2014

High Technology, Consumer Privacy, And U.S. National Security

Laura K. Donohue
Georgetown Law, lkdonohue@law.georgetown.edu

Follow this and additional works at: http://digitalcommons.wcl.american.edu/aublr
Part of the International Trade Law Commons, and the National Security Law Commons

Recommended Citation

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University Business Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
SYMPOSIUM ARTICLES

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

LAURA K. DONOHUE*

Introduction .................................................................................................................. 12
I. Economic Impact of NSA Programs ....................................................................... 15
   A. Lost Revenues and Declining Market Share .................................................. 15
   B. Trade Agreements .......................................................................................... 18
   C. Data Localization and Data Protection .......................................................... 20
   D. Internet Governance ....................................................................................... 23
II. Economic Security as National Security ............................................................... 25
   A. Economic Security from the Founding ........................................................... 26
   B. National Security Infrastructure ...................................................................... 32
   C. Unintended Harmful Consequences ............................................................... 33
III. Steps Required To Redress the Current Situation ............................................. 36
   A. FISA Alterations ............................................................................................. 36
   B. Privacy Law Harmonization .......................................................................... 39
      1. Residual Rights in Third Party Data ............................................................ 42
      2. Legal Framework ......................................................................................... 43
      3. Safe Harbor Considerations ........................................................................ 45
   C. Establishing Economic Security as National Security .................................... 46
Conclusion ................................................................................................................... 47

* Professor of Law, Georgetown Law and Director, Center on National Security and the Law, Georgetown Law. Special thanks to David Vladeck for his comments on an earlier draft of this Article, and to Ellen Noble and Morgan Stoddard for their excellent research assistance. This Article draws in part from written testimony prepared for the U.S. House of Representatives Committee on Energy and commerce, Subcommittee on Commerce, Manufacturing, and Trade, for the hearing “Cross Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs?” Sept. 17, 2014.
INTRODUCTION

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

The first Snowden documents, printed on June 5, 2013, revealed that the government had served orders on Verizon, directing the company to turn over telephony metadata under Section 215 of the USA PATRIOT Act. The following day, The Guardian published classified slides detailing how the NSA had intercepted international content under Section 702 of the FISA Amendments Act. 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. The companies involved read like a who’s who of U.S. Internet giants: Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, and Apple.


2. Greenwald, NSA Collecting Phone Records, supra note 1.

3. Id.

4. Id.

5. Id.
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{8} Documents further suggested that the NSA had helped to promote encryption standards for which it already held the key or whose vulnerabilities the agency understood but had not taken steps to address.\textsuperscript{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.\textsuperscript{10}

As a result of the growing public awareness of these programs, U.S. companies have lost revenues, even as non-U.S. firms have benefited.\textsuperscript{11} In

\begin{itemize}
\item \textsuperscript{7}Barton Gellman & Ashkan Soltani, \textit{NSA Collects Millions of E-mail Address Books Globally}, WASH. POST, Oct. 14, 2013, 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.
\item \textsuperscript{8}Gellman & Soltani, \textit{supra} note 1.
\item \textsuperscript{9}James Ball, et al., \textit{Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security}, THE GUARDIAN (Sept. 6, 2013, 8:24 PM), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.
\item \textsuperscript{10}Steven Levy, \textit{How the NSA Almost Killed the Internet}, WIRED (Jan. 7, 2014, 6:30 AM), http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/all/.
\item \textsuperscript{11}See, e.g., Sam Gustin, \textit{NSA Spying Scandal Could Cost U.S. Tech Giants Billions}, TIME (Dec. 10, 2013), 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, \textit{U.S. High-Tech Industry Feeling the
addition, numerous countries, concerned about consumer privacy as well as the penetration of U.S. surveillance efforts in the economic and political spheres, have accelerated data 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.

It could be argued that some of these effects, such as data localization initiatives, are merely opportunistic—i.e., other countries are merely using the NSA revelations to advance national commercial and political interests. Even if true, however, the NSA programs provide other countries with an opportunity. They have weakened the U.S. hand in the international arena.

Congress has the ability to redress the current situation. 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.

The NSA programs, and public awareness of them, have had an immediate and detrimental impact on the U.S. economy. They have cost U.S. companies billions of dollars in lost sales, even as companies have seen their market shares decline. American multinational corporations have had to develop new products and programs to offset the revelations and to build consumer confidence. At the same time, foreign entities have seen revenues increase. Beyond the immediate impact, the revelation of the programs, and the extent to which the NSA has penetrated foreign data flows, has undermined U.S. trade agreement negotiations. It has spurred data localization efforts around the world, and it has raised the spectre of the future role of the United States in Internet governance. Even if opportunistic, these shifts signal an immediate and long-term impact of the NSA programs, and public knowledge about them, on the U.S. economy.

