When Trade and Tech Collide
Digital Policy Challenges and Solutions for 2016 and Beyond

Claude Barfield

AEI

AEI Technology Policy Working Paper 2015-01
October 2015
INTRODUCTION AND THEMES

The American Enterprise Institute has undertaken a two-year research project to develop a Global Internet Strategy (GIS) for the United States. The GIS project is designed both to frame the overall debate about America’s role in cyberspace and to put forward specific recommendations in key cyber policy areas for consideration and adoption by Congress and the next presidential administration. The project will focus on four main issue areas: economics, trade, and international development; cybersecurity and national defense; Internet freedom and civil liberties; and network and data integrity.

This paper is intended to provide detailed background analysis and policy recommendations for the area of economics and trade. It will be bound, however, by the broad objectives that underpin the other GIS program goals, such as protecting and promoting freedom of expression and combating fragmentation of the Internet, safeguarding national security interests, and defending a multistakeholder model of Internet governance.

The opening sections of the paper will pull together the most recent data on the role of the Internet in the global economy, including statistics on data flows, the role of high-tech companies in national economies, and the increasing centrality of digital-based operations and business models on national manufacturing and service sectors. It will place particular emphasis on the competitive strengths and challenges for US firms.

The section will also describe the impact of the emerging digital economy on traditional trade and investment flows, as well as the role of the Internet in both enhancing and even creating new supply chains, in which intermediate goods and services cross and re-cross national boundaries in the development of final goods and services.

The following sections will move to analyses of the major barriers to digital trade, including straightforward market access barriers, as well as such protectionist policies as data localization, local content requirements, and discriminatory standards. These sections of the paper will have two goals: (1) analyzing the negative economic consequences to digital trade from such market access restrictions, both from the perspective of the home country and from the perspective of foreign ICT companies; and (2) evaluating proposals advanced by the United States and its trading partners according to a set of free market/free trade principles.
The analysis next will take up the complex issues that stem from intersections between trade and investment policy and privacy and security imperatives. Three issues will receive extended treatment: the standoff between the United States and Europe over data protection and the Safe Harbor agreement; the controversy over encryption, and Europe’s attempt to assert worldwide control over its parochial interpretation of the “right to be forgotten.” On data privacy, a recent decision by the European Court of Justice (ECJ) striking down the current Safe Harbor agreement between the US and EU have produced an instant crisis. The paper will trace the history of the conflict, the implications of the ECJ ruling and lay out recommendations for a US response. The debate over new, impenetrable encryption technologies is largely an internal one thus far, pitting US high-tech companies and privacy advocates against US law enforcement officials. The paper will detail the tradeoffs and dilemmas facing both the government and the private sector, and explore the pros and cons of technological solutions that have been advanced over the past year.

The paper will then turn to a new frontier for digital policy: the complicated connections between traditional espionage (carried out by the US, its allies, and opponents with equal fervor) and the poorly defined and dimly understood area of economic espionage. Recently, the focus has been on China, but a number of nations, including the Russian, French, and Israelis, are also adept at these practices. The paper will explore in some detail the US position regarding economic espionage—that economic spying is within bounds so long as it does not entail passing along such information to aid domestic companies. How likely is it that other nations will adhere to this distinction? What are the boundaries between traditional espionage and newer forms of economic espionage?

Whatever the case, the contention of this exercise is that the United States, in conjunction with other nations (including the Chinese) must quickly turn to the task of establishing common definitions and rules for economic espionage. It has been suggested that such rules should be included in the disciplines of the World Trade Organization. Our analysis will discuss the difficulties and challenges of this and other options, but it will conclude that it is by no means clear that any current international legal system is adequate—and that new rules and obligations are likely to be needed, through future international negotiations.
This leads finally to an assessment of current negotiations for new digital trade rules: the Trans-Pacific Partnership Agreement, the Trans-Atlantic Partnership Agreement, and the WTO Trade in Services Agreement. The paper will conclude with a description and analysis of the state of play in all three negotiating platforms. Particular attention will be focused on the recently completed TPP agreement, for which details are just emerging as this working paper is being completed.

PART I: BACKGROUND: THE INTERNET, ECONOMICS, AND TRADE

1.1. THE IMPACT OF THE INTERNET ON THE GLOBAL ECONOMY

The astonishing growth of the Internet has sent both economists and policymakers scrambling to refine economic analyses and policy agendas to match and facilitate the spillover effects of broadband technologies on national economies. In 2015, 3.2 billion people have access to the Internet,¹ and the international community is working to increase this number to at least 4.5 billion by 2020.² The growth is being fueled in large part by two factors: more users and faster, more ubiquitous access. Broadening access, particularly via smartphones and other mobile devices, and the popularity of social media is further compounding the Internet’s growth and impact.³

The digital economy is no longer confined to the information technology sector but has become economy-wide, as manufacturing and service industries increasingly have become digitalized. The Internet provides huge new opportunities to access distant markets, but it is also the source of enhanced productivity within companies and across supply chains. E-commerce and the Internet have paved the way for entirely new business models and have spawned many of the world’s most innovative companies. These include Facebook and Twitter, the progenitors of social networking; Amazon, Apple, and Alibaba, which have utilized the Internet to generate e-commerce and connect buyers with sellers around the globe; and Google, which has become the default search engine for much of the world. Further, the digitization of products such as books,

---

music, movies, medical equipment, and services such as transportation modes (taxis), health care, and education have generated more efficient and innovative business opportunities.\textsuperscript{4}

Economists are just beginning to model and estimate the impact of the Internet on national productivity and growth. Though preliminary studies are likely to be continually revised in the future, most point in the same positive direction. For instance, a recent World Bank study found that a 10 percent increase in broadband penetration resulted in a 1.38 percent increase in growth in developing countries and a 1.21 percent increase in growth in developed economies.\textsuperscript{5} A McKinsey Global Institute report concluded that from 2004 to 2009 the Internet contributed up to 21 percent to GDP growth in the developed world and 11 percent in the BRIC nations (Brazil, Russia, India, and China).\textsuperscript{6}

The Internet’s impact on the global economy is multifaceted. In this paper, we will explore the impact of the network on productivity and labor markets, and the special role it plays in small and medium-sized companies and in the developing world.

