief amongst European concerns was the failure of the agreement to provide adequate protections.

In light of the massive data breaches we have had over the past five years in the United States, the practices of a largely unregulated high technology industry, and the ubiquitous nature of NSA surveillance, Europeans are even less supportive of the Safe Harbor provisions. They amount to a self-regulated scheme in which the Federal Trade Commission merely looks at whether a company, which has voluntarily opted-in to the program, fails to do what it has stated it will do, within the bounds of its own privacy policy. Stronger measures are necessary to restore European confidence in U.S. high technology companies.

[121] In Re: Google Inc. Gmail Litigation, Case No. 5:13-md-02430, N.D.C.A.

C. Establishing Economic Security as National Security

Economic strength as national security, as was previously discussed, is not a new concept. The Founding itself was premised, in part, on the importance of economic security as being vital to U.S. national interests. In 1787 the Articles of Confederation were written out of existence on economic security grounds, as the country sought to reassure the international community that it was a viable trading partner. Since that time, the United States has at times had to remind itself of the importance of the economy to U.S. national interests. We are once again at such a time.

High technology is a vital part of the U.S. economy. It is both a symbolic and actual manifestation of the country's commitment to innovation in every sphere of life. It plays to the United States' strengths as a nation. It has the potential to change regimes, to alter political relationships, and to shape the daily lives of people around the globe. And it deserves special attention. The danger is that U.S. industry will become less competitive and that the U.S. will thus lose its dominance in the Internet economic sphere.

To some extent, we do, structurally, pay some attention to the importance of the economy. But many consequential decisions are thus not aired in full light of the possible implications for U.S. national security.[122] One way Congress could rectify this would be to take a look at how to integrate economic concerns, as a statutory matter, into the national security infrastructure.

V. CONCLUDING REMARKS

To redress the negative effects that have followed from public awareness of the NSA programs conducted under Section 215 of the USA PATRIOT Act and Section 702 of the FISA Amendments Act, the most important step that Congress could take would be to reign in the surveillance authorities themselves, in the process providing greater transparency and oversight. An alteration in U.S. privacy law would also help to reassure U.S. customers and individuals located outside domestic bounds that consumer privacy is protected, thus allowing industry accurately to assert that the circumstances have changed. Consideration of how to integrate economic concerns into the national security infrastructure would further help to emphasize the importance of taking account of the impact of new initiatives on the United States.

[122] *Id.*