A. Lost Revenues and Declining Market Share

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. Perhaps nowhere is this more apparent than in cloud computing.

Previously, approximately 50% of the worldwide cloud computing revenues derived from the United States. The domestic market thrived: between 2008 and 2014, it more than tripled in value. But within weeks of the Snowden leaks, reports had emerged that U.S. companies such as Dropbox, Amazon Web Services, and Microsoft’s Azure were losing business. By December 2013, ten percent of the Cloud Security Alliance had cancelled U.S. cloud services projects as a result of the Snowden information. In January 2014 a survey of Canadian and British


15. Id.


17. Mieke Eoyang & Gabriel Horwitz, Op-Ed., NSA Snooping’s Negative Impact on Business Would Have the Founding Fathers ‘Aghast, FORBES (Dec. 20, 2013, 8:00
businesses found that one quarter of the respondents were moving their data outside the United States.\textsuperscript{18} 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.\textsuperscript{19} Other commentators, such as Forrester Research analyst James Staten, have put actual losses as high as $180 billion by 2016, unless something is done to restore confidence in data held by U.S. companies.\textsuperscript{20}

The monetary 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.\textsuperscript{21} Servint, a webhosting company based in Virginia, reported in June 2014 that its international clients had dropped by 50% since the leaks began.\textsuperscript{22} 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.\textsuperscript{23} 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.”\textsuperscript{24}

The European commissioner for digital affairs, Neelie Kroes, predicts that


\textsuperscript{19}Id.; see also Mary DeRosa, \textit{U.S. Cloud Services Companies Are Paying Dearly for NSA Leaks}, NEXTGOV (Mar. 24, 2014), \url{http://www.nextgov.com/technology-news/tech-insider/2014/03/us-cloud-services-companies-are-paying-dearly-nsa-leaks/81100/} (reporting estimates of losses of $22 billion over the next three years).

\textsuperscript{20}IT Industries Set to Lose Billions Because of Privacy Concerns, \url{http://www.nextgov.com/technology-news/tech-insider/2014/03/us-cloud-services-companies-are-paying-dearly-nsa-leaks/81100/}.


\textsuperscript{22}Julian Hattem, \textit{Tech Takes Hit from NSA}, THE HILL (June 30, 2014, 6:00 AM), \url{http://thehill.com/policy/technology/210880-tech-takes-hit-from-nsa}.


\textsuperscript{24}Id.
the fallout for U.S. businesses in the EU alone will amount to billions of Euros.\textsuperscript{25}

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.\textsuperscript{26} Salesforce.com made a similar announcement in March 2014.\textsuperscript{27} Google moved to encrypt terms entered into its browser.\textsuperscript{28} In June 2014 it took the additional step of releasing 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.\textsuperscript{29} The following month Microsoft announced Transport Layer Security for inbound and outbound email, and Perfect Forward Secrecy encryption for access to OneDrive.\textsuperscript{30} 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.\textsuperscript{31}

Foreign technology companies, in turn, are seeing revenues increase. 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.\textsuperscript{32} Its customer base increased 34% in the aftermath of the Snowden leaks.\textsuperscript{33} Mateo Meier, CEO of Artmotion, Switzerland’s

\textsuperscript{25} Eoyang & Horwitz, supra note 17.
\textsuperscript{26} Miller, supra note 11.
\textsuperscript{27} Id.
\textsuperscript{28} Danny Sullivan, Post-PRISM, Google Confirms Quietly Moving to Make All Searches Secure, Except for Ad Clicks, SEARCH ENGINE LAND (Sept. 23, 2013, 11:53 AM) http://searchengineland.com/post-prism-google-secure-searches-172487.
\textsuperscript{29} Klint Finley, Google Renews Battle with the NSA by Open Sourcing Email Encryption Tool, WIRED (June 3, 2014, 7:41 PM), http://www.wired.com/2014/06/end-to-end/.
\textsuperscript{31} Thomlinson, supra note 30.
\textsuperscript{32} Miller, supra note 11.
\textsuperscript{33} Id.
biggest offshore data hosting company, reported that within the first month of the leaks, the company saw a 45% rise in revenue.\textsuperscript{34} Because Switzerland is not a member of the EU, the only way to access data in a Swiss data center is through an official court order demonstrating guilt or liability; there are no exceptions for the United States.\textsuperscript{35} In April 2014, Brazil and the EU, 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.\textsuperscript{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.\textsuperscript{37} 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.\textsuperscript{38}

\textit{B. Trade Agreements}

The NSA programs, and media coverage of them, have further impacted bi- and multi-lateral trade negotiations, undermining U.S. economic security. Consider two of the most important talks currently underway: the Transatlantic Trade and Investment Partnership (TTIP) and the Trans-Pacific Partnership (TPP).