1.1.1. PRODUCTIVITY GAINS

Economic growth is ultimately dependent on increasing productivity, and the Internet enhances productivity growth potential through a number of paths. Broadband services can increase the efficiency of the production process through cheap and real-time communication between parts suppliers and the home office. This allows tighter management of the production chain, as disparate elements of the chain can be accessed simultaneously and updated as necessary. Cloud computing allows many internal company functions—accounting, legal, human resources—to be outsourced more cheaply and with less hassle. Finally, cloud computing allows instant communication with suppliers and customers, allowing quick responses to changing customer requirements and needs. And it can provide opportunities to introduce more cost effective means

\textsuperscript{4} European Centre For International Political Economy, “The Economic Importance of Getting Data Protection Right,”
\texttt{www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf}


of delivery to customers, by end-to-end tracking of both parts and end products, and generally managing the logistics of the supply and customer chains.

Summing up, a recent United States International Trade Commission (USITC) report concluded that the Internet produces gains of 7.8–10.9 percent in the productivity of digitally intensive industries. For the United States, the same report estimates that digital trade has accounted for an increase of US GDP by 3.4 to 4.5 percent and created some 2.4 million jobs.\(^7\)

1.1.2. LABOR MARKETS

The Internet is a powerful catalyst for job creation. While some jobs have in fact been destroyed by the emergence of the Internet, a detailed analysis of the French economy showed that while the Internet eliminated 500,000 jobs over the past 15 years, it generated 1.2 million others, a net addition of 700,000 jobs (or 2.4 jobs created for every job destroyed). Similar results came out of McKinsey’s global SME survey, which found that 2.6 jobs were created for every 1 destroyed. In addition, companies that fully integrate Internet technology and use it extensively create more than twice as many jobs as the average. For companies that use it sparingly or not at all, the Internet has a neutral to slightly negative effect.\(^8\)

1.1.3. SMES AND DEVELOPING ECONOMIES

Special note should be taken of the outsized impact of the Internet and broadband services on two very different constituencies: small and medium-sized businesses (SMEs) and (with some overlap) developing economies.

SMEs. The Internet has become the central factor in the ability of SMEs around the world to compete in the international marketplace. The health and growth of SMEs is vitally important to the health of and job growth in national economies, particularly for developing countries where they are the main driver of job creation. A recent World Bank study across some 104 countries


concluded that SMEs were the biggest contributors to employment, being responsible for 56 percent of permanent full-time employment and 88 percent of new jobs in low-income countries.9

Establishment of secure websites allows SMEs entrance to worldwide markets without the necessity and expense of a physical presence. The use of broadband Internet services provides SMEs expertise to overcome challenges in financing, legal aid, and advertising. Strategic use of the Internet also provides SMEs with strategic market information regarding potential business opportunities in foreign lands, as well as the insights into specific national consumer tastes and needs. Access to cloud computing can level the playing field with larger corporations by reducing IT infrastructure costs in managing internal networks as well as regional or global supply chains.

The Developing World. Today, some 4.5 billion people in the developing world are still not connected to the Internet. Most of them, however live within areas covered by 2G or 3G mobile access.10 Mobile broadband will therefore be key to getting people online, but greater mobile penetration will depend on handset costs continuing to fall and the ability of users to become digitally literate.

Research by the Boston Consulting Group shows that people in emerging economies are more frequent and active users of online government services than those in developed countries. People in emerging economies are also particularly heavy users of services with social benefits, such as those related to health care and education.11

Connectivity is the operative factor for developing countries. And increasingly the Internet, sometimes delivered by traditional landline networks but more often now over mobile devices and wireless networks, has become the essential platform. Through this platform, citizens of

---

developing countries, as noted above, have gained access to health information and more secure financial services.

In many developing countries, agriculture employs some 40 percent of the workforce. Through mobile devices, a number of farmers and cooperatives in South America and Africa are accessing services that provide weather information and prediction, analysis of current and future crop prices, and technical expertise. This Internet potential for farmers in the developing world is just beginning to be realized, but one study has suggested that greater real-time information about trends in crop prices could increase farmers’ income by more than 20 percent.\(^\text{12}\)

### 1.2. THE INTERNET AND INTERNATIONAL TRADE

Over the past three decades, advances in communications technology and transportation have revolutionized international trade operations and patterns. And in the past decade, the arrival of the Internet as a powerful technological instrument and facilitator for trade and investment has further spawned new trade patterns and international business models. While traditional product-level competition between nations remains an important component of international commerce (new Fords versus new Toyotas), multinational supply chains increasingly characterize a sizable element of trade flows.

Though possibly overutilized, the iPhone supply chain still best symbolizes the nature and reality of the new trade paradigm. The brains of the iPhone are designed by Apple, but hundreds of components are designed and manufactured by numerous companies in nations around the world, from Asia (South Korea, Thailand, Japan, and Taiwan, among others) and Europe (France and Italy) to companies in the US (Hewlett Packard and Intel, among others). Parts and components often cross borders several times as companies refine basic designs and contribute more added value. Finally, much of the final product is assembled in China.

---

For this report, the point is that only a sophisticated mastery of the Internet and advanced broadband services can allow companies to meet the challenges of just-in-time design and manufacturing. Cross-border data flows are central to efficient supply chains.

These new supply chain models have also created an ever-larger demand for data-driven services. As noted above, this begins internally as multinational firms must establish electronic systems for financial, legal, and human resources to manage both domestic and foreign growth. Further, worldwide sales of iPhones and other products necessitates distribution, transportation, and facility management systems, as well as cross-border financial and distribution arrangements—all dependent on real-time cross-border data flows.

Additionally, the Internet can make supply chain management and product delivery cheaper and quicker. Online communications with buyers and parts suppliers is one path. Further, where delivery of a product or service online is possible there is the avoidance of customs or transportation costs. The USITC has estimated that the Internet can reduce trade costs by an average of 26 percent.13

With this image of the Internet’s impact on trade and the global economy, we turn to the challenges facing this new paradigm.

**PART II: DIGITAL TRADE UNDER THREAT**

As the opening sections of this paper have demonstrated, digital technologies are producing momentous changes in the social and economic fabric of national economies and, ultimately, the world economy. Our concepts of space and time have been profoundly impacted. Yet it is also true that national and global regulatory laws and practices remain far behind the realities of the new real-time nature of both private and public activities. Thus, a central task for national and international policymakers is to identify obstacles to the emergent open and competitive Internet that can continue to empower citizens, enable entrepreneurs, and promote prosperity.

---

2.1 BARRIERS TO DATA FLOWS ON THE INTERNET

A free flow of data has been vital for the growth and usefulness of today’s Internet. Now, however, data flows are under threat from being restricted, rerouted, or stopped altogether. Barriers to data flows come in many different forms. This paper will discuss general market access barriers, data localization mandates, local content requirements, and required transfer of intellectual property.

2.1.1. DATA ACCESS BARRIERS, LOCALIZATION MANDATES, AND IP TRANSFERS

General Market Access Barriers. Though there are barriers specific to digital trade, digital commerce is impacted by market access barriers common to many goods and services sectors. For instance, customs duties and rules can be manipulated to fend off foreign competition, in the form of either discriminatory duties or opaque regulations. Some countries demand a local presence for service providers or require a local partner. Others legislate unique national standards and make little or no provision for regulatory due process.

Data Localization. Companies make localization decisions based on a number of criteria, including cost optimization, local resources, distance to consumers, and so forth. However, distinguished from these competitive reasons for data or server localization, governments often intervene with localization requirements that impede or directly thwart optimal business decisions.

Data localization measures broadly require companies to conduct digital activities within a country’s borders. In the inclusive definition utilized by the Office of the United States Trade Representative (USTR), localization barriers to trade are defined as measures “designed to protect, favor, or stimulate domestic industries, service providers, and/or intellectual property (IP) at the expense of goods, services, or IP from other countries. Localization barriers are
measures that can serve as disguised trade barriers when they unreasonably differentiate between domestic and foreign products, services, IP, or suppliers.”

Publicly mandated localization decisions can take a variety of forms. First, a number of countries either explicitly or implicitly require local or domestic data storage. Among the countries with such laws are Argentina, Australia, Canada, China, Greece, Venezuela, and Indonesia. Alongside these general localization measures, some countries justify restrictions for particular reasons. For instance, a number of countries (like Argentina, Venezuela, and China) require local data servers for data on financial transactions as a complement to regulatory regimes. Others, such as Indonesia, require explicit approval before moving financial data offshore. Medical and health records provide other examples of intrusive data protection laws in the name of prudential regulations. For instance, Canada and Australia have legislated blanket bans on moving certain health data out of the country. In contrast, the US has created a regulatory framework that allows free movement of personal medical data, provided certain administrative and technical safeguards are provided. (The US approach has been called a risk-based approach, while the Canadian and Australian regimes are blanket locality-based approaches.)

Local content requirements. These requirements constitute another important barrier, and they are the most rapidly growing trade-distorting data protection policy. Local content mandates require that a certain percentage of a good or service be produced locally. For all trading sectors, it has been estimated that in 2010, some 5 percent of global goods and services trade has been affected by local content requirements—almost a trillion dollars out of more than $18 trillion of total global trade in goods and services. Many local content requirements are economy-wide and affect both public and private procurement contracts. Other relate specifically to information and communications sectors. India, for instance, requires that foreign companies incorporate 25–40 percent local content as a condition of servicing that country’s information technology

14 Office of the United States Trade Representative, “Localization Barriers to Trade,” http://ustr.gov/trade-topics/localization-barriers
16 Ibid., 5-5
17 Ibid., 5-4
market. Further, in other countries, local content mandates require local content production of a good or service as a condition of market entry by foreign corporations. The most harmful trade-distorting mandates require the use of local data centers for digital services such as Internet searches. Some two dozen countries have introduced data center requirements.\textsuperscript{20}