TTIP is a trade and investment negotiation that is being conducted between the European Commission and the United States. The purpose of the agreement is to create better trade relations between the two region, enabling companies on both sides of the Atlantic to thrive. The revelations about NSA activities have had a profound impact on the negotiations.

In March 2014 the European Parliament passed a resolution noting “the impact of mass surveillance.” It stated, “the revelations based on documents leaked by former NSA contractor Edward Snowden put political leaders under the obligation to address the challenges of overseeing and controlling intelligence agencies in surveillance activities and assessing the impact of their activities on fundamental rights and the rule of law in a democratic society.”\textsuperscript{39} It recognized that the programs had undermined

\textsuperscript{34} Gilbert, \textit{supra} note 16.

\textsuperscript{35} \textit{Id.}

\textsuperscript{36} Miller, \textit{supra} note 11.

\textsuperscript{37} \textit{Id.}


“trust between the EU and the US as transatlantic partners.” Not least were concerns that the information could be used for “economic and industrial espionage”—and not merely for the purpose of heading off potentially violent threats. Parliament strongly emphasized, “given the importance of the digital economy in the relationship and in the cause of rebuilding EU-US trust,” that its “consent to the final TTIP agreement could be endangered as long as the blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not completely abandoned and an adequate solution is found for the data privacy rights of EU citizens.” The resolution underscored that any agreement to TTIP would hinge on the protection of the data privacy rights as reflected in the protection of fundamental rights in the EU Charter.40

Even if the surveillance programs do not entirely derail TTIP, they have the potential to significantly retard negotiations.41 Much is at stake. The Center for Economic Policy Research in London, for instance, estimates that a successful TTIP could improve U.S. workers’ wages, provide new jobs, and increase the country’s GDP by $100 billion per year.42 Another study, conducted by the Bertelsmann Foundation, suggests that TTIP “could increase GDP per capita in the United States by 13 percent over the long term.”43 To the extent that the programs weaken the U.S. position in the negotiations, the impact could be significant.44

Although the United States Trade Representative is trying to counter the political fallout from the NSA debacle by putting local data protection initiatives on the table in the TTIP negotiations, the EU has steadfastly resisted any expansion into this realm.

TPP, in turn, is a trade agreement that the United States is negotiating with 11 countries in the Asia-Pacific region (Australia, Brunei Darussalam,
Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam). TPP (with participation of Japan), accounts for nearly 40% of global GDP, about 1/3 of world trade. Two of the United States’ objectives in these negotiations are directly implicated by the Snowden releases: e-commerce / telecommunications, and intellectual property rights.

The NSA programs relate to a number of categories under e-commerce—such as rules preventing discrimination based on the country of origin, and efforts to construct a single, global Internet. Nevertheless, as discussed below, some of the countries involved in TPP have already adopted data localization laws. The NSA programs have thus weakened the United States’ negotiation position in these discussions, by making it more difficult to reach agreement in key areas.

In addition to e-commerce considerations, as part of the TPP negotiations, the United States has prioritized intellectual property rights. Some 40 million American jobs are directly or indirectly tied to “IP-intensive” industries. These jobs tend to be high-paying and stimulate approximately 60% of U.S. merchandise exports, as well as a significant portion of services. Efforts to make progress in TPP by developing stronger protections for patents, trademarks copyrights, and trade secrets—including safeguards against cyber theft of trade secrets—is made more perilous by the existence of the NSA programs.

C. Data Localization and Data Protection

Over the past eighteen months, countries around the world have increasingly adopted data localization laws, restricting the storage, analysis, and transfer of digital information to national borders.45 To some extent, the use of barriers to trade as a means of incubating tech-based industries predated the Snowden releases.46 In the aftermath of the leaks, the dialogue has gained momentum. The asserted purpose is to protect government data and consumer privacy.

As of the time of writing, China, Greece, Malaysia, Russia, South Korea, Venezuela, Vietnam, Iran, and others have already implemented local data server requirements.47 Turkey has introduced new privacy regulations


preventing the transfer of personal data (particularly locational data) overseas. 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. Germany and France are considering a Schengen routing system, retaining as much online data in the European Union as possible.