Supplementing the direct local content requirement, a number of nations have legislated preferences for domestic companies in public procurements of information and computer technology. These can take the form of price breaks for local digital firms or local standard idiosyncrasies. Among the economies that favor local companies through some means are Brazil, Canada, China, India, Nigeria, Paraguay, and Venezuela.\textsuperscript{21}

Transfer of intellectual property. Finally, certain countries require that a foreign enterprise transfer intellectual property or technology as a condition for doing business in a country. China stands out in this regard, with multiple examples of forced—or attempted—cases where sharing elements of software or hardware have been demanded as a prior requirement to enter or to continue to complete in the local market.\textsuperscript{22}

\section*{2.1.2. THE CASE AGAINST LOCALIZATION BARRIERS}

The negative economic impact of data flow barriers can not only harm competing foreign corporations, but also companies in the home market. Further, the negative impact can also produce system wide effects that damage the global Internet.

A number of countries have been falsely lured into technology/industrial policies to advance the fortunes of their ICT companies over those of foreign competitors. Rarely have these protected markets succeeded in delivering globally competitive national champions. The downsides are significant. First, by prohibiting or severely limiting market access to foreign firms, governments are simultaneously robbing domestic firms of the best technological input. This particularly negatively impacts small and medium-sized firms that would be cut off from cheap and advanced

\textsuperscript{20}Ibid, 3.
Internet services available from multinational firms. The negative effects will be widely felt; also, nontech firms will face higher local costs and less advanced communications services.

The issue is especially acute for the developing world. A recent Deloitte study has concluded that expanding Internet access to the 4 billion people in developing countries to the levels of developed countries would increase productivity by 25 percent, add $2.2 trillion to their collected GDP, and increase GDP growth by more than 70 percent.23

Data localization, over the long run, will also adversely affect both Internet productivity and world innovation. Without dipping too far into economic theory, it can be noted that Internet productivity is intimately connected to the so-called “network effect,” which holds that productivity and the value of the platform is proportional to the number of users on the system. The more people that use email, for example, the more valuable email becomes. By limiting national users, data localization will raise costs overall and dampen the innovative impact of networks.24

Beyond this, data localization measures will ultimately negatively impact ICT and other high-tech industries, such as pharmaceuticals and aerospace. These high-tech sectors are characterized by the high fixed costs of R&D and design combined with relatively lower marginal production costs. They need economies of scale to cover these fixed initial costs. This necessitates cheap and efficient cross-border flows, both within the corporate structure and with outside parts and components suppliers. Pressure to remain within small fixed boundaries will inevitably result in higher product and services costs and a less efficient supply chain.25

2.1.3. US GOVERNMENT ACTION

Clearly, with US multinational ICT companies standing at the technological frontiers of international competition, it is in America’s interest to push back against digital protectionism

and a fragmentation of a free and open Internet. As noted above, data localization and fragmentation requirements can take many forms. The United States government has already initiated efforts to combat the growing threats to open competition and the free flow of data. These are commendable, but it is time for both the president and Congress to take steps to raise digital trade issues to the highest priority—and to make clear to our trading (and security) partners that we intend to defend our interests and companies against discriminatory regulations and domestic favoritism through local subsidies or technology transfer blackmail.

These digital strategies must become the top goals in the multiple trade negotiations described later in this report. But the White House, along with the most relevant federal agencies—USTR and the Commerce and State Departments—should also pursue US cyber economy goals through a myriad of diplomatic and commercial fora and within all relevant international organizations such as the World Bank and the OECD.

US demands must be tempered with sensitivity to legitimate government restrictions to safeguard privacy or to prevent access to morally offensive content such as child pornography. Within this protective framework, however, the US must be on guard that allegedly high moral purposes are not covers for market exclusion. Actually, many of the more egregious protections are rather straightforward: it should not be difficult for US negotiators to identify and push back against laws and regulations that require local data storage, a local partner, or the transfer of cutting-edge technology. National champions cannot hide, and though it is not within the power of the US to dismantle them, we can demand that WTO rules for nondiscrimination and equal treatment be enforced to provide a level competitive playing field.

2.2. THE SNOWDEN IMPACT

This report is not the place to deal with some of the most difficult questions flowing from the massive document theft engineered by Edward Snowden in 2013 and then made public in strategic press leaks over the past two years. Whether Snowden is a hero or a traitor (or both) will be left to others to decide. What is, however, very much of profound relevance and concern is the impact of post-Snowden cybersecurity policies on the competitiveness of US global firms, and the challenges to US trade and diplomatic relations with key allies.
Upfront, two results are clear: (1) though the market share and dollar costs of the Snowden revelations cannot be precisely measured at this point, the consensus among government officials and industry is that it is substantial—and ongoing; and (2) the backlash against the Snowden documents has produced a continuing rift between the US government and US high-tech companies over the proper responses to both Snowden and to the larger balance between national security imperatives and privacy and security for individual and private-sector data.

The most damaging programs uncovered by Snowden and his media allies were PRISM, which allows the NSA access to data on many online services without a warrant; Heartbleed, which seemed to show that US security agencies had exploited utilized hidden software flaws without notifying the firms in question; and BULLRUN, through which the NSA attempted to undermine encryption standards to make penetration of online data quicker and easier.\(^{26}\) The PRISM documents revealed that—willingly or not—almost a dozen leading US high-tech companies had cooperated with the NSA, with the bulk of material coming from Yahoo, Microsoft, and Google.\(^{27}\)

Since 2013, projections of the economic impact of the Snowden revelations on US firms have varied widely and have been often revised. For instance, Forrester Research, a well-known technology research firm, first set the cost at $180 billion, but later revised this estimate down to $47 billion for cloud computing and outsourcing providers.\(^{28}\) Recently, the Information Technology and Innovation Foundation has put the price between $21.5 and $35 billion, though it argues that this estimate will grow in the future as US firms continue to be hammered by the international backlash.\(^{29}\)

---

But some experts believe that the negative economic impacts are overstated. In response to a Reuters’ inquiry, a leading trade association executive stated early on: “I know you want sectors and numbers but I don’t have it.”\(^{30}\) Still, while the exact total costs may be cloudy, in the two years since the Snowden revelations, there has been ample anecdotal evidence of the costs to individual companies. In Germany, public-private Deutsche Telecom has openly warned German Internet users against US companies and touted its own “defenses” against international incursions; similarly, Swisscom, a public/private Internet provider, has pushed the “Swiss Cloud” as an alternative to global—and allegedly insecure—US companies.\(^{31}\) Verizon lost several contracts with the German government, which gave as an excuse the lack of defense against US government data demands.\(^{32}\) The Brazilian government withdrew an almost certain defense contract from Boeing, citing fears of NSA connections.\(^{33}\)

The greatest fallout has come in China, where the government took the opportunity to introduce a number of protectionist measures in the name of security. Immediately after the first Snowden documents were published, Chinese official media began a campaign to “de-Cisco” the Chinese economy.\(^{34}\) This was followed by the accusation that major US technology firms were actually “guardian warriors” for the US spy agencies. The “guardian warriors” list included the cream of US technology firms operating in China: Apple, Cisco, IBM, Microsoft, Oracle, and Qualcomm.\(^{35}\) Cisco, which had long provided backbone hardware to Chinese local governments and companies, was particularly hard hit and saw its revenues in China fall dramatically during 2013 and 2014.\(^{36}\)


\(^{34}\) Shannon Tiezzi, “Why Snowden’s Revelations Were a Win for China,” The Diplomat, January 9, 2014, thediplomat.com/2014/01/why-snowdens-revelations-were-a-win-for-china/


\(^{36}\) Jack Clark, “BIG Trouble in BIG China: Cisco Shares Fall off a Cliff as CEO Warns of Slump,” The Register, November 13, 2014, www.theregister.co.uk/2013/11/13/cisco_earnings_asia_problem/
Beijing also attempted to force companies that sell equipment to Chinese banks to fork over secret source code. More broadly, Beijing used the Snowden revelations as one excuse to step up a major effort of “indigenous innovation,” which included fostering and protecting high-tech information technology and Internet sectors. And in the past few months it has introduced a cybersecurity law that contains sweeping new restrictions and mandates on foreign companies (see below).

2.3 PRIVACY PROTECTION

The evolving relationship between the European Union and the United States provides excellent means of analyzing negotiations between two large economies over the rules for data flows, particularly personal information, in light of differing attitudes and regulations toward data privacy.

2.3.1. THE EU DATA PROTECTION DIRECTIVE AND THE SAFE HARBOR AGREEMENT

The 1995 Data Protection Directive codified EU principles in relations to rights of data privacy. Briefly explained, it gave legal protection to a group of privacy principles, including consent for the data collection and public disclosure of any personal data collected, disclosure as to who is collecting the data, access to information about the data being collected and opportunity to correct inaccuracies, guaranteed security for any data collected, and accountability for the data collectors. The directive also contained rules for transfer of data to third parties (countries), which mandated a high level of data protection. Exceptions were allowed if the controller (collector of the data) could guarantee compliance with EU data protection rules. The European Commission, along with the European Council of State, and the European Parliament are currently going through the extended process of updating the 1995 directive.

The United States has no legislation comparable to the EU directive; rather, it relies on an ad hoc approach in which certain sectors have been singled out for special attention, namely the Video Privacy Protection Act and the Fair Credit Reporting Act. Beyond this, Americans depend on the sweeping protections afforded under the First Amendment guarantee of free speech. Thus, after the EU directive was passed, the US and the EU negotiated a so-called Safe Harbor agreement. Under Safe Harbor, US companies certify that they meet the privacy obligations prescribed in the 1995 directive. These include notice to individuals that data are being collected, an option for the individual to opt out of the data collection effort, certification that data are transferred only to third parties that also abide by the Safe Harbor rules, adequate data security, access to individuals who can see and correct data if necessary, and proof of effective enforcement of the rules.

Though there were periodic complaints that US companies were not living up to the letter of Safe Harbor mandates, it was only with the revelations that poured out of the purloined Snowden NSA documents that European leaders became alarmed and pressure rose either for the Safe Harbor agreement to be scuttled or for stricter oversight and supervision—and new rules—to be instituted or promulgated. In terms of the EU data protection rules, specifically, publication of the details of the NSA’s PRISM program—whereby US telecoms firms were forced to share data with the security agencies—caused a huge backlash from the European public, as well as EU political leaders.39

Even before Snowden, the EU had begun working on a revision of the 1995 directive. In the aftermath of these revelations, work on this revision gained greater urgency—though the tripartite exercise described above has still proceeded slowly. In addition to this effort, the EU demanded that the US enter into negotiations to update the existing Safe Harbor agreement, to take into account programs such as PRISM and to limit future data exchanges of the personal data of EU citizens between US private companies and the NSA.