As a regional matter, the European Union (EU) Commission’s Vice President, Viviane Reding, is pushing for Europe to adopt more expansive privacy laws. In March 2014, the European Parliament passed the Data Protection Regulation and Directive, imposing strict limits on the handling of EU citizens’ data. Reding announced, “The message the European Parliament is sending is unequivocal: This reform is a necessity, and now it is irreversible. Europe’s directly elected parliamentarians have listened to European citizens and European businesses and, with this vote, have made clear that we need a uniform and strong European data protection law, which will... strengthen the protection of our citizens.” 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. Apart
from the new directive, 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. Some 3000 U.S. companies rely on this framework to conduct business with the EU.

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. 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

58. See id.
introduced. Their potential economic impact is substantial. 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.61

The current dialogue is merely the latest in a series of growing concerns about the absence of effective privacy protections within the U.S. legal regime. High tech companies appear to see this as a concern. 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.”62

It is with the impact of lack of privacy controls in the surveillance sphere 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 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.”63 Numerous high technology CEOs supported the initiative, such Google’s Larry Page, Yahoo’s Marissa Mayer, and Facebook’s Mark Zuckerberg.64 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.”65

D. 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.

62. Gustin, supra note 11.
64. Id.
65. Id.
dominance and to have the International Telecommunication Union (ITU), an entity within the UN, become the governing body.\textsuperscript{66} The global backlash against the NSA programs raises question about the future of Internet governance. The revelations have not only contributed further to such calls, but they have spurred increased discussion of the need for regional Internet control.\textsuperscript{67}

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.\textsuperscript{68} 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.\textsuperscript{69} 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 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.\textsuperscript{70} 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 United States 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.\textsuperscript{71}


\textsuperscript{67} See, e.g., ICANN, https://www.icann.org/ (last visited Feb. 18, 2015).


\textsuperscript{69} See, e.g., Amanda Holpuch, \textit{Brazil's Controversial Plan to Extricate the Internet From U.S. Control}, \textsc{The Guardian} (Sept. 20, 2013), http://www.theguardian.com/world/2013/sep/20/brazil-dilma-rousseff-internet-us-control ("Rousseff proposed a set of ambitious, and controversial, measures that include: constructing submarine cables that do not route through the US, building internet exchange points in Brazil, creating an encrypted email service through the state postal service and having Facebook, Google and other companies store data by Brazilians on servers in Brazil.").

\textsuperscript{70} Id.

\textsuperscript{71} Id.
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.”

In the wake of the Snowden documents, ICANN and Brazil have formed an alliance, condemning U.S. actions. Concern about the latest revelations spurred a major conference in April 2014, 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 multi-stakeholder Internet governance.”

It is not clear how the newest shifts will be resolved—either temporarily or in the future. But significant questions have been raised: 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?

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, 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 also the opportunity to submit proposals for contracts for which they previously would have been allowed to compete. The future of Internet governance hangs in the balance.

II. 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.

---

72. Id.
73. Id.
74. 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).
75. Miller, supra note 11.
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 Snowden leaks, 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. 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 in law.\(^{76}\) The 1947 National Security Act, for instance, which, \textit{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.\(^{77}\) 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 purview, who can certify an application to FISC, and under what conditions \textit{in camera} and \textit{ex parte} proceedings can be held.\(^{78}\) 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.\(^{79}\) But no definition is provided in FISA. Nor does the USA PATRIOT Act prove more illuminating—despite referring to national security more than two dozen times.\(^{80}\)

Definitions of national security that are found in the U.S. Code tend to limit consideration to foreign affairs and matters related to military strength.\(^{81}\) Under the Classified Information Procedures Act, “national

---


78. 50 U.S.C. §§ 1803(e), 1804(a), 1806(f), and 1845(f) (2012).

79. 50 USC §1825(b) (2012).


security” is understood as involving matters related to the “national defense and foreign relations of the United States.” 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.83

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.84

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

Executive Branch articulations are similarly unhelpful. President George W. Bush’s five-page National Security Presidential Directive 1 referred to

---

"national security" thirty-three times, without any definition. 85 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. 86 Like the Executive Branch, courts tend to look to the military and diplomatic aspects of national security, instead of their economic concomitant. 87

Despite the lack of emphasis on economic strength in statutory definitions, 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 economic strength, to protect the Union. For Alexander Hamilton, absent military might, diplomatic stature, and commercial success, the country would cease to exist. 88

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 the Attorney General, reflected the purposes for which Union had been sought: foreign relations, military strength, economic growth, and the rule of law. 89 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.” 90

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. 91

88. FEDERALIST No. 1, (Alexander Hamilton).
89. 19 JOURNALS OF THE CONTINENTAL CONGRESS, 1774-1789, at 125-26 (available at http://memory.loc.gov/cgi-bin/ampage?collid=lljc&fileName=019/lljc019.db&recNum=137&itemLink=r%3Fammem%2Fhlaw%3A%40field%28DOCID%2B%40lit%28jc0191%29%29%29%230190001&linkText=1)
91. 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).
History is telling. 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. 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. The 1850 Clayton-Bulwer Treaty ensured that future canal access through Central America would be open to international trade.

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. Upon taking office, President Franklin Pierce reiterated the same policies: of the complicated European tumults and anxieties, the 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. 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.

To the extent that the NSA programs, and public knowledge of them, has harmed the U.S. economy, they have harmed U.S. national security. The country’s economic strength is part of what enables the United States to

respond to external and internal threats. The ability to defend the country against would-be aggressors requires resources—e.g., to build and equip a military force, to move troops, to respond to attacks in whatever form they may materialize. Many of the supplies needed to fend off overreaching by either states or non-state actors derive not from government production, but from the private sector. To the extent that a weak private sector emerges, the government’s ability to respond is harmed.

Beyond this, economic security allows the country the freedom to determine its international and domestic policies on the merits, not on need. Where the United States is in a strong economic position, it is less vulnerable in international negotiations, such as those related to trade. It is also in a politically superior position, where it can use its wealth to accomplish the desired ends.

A strong economy also ensures that citizens have their needs met, with sufficient income levels for housing, food, clothing, and education. This, in turn, generates social and political stability, which allows for the development of communities, which creates greater cohesion among citizens. It also contributes to the evolution of democratic deliberations, reinforcing the rule of law.

Economic security allows for growth and innovation, which is fed by education and opportunity. Innovation, in turn, allows the country to continue to adapt to the evolving environment and international context. There are further considerations. But these suffice to illustrate the importance of economic strength to U.S. national security writ large.

High technology is central to the U.S. economy. A recent study by the Bay Area Economic Council Institute sought to ascertain how important the high tech industry is just for the U.S. labor market. It found that not only are high-tech jobs critical for generating employment in other sectors, but that growth in the high-tech sector has increasingly been happening in areas of great economic and geographic diversity, suggesting that the high-tech industry is not limited to one ethnic, social, or economic strata.

High-technology has been one of the fastest-growing sectors: between 2004 and 2012, the employment growth in high-tech outpaced private sector growth by a ratio of 3:1. Jobs in Science, Technology, Engineering, and Mathematics (STEM) outpaced job gains across all occupations by a ratio of 27:1.98 Employment predictions put the demand for high-tech workers to increase 16.2% 2011 to 2020, with STEM employment increasing 13.3% during the same period.99

99. Id.
The study found that the generation of jobs in high-technology had far-reaching effects. In addition to the income gains generated by innovation, productivity and a global marketplace, high-technology industrial growth generated other types of jobs. Health care, education, law, restaurants, hotels and personal services, as well as goods-producing construction sectors grew in tandem with high tech, largely because of a local multiplier effect: "For each job created in the local high-tech sector," the study concluded, "approximately 4.3 jobs are created in the local non-tradable sector in the long run."

Even as early as 2002, the National Science Foundation found that the global market for high-technology goods is growing at a swifter rate than for other manufactured goods. More than this, "high-technology industries are driving economic growth around the world."

This study built on one released in 1995 by the National Academies, which had looked carefully at the role and importance of high tech companies in the U.S. economy.

Study after study reflects the importance of high-technology in the U.S. economy. In 2015, a Brookings study found that "advanced industries" (which include high-technology, STEM, and industries, like aerospace, which are heavily dependent on advanced technologies), "represent a sizable economic anchor for the U.S. economy." They led the post-recession recovery. Brookings found that with only 9 percent of the total U.S. employment, advanced industries produce some $2.7 trillion per year—around 17% of the country’s GDP. Further, about 60 percent of U.S. exports are tied to this sector, with 2.2 jobs being created domestically for every new advanced industry job. In sum, "Directly and indirectly... the sector supports almost 39 million jobs—nearly one-fourth of all U.S. employment."

What these numbers mean is that hits to high technology directly impact the U.S. economy. The country’s strength relies, in part, on wealth and resources—particularly the production and consumption of goods and services. With the economy so central to U.S. national security, one might...
be forgiven for assuming that economic interests—particularly those that affect significant sectors—are well-represented in the institutional structure that governs national security. Unfortunately, they are not.