On October 8, the European Court of Justice (ECJ) ruled that the Safe Harbor framework that permits US companies in to the EU to transfer data to the US is invalid. Leaning heavily on the Snowden disclosures, the court ruled that EU citizens were not adequately protected as

mandated by the European privacy laws and principles. The court also ruled that individual EU member states could investigate and rule on privacy complaints from their citizens.  

US government officials quickly condemned the ECJ ruling as out of date regarding US privacy and security laws (particularly since the passage of the USA Freedom Act in Summer 2015). The Department of Commerce criticized the ECJ for needlessly introducing “significant uncertainty” for businesses on both side of the Atlantic. It was pointed out that more than 4,000 US businesses operated under the existing Safe Harbor agreement.

US officials also were quick to point to a newly enacted French law that will allow authorities to spy on digital and mobile phone communications of anyone linked to a “terrorist” organization without authorization from a judge. The law forces Internet service providers and phone companies to give up their data upon request. Finally, the legislation permits French intelligence services to vacuum up data for analysis. The metadata would be anonymous, but intelligence officials could then dig deeper upon permission from an independent panel. This goes far beyond the much-criticized US PRISM program.

The ECJ ruling will have enormous disruptive effects on data flows between the United States and Europe. Even before the decision, however, the US Department of Commerce and EU officials were deeply involved in updating the existing Safe Harbor agreement—and according to press reports, are close to concluding the negotiations. In light of the gravity of the economic consequences of failure, the White House should make it clear to top European officials that it expects both an expeditious and flexible result. Ultimately, the best long-term solution might well be to include provisions regarding Safe Harbor in the proposed US-EU free trade agreement, whose chapters will be legally binding.

---


2.3.2. THE RIGHT TO BE FORGOTTEN

Among the principles included in the 1995 EU directive was the right of EU citizens to have access to any information collected on them and to correct mistakes or flag out-of-date material. In recent years, this individual right has been expanded by European courts and governments in ways that threaten the credibility and integrity of information on the Internet.

In 2014, the European Court of Justice (ECJ) ruled that individuals had the right to demand that links on the Internet with information about themselves be removed from search engines—even if the information was accurate.44 This comes under the doctrine of the “right to be forgotten”—or more accurately, the “right to delist.”

A US corporation, Google, controls some 80 percent of the European market for Internet search, and EU officials forced the company to spend millions of dollars and untold manpower to comply with the new ruling. It thus forced on a private corporation the responsibility of deciding which requests for data removal were valid under the court’s ruling—with little or no guidance from the EU officials. Google Chairman Eric Schmidt protested strongly that the company “didn’t ask to be the decision maker” for the regulations; but by the end of 2014, Google had complied with 41 percent of requests to remove links (208,000 of 503,000 links) under the “right to be forgotten.”45

In July 2015, Europe raised the stakes and the challenges on the “right to be forgotten” once more. While Google had dutifully removed information from all European links, CNIL, France’s data protection authority, now demanded that Google remove the links from it search engines on a worldwide basis. It argued, “In order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing.”46 In effect, the French government, extrapolating from the ECJ decision, is mandating that a US-based multinational company follow the extraterritorial dictates of a

national regulator on a worldwide basis. Failure to comply would result in a fine of about $375,000.47

Google has strongly resisted the French demands. In a blog post, Google Global Privacy Counsel Peter Fleischer stated: “We believe that no one country should have the authority to control what content someone in a second country can access. . . . As a matter of principle, therefore, we respectfully disagree with the CNIL’s assertion of global authority.”48

The European action has triggered similar pressure in the United States. A US nonprofit organization, Consumer Watchdog, has petitioned the Federal Trade Commission (FTC) to mandate that Google allow US citizens the same “right to be forgotten” that is now the law in Europe. This would be a very bad result, as a probing editorial in the Washington Post points out. Under the title “Americans Shouldn’t Demand a ‘Right to Be Forgotten’ Online,” the Post pilloried arguments in favor of the right to be forgotten.49 It noted first that the US First Amendment to the Constitution would preclude a total removal, though the FTC might restrict some information or make it harder to locate. And it warned that companies such as Google might well in the future decide that “carefully evaluating delisting requests isn’t worth the time” and just comply totally. The Post concluded that the FTC should refuse to intervene and thus avoid “starting down the road of stifling the Internet’s remarkably free flow of information.”50

2.3.3. US GOVERNMENT ACTION

Thus far, the Obama administration has been conspicuously silent on issues of privacy and international relations. That should end. There are a number of avenues for the president and his team to take action.

First, the United States and the EU are negotiating the US-EU Transatlantic Trade and Investment Partnership (TTIP) agreement, which will include so-called 21st-century provisions

50 Ibid.
for data flows and Internet regulation. Europe’s “right to be forgotten” directly flouts principles
of free trade in data, as well as in other goods and services. US negotiators should introduce this
issue into the ongoing talks, with the stipulation that, at a minimum, Europe’s attempt to force a
worldwide delisting of information would not be allowed. In addition, since the TTIP
negotiations are likely to stretch out over some years, the Obama administration should
immediately initiate bilateral negotiations on this issue. These could be directed on the US side
by the US Trade Representative or the Secretary of Commerce.

2.4. ENCRYPTION

Nowhere is the rift between the Obama administration and the high-tech sector starker than in
the ongoing battle over encryption. Companies such as Apple and Google, labeled as abettors of
terrorists and sex offenders, echo Pogo’s famous lament: “We have met the enemy and he is us.”
To review, standoffs between the federal government and the US ICT sectors are not new. In the
1990s, the Clinton administration attempted to force telecommunications companies with strong
encryption systems to retain a copy of the keys necessary to decrypt information (the Clipper
Chip, as it was called) and turn it over to law enforcement officials upon legal authorization. The
companies strongly—and successfully—resisted these proposals on the grounds of the enormous
expense and the risk that the “bad guys” would also be able to obtain the keys and thus access
private information. 51

The current battle stems from the decision by Apple, followed quickly by Google and then
makers of standalone apps such as WhatsApp and Signal, to introduce sophisticated end-to-end
encryption software. 52 In the case of the iPhone, for instance, this would allow only the user—
and no outside individual, public official, or even Apple itself, to obtain the code to unlock the
device. 53 (The encryption methodology itself was not new, but before users had been forced to

51 Harold Abelson et al., “Keys under Doormats: Mandating Insecurity by Requiring Government Access to All
Data and Communications,” Massachusetts Institute of Technology, July 6, 2015,
following-google-apple
go through complicated process to encrypt their phones). The companies were driven to this technological fix by the Snowden revelations and the drumfire of charges they had endured from their competitors and the resulting lack of trust by consumers.

Led by FBI Director James Comey, US security and law enforcement officials immediately registered their strong opposition to the new private sector encryption software and devices. In numerous appearances over the past year—CBS’s 60 Minutes, speeches at think tanks including the Brookings Institution, and testimony before a congressional committee—Comey has attempted to make the case against the new encryption software and devices now in circulation. He verbally indicted “companies marketing something expressly to allow people to place themselves beyond the law.”

Comey is an able and savvy public servant, but to a great degree his arguments have been undercut by confounding technological realities. Over the past year, neither Comey nor other security officials have been able to get beyond two hurdles to decrypting devices for public law enforcement officials. The first, presented in great detail several months ago by a top-flight group of cryptographers (the so-called “MIT paper”), is that the introduction of one or more source keys would greatly increase the opportunities for other hackers or foreign government agencies to also penetrate the phone defenses. And second, Apple, Google, and other affected US companies are worldwide competitors. If the US government were to mandate backdoors, other governments—not least the Chinese and Russians—would certainly make the same demands.

Though it occurred some months ago, Comey’s Brookings speech still fairly reflects the state of play, or state of confusion. When asked how one could decrypt the phones without creating large technical vulnerabilities, he replied, “I don’t think I’m smart enough to give you a highly reliable answer there.” He stated that the government was not seeking backdoors, but could not explain how an upfront design would not produce the same security risks. He was adamant that the FBI was not seeking a “universal key,” but could not explain whether this would result in multiple keys for differing phone models or whether companies would end up with “NSA-ready” phones in the US and different versions for international sales. And when asked about the implications

for similar decryption demands from China or Russia, he simply noted: “That’s a good question. . . . It’s something I’ve thought about, but frankly, not well enough to give you an intelligent answer at this point.” Still, in the end, he warned: “We may get . . . to a place where the [US], through its Congress, says you know what? We need to force this on American companies and maybe they’ll take a hit. . . . [But] we as a society are willing to have American companies take that hit.”

Comey and other administration officials have also tried to be conciliatory. In the above-cited speech, the FBI director praised the patriotism of US technology companies, stating that Apple and Google “are run by good people who care deeply about public safety and national security.”

In recent months, the Obama administration has met with the private sector to seek accommodation—including several high-level White House meetings and a Silicon Valley summit. But the standoff continues, and Silicon Valley corporate leaders remain opposed and even defiant against weakened encryption. Apple’s CEO Tim Cook called the FBI demands “incredibly dangerous” and “another attack on our civil liberties.” He further stated that Apple has “never worked with any government agency from any country to create a backdoor. . . . And we never will.” And Google Chairman Eric Schmidt has charged that on encryption, law enforcement and security officials have only themselves to blame, as it was their practices that brought about the push for encryption. In a clear reference to the Snowden revelations, he asserted: “The people who are criticizing this are the ones who should have expected this.”

Opponents of backdoors or law enforcement “keys” recently received support from surprising sources. In a July 28, 2015, opinion piece, three former top US security officials came down strongly in favor of “ubiquitous data encryption” and defended the resistance of US technology companies to pressure from the FBI and other law enforcement agencies. The coauthors were former NSA Director Mike McConnell, former Department of Homeland Security Secretary

57 Ibid.
Michael Chertoff, and former Deputy Defense Secretary William Lynn. While acknowledging that the FBI and the Justice Department had raised legitimate concerns about end-to-end encryption, they concluded: “History teaches that the fear of ubiquitous encryption will cause our security to go dark is overblown. . . . The greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.”

In the op-ed, the three former officials cited and agreed with other cryptographers that introduction of duplicate or multiple source keys would inevitably weaken security; and they also agreed that if the US government forced such decryption devices on US companies, there would be no way to oppose the same treatment by foreign governments (read: China and Russia). Finally, these former security officials directly cited the essential ties between US competitiveness and national security: “ Strategically, the interests of US businesses are essential to protecting US national security interests. . . . If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential. And that imperative may outweigh the tactical benefit of making encrypted communications more easily accessible to Western authorities.”