B. National Security Infrastructure

The National Security Council ("NSC") is "the principal forum for consideration of national security policy issues requiring Presidential determination." 105 The President looks to the forum for advice and assistance in matters ranging from domestic, foreign and military, to intelligence and economic. 106

It is thus 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. 107 The Chair of the Joint Chiefs of Staff acts as the statutory military advisor, the Director of National Intelligence as the statutory intelligence advisor, and the Director of National Drug Control Policy as the statutory drug control policy advisor. 108

Under PDD-1, the NSC includes the Secretary of Treasury, and "[w]hen 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." 109

When the emphasis 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 issues are not brought directly to the NSC. 110

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 issues may be treated with seriousness,

106. Id.
108. Id.
110. DeRosa, supra note 19.
but they are not meaningfully integrated into the national security infrastructure.

C. Unintended Harmful Consequences

There are various ways in which the NSA's apparent failure to take account of the potential impact of public knowledge of the programs on U.S. industry may have acted to undermine U.S. security beyond weakening the economy. The backlash risks shielding foreign government actions from public scrutiny. It potentially undermines the ability of the United States to develop international norms against ubiquitous surveillance, which can be used for political or economic espionage. And it raises the possibility that the country will lose digital sight of active threats against the United States.

As was previously noted, the data localization movement, given momentum by the NSA revelations, risks the creation of distinct, parallel Internets, which would stifle the free flow of information that connects not just economies, but cultures and people, with potential rollbacks for an increasingly globalized world. This would affect the country's interest in democratic engagement and it would harm the United States' international reach. The creation of national search engines, national email systems, and national social networks, moreover, means that foreign governments will have direct control over electronic communication networks, facilitating censorship and domestic surveillance and limiting outside view of the extent to which such steps are being taken.

When Turkish Prime Minister Recep Erdoğan, for instance, recently tried to shut down Twitter, the international community was immediately put on notice.\[111\] #TwitterisblockedinTurkey #dictatorerdogan, and #occupytwitter quickly moved to popular trending topics internationally.\[112\] The United States, EU, and others formally objected to the action through diplomatic channels. Had Turkey been an isolated network, it may have secretly censored the politically damaging information (in this case, leaks alleging corruption in the Erdoğan government), without generating such immediate, international attention.

Along the same lines, in July 2014 President Vladimir Putin signed a new law requiring Internet companies to store all Russian users' data within domestic borders. Russia's media and parliament members have

---


used Edward Snowden’s leaks about NSA spying to rally support for the new law. The legislation serves to intensify Putin’s control over Internet companies. With internal data centers, it will be easier for the Russian president to enforce censorship policies and to collect information about members of the political opposition. The law could also give Putin an excuse to shut down major social media networks if they fail to comply with the new regulations.

The NSA revelations also have 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. Because of the NSA programs, U.S. objections to China selling surveillance technology to oppressive regimes look rather weak. Post-Snowden, Chinese efforts have become even more public and devastating to U.S. interests.

Since 2005, when President Mahmoud Ahmadinejad first took office, Iran has stated its plan to develop a national Internet network. In the intervening decade, the country has been unable to do so. But in 2014 Iran’s Ministry of Communications and Information Technology announced that China would officially be collaborating with them on the creation of the National Information Network. Part of Iran’s aim has been to develop a system that allows the country to turn off the international components of the Internet, in a way that will enable the government and domestic banking industry to continue to operate. With more than half the population under age 35, Iran has a tech-savvy citizenry, which has, to date, found various ways around government efforts to block


social media and other international sources. It is not clear whether Iran will be able to completely divest itself of access to the world wide web. What is clear is that in a post-Snowden era, their efforts to do so are being facilitated by countries with interests diametrically opposed to the United States.

Online warfare between China and the United States 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. The following month, a security firm, Mandiant, revealed that the Chinese military unit 61398 had stolen data from U.S. companies and agencies. In March 2013 President Obama’s National Security Advisor publicly urged China to reduce its surveillance efforts—after which classified documents leaked to the public demonstrated the extent to which China had infiltrated U.S. government servers. Two months later, the National Security Advisor flew to China to lay the groundwork for a summit, in which cyber surveillance would prove center stage. Two days before the Obama-Xi meeting was scheduled to take place, The Guardian ran the first story on the NSA programs. 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. Although differences may mark the two countries’ approaches (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 the high ground to try to restrict cyber-surveillance.

A final point is worth noting in this context. To the extent that non-U.S. companies are picking up customers and business overseas, the United States’ ability to conduct surveillance may be further harmed—thus going directly to the country’s national security interests. In other words, it may be in the country’s best interests to keep traffic routed through U.S. companies, which would allow the national security infrastructure, with appropriate legal process, to access the information in question.

118. Id.
119. Id.
120. Id.
121. Id.
122. Id.
apparent overreach of the NSA, however, may end up driving much of the traffic elsewhere, making it harder for the United States to obtain the information needed to protect the country against foreign threats.

III. 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 EU. The two entities are not as far apart as the dialogue might lead one to 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 privacy—would allow U.S. industry to argue changed circumstances 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 on how to take on board—and to mitigate—potentially devastating economic consequences of government surveillance efforts.

A. FISA Alterations

In addition to its economic impact, the NSA program relating to telephony metadata runs contrary to Congressional intent in introducing the FISA, contradicts the statutory language, and violates the Fourth Amendment.\(^1\) In 2014, the Privacy and Civil Liberties Oversight Board came to a similar conclusion,\(^2\) as did the President’s own appointed

124. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE
Review Group, charged with considering the telephony metadata collection program, in 2013.\textsuperscript{125}

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."\textsuperscript{126} The alternative approach was to be developed by March 28, 2014. Nine months later, on September 13, 2014, the FISC approved the Department of Justices's ("DOJ") request to extend the program for another 90 days—without any transition program in place. More than a year after the announcement, a new program has yet to be put into place.

The President issued a new presidential directive 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.

As a matter of Section 702 and the interception of international content, PRISM and Upstream collection present global concerns. Neither program has yet to be 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 communications, where the individual is reasonably believed to be located outside the United States, 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.\textsuperscript{127} 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.\textsuperscript{128} His reading stems from a deeply Aristotelian approach: i.e., one that emphasizes membership in the


\textsuperscript{127} Donohue, Section 702, supra note 1.

political community as a concomitant of forming a structure of government.\textsuperscript{129} As members of the polis, U.S. persons, both distributively and collectively, obtain the protections of the Constitution.

Viewed 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."\textsuperscript{130}

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.\textsuperscript{131} 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 massive amounts of U.S. persons' information, including entirely domestic conversations), as a matter of policy, both PRISM and the use of to/from or about Upstream collection 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.

The Obama Administration has begun to take steps to acknowledge the importance of data privacy for European citizens, but its actions have thus far been limited to law enforcement, excluding surveillance conducted for national security purposes. In June 2014, Attorney General Eric Holder announced that, as part of the EU-U.S. Data Protection and Privacy Agreement, the Administration would work with Congress to provide EU citizens the ability to seek redress in U.S. courts where personal data,\textsuperscript{129} ARISTOTLE, POLITICS, bk. I (Benjamin Jowett trans.) (c. 350 B.C.E.), available at http://classics.mit.edu/Aristotle/politics.1.1one.html.\textsuperscript{130} Verdugo-Urquidez, 494 U.S. at 265.\textsuperscript{131} Orin Kerr, The Fourth Amendment and the Global Internet, 67 STAN. L. REV. 285, 308 (2015).
shared with the United States by European countries for law enforcement purposes is subsequently intentionally or willfully disclosed.\textsuperscript{132} The Office of the Director of National Intelligence claims this action as part of the privacy-protective measures implemented in the wake of the Snowden disclosures.\textsuperscript{133} The agreement, however, is limited to information provided by European countries, making it somewhat beside the point. More relevantly, the Administration supported the USA FREEDOM Act, which would have prohibited the bulk collection of telephony metadata under Section 215 of the USA PATRIOT Act (as well as the Pen Registers and Trap and Trace provisions of FISA and National Security Letters, which appear in five parts of the U.S. Code). Congress, however, failed to pass the USA FREEDOM Act. Actions taken with regard to Section 702 have been minimal and generally focused on U.S. persons.

B. Privacy Law Harmonization

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

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.\textsuperscript{134} These documents constitutionally ground two fundamental liberty interests in their respective regions' governing frameworks: (a) the right to


\textsuperscript{133}. Signals Intelligence Reform 2015 Anniversary Report, Office of the Director of National Intelligence, IC ON THE RECORD, available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties ("In furtherance of its commitment to protecting privacy in the law enforcement context, the Administration is working with Members of Congress on legislation to give citizens of designated countries to the right to seek judicial redress for intentional or willful disclosures of protected information, and for refusal to grant access or to rectify any errors in that information.")

\textsuperscript{134}. Compare U.S. CONST., amend. IV ("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.") with Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, available at http://coventions.coe.int/Treaty/en/treaties/html/005.htm ("Everyone has the right to respect for his private and family life, his home and his correspondence.").
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. 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.

As a substantive matter, the two regions have adopted similar provisions. In the EU and the U.S., for instance, heightened protections are provided

135. Compare U.S. Const., amend. IV (“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.”), with Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, available at http://coventions.coe.int/Treaty/en/treaties/html/005.htm (“Everyone has the right to respect for his private and family life, his home and his correspondence.”).


for what is known as personally-identifiable information. 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).

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.

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.

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 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. 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.


144. Compare, e.g., Recitation Nos. 38 (notice) and 41 (right of access), 1995 O.J. (L 281) 31, 35 with Greenwalk & McAskill, supra note 1.

145. Compare, e.g., 1995 O.J. (L 281) 31, 40, 43, (referring specifically to article 14
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 regions differ that could be addressed through legislative reform: 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.146

In contrast, the EU considers that the individual who has provided data to a third party to still have a privacy interest in the information.147 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.148

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.149 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,

---

147. See, e.g., Recitation No. 47, 1995 O.J. (L 281) 31, 36.
suggested that in most criminal investigations, long-term monitoring “impinges on expectations of privacy.” 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 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.

Justice Sotomayor went one step further, calling into question the entire basis for the 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.” 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.

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.”

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

150. Id. at 964 (Alito, J., concurring).
151. Id. at 963 (Alito, J., concurring).
152. Id. at 957 (Sotomayor, J., concurring).
153. Id.
154. Id.
Moreover, 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.

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.

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.\textsuperscript{157} 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.\textsuperscript{158} United States District Judge Lucy Koh determined that the case was too far along to suffer delays.\textsuperscript{159} 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.\textsuperscript{160} The lawsuits, filed in California, Florida, Illinois, Maryland, and Pennsylvania, at great expense, are ongoing.

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 revelations, 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.\textsuperscript{161}

The Safe Harbor provisions, developed from 1999 to 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

\textsuperscript{157} Dan Gillmor, \textit{As We Sweat Government Surveillance, Companies Like Google Collect Our Data}, \textit{THE GUARDIAN} (Apr. 18, 2014), http://www.theguardian.com/commentisfree/2014/apr/18/corporations-google-should-not-sell-customer-data.

\textsuperscript{158} Joffe v. Google, Inc., 746 F.3d 920 (9th Cir. 2013).


\textsuperscript{160} Id.

concerns was the failure of the agreement to provide adequate protections.

In light of the massive data breaches 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 now even less supportive of the Safe Harbor provisions. They amount to a self-regulated scheme in which the U.S. Federal Trade Commission 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.

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 in part because of concern about building a stronger economy to allow the government to fulfill its domestic obligations, and to reassure the international community that the United States 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 moment.

High technology is a vital part of the U.S. economy. It is 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 lose its dominance in the Internet sphere.

To some extent, we do, structurally, pay some attention to the importance of the economy for U.S. national security. But many consequential decisions are not aired in full light of the possible implications for U.S. economic interests. One way Congress could

162. See European Parliament Resolution supra note 39 ("Takes the view that, as under the current circumstances the Safe Harbour principles do not provide adequate protection for EU citizens").
164. See FEDERALIST No. 11 (Alexander Hamilton) ("The speculative trader will at once perceive the force of these observations, and will acknowledge that the aggregate balance of the commerce of the United States would bid fair to be much more favorable than that of the thirteen States without union or with partial unions.").
rectify this would be to take a look at how to integrate economic concerns, as an institutional matter, into the national security infrastructure—and not just at the highest levels, but at a programmatic level, where key decisions about programs are being made.

CONCLUSION

The Snowden documents revealed not just the extent to which high technology companies had been coopted or compromised, but also that the targets of NSA surveillance include allied and non-allied countries. The impact of this information has meant that U.S. companies have lost revenues and experienced declining market share. Simultaneously, the United States’ position in international trade negotiations has been weakened. Public awareness of the NSA programs spurred international efforts to implement data localization. Jurisdictional questions and national borders previously marked the worldwide Internet discussions. But countries began using the NSA programs to justify restricting data storage to national borders, making it more difficult for the United States to gain access. The backlash has led some commentators to raise concern that “the Internet will never be the same.” At risk is the balkanization of the Internet, undermining its traditional culture of open access, and increasing the cost of doing business.

By undermining high technology companies, U.S. economic security—which is central to U.S. national security—is at risk. Part of the problem

26, 2013).


170. Id.
appears to be that the national security institutional structure has failed to adequately reflect the importance of economic concerns. Beyond this, there have been a number of unintended consequences even within spheres traditionally understood as within a national security realm.

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, allowing industry accurately to claim 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.