As this point, the stalemate continues. Previously, the administration had suggested that it would go to Congress for legislative redress. A recent New York Times report has revealed that the administration is divided on how to proceed, with some officials now arguing for a court case against the companies and others believing that a judicial victory for the government would be difficult. On October 10, the Obama administration let it be known that it would not seek legislation mandating backdoors to aid in the capture of criminals or terrorists. Administration officials admitted that there presently is no safe way to force such action without increasing the possibility that authoritarian governments and criminals could not also utilize the backdoors for

---


nefarious purposes.\textsuperscript{63} It should be noted, however, that the FBI still opposes this decision, and either this or later administration could still seek such legislative mandates in the future.

The bottom line: The encryption debate forces a careful balancing of privacy and security. As matters now stand, the balance tilts in favor of the proponents of end-to-end encryption. There are two reasons for this result. First, there is what remains a technological reality: according to all leading experts and cryptographers, there is at present no way to comply with demands for backdoors or source keys without introducing grave weaknesses into the system. As the three former national security officials cited above noted: “Requiring duplicate keys introduces vulnerabilities in encryption that raise the risk of compromise and theft by bad actors.”

Of equal importance is the international dimension: as worldwide competitors, Apple, Google and other US companies cannot discriminate among markets and customers. Handing over duplicate keys to US government agencies will inevitably lead to understandable demands from foreign governments. Some of these governments are already moving to mandate such requirements. For instance, British Prime Minister David Cameron has vowed to force companies doing business in the United Kingdom to share encryption keys with British security agencies.\textsuperscript{64} Of greater worry, the Chinese government is contemplating the same requirement. Again as McConnell, Chertoff, and Lynn argue, if the US government makes this demand, “China will insist on the same. There will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications to a wide spectrum of governmental access regimes with varying degrees of due process.”\textsuperscript{65}

2.5. THE MANY FACES OF CYBERESPIONAGE

Espionage, or spying, is an age-old practice conducted by all nations. In the age of the Internet, however, its dimensions and scope have expanded dramatically, flanked often by private organizations and individuals seeking political or economic gains and societal disruption. Within


this expanded universe, the nature and limits of spying for economic purposes is underpinned by no international rules or practices. The United States and other nations, thus, remain in a reactive mode when dealing with economic incursions that can destroy legitimate competition and inhibit innovation. This section will present an overview of the challenging issues and set forth potential defensive and offensive paths to meeting those challenges.

2.5.1. THE 2015 EXECUTIVE ORDER AND US-CHINA CYBER “UNDERSTANDING”

On April 1, 2015, President Obama signed an executive order (EO) that expanded the federal government’s ability to respond to malicious cyberattacks. The president stated: “Cyberthreats pose one of the most serious economic and national security challenges to the United States. . . . This executive order offers a targeted tool for countering the most significant cyberthreats that we face.”

The cyberattacks included as examples in the EO included:

- Harming or significantly compromising the provision of services by entities in the US critical infrastructure;
- Significantly disrupting computers or computer networks, including through distributed denial-of-service attacks;
- Misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial of competitive advantage or private financial gain;
- Knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain;
- Attempting, assisting, or providing material support for any of the harms listed above.

Sanctions pursuant to the EO would include denial of use of US financial systems, including cutting the perpetrators off from all banking, security, and insurance facilities, and a mandate for US corporations to cease all business with the indicted individuals or entities.

---

Only a few months after releasing the EO, in late September, a long-awaited summit between President Obama and Chinese President Xi Jinping took place in Washington. In the weeks before the summit, the Obama administration had ratcheted up pressure on the Chinese, warning that the US was about to take action against Chinese private or government-sponsored hackers. It promised to identify publicly the individuals and companies involved in or benefiting from the economic espionage and bring the full force of US laws against them.

After frantic, last-minute negotiations—and to the surprise of many—President Xi agreed to major US demands regarding economic cyberespionage. Specifically, as the summit “understanding” fact sheet stated: “China and the United States agree that neither country’s government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.”67

At least on paper, this statement represents an important step forward for US-Chinese cyber relations. But as President Obama also affirmed, the United States was not foreclosing unilateral action should the economic espionage continue; he promised, “I did indicate to President Xi that we will apply those and whatever other tools we have in our toolkit to go after cyber criminals, either retrospectively or prospectively.”68 It is important that the administration follow through on this avowal. The US has signaled that it already has assembled the evidence for future indictments, and the amount of good faith granted to the Chinese should not be in months, but in weeks. Should ongoing Chinese incursions continue, or should there be new violations of the summit agreement, President Obama should act with dispatch.

Behind what may seem a clear-cut EO and summit agreement are a multitude of questions and challenges relating to the boundaries of economic espionage and international norms in combatting such activity. There is certainly consensus that, as listed in the EO, destruction of property, including online data, would give cause for retaliation. Further, attacks on a nation’s basic infrastructure (electrical grids and banking and securities institutions) would be considered

an act of war. But this list leaves out numerous gray areas where both the response imperatives and the legal justification are murky.

This point is best illustrated with analysis of two recent, significant events and their repercussions: first, the US indictment of five Chinese People’s Liberation Army (PLA) officers for cybertheft in 2014; and second, the recent theft of the personal records of some 22 million US government personnel from the US Office of Personnel Management (OPM).

2.5.2. LESSONS FROM THE INDICTMENT OF FIVE CHINESE PLA OFFICERS

The 31-count indictment of five members of PLA Unit 61398 alleged that they conspired to commit computer fraud, accessed computers without authorization, damaged computers through the transmission of malware code, and stole trade secrets from five US-based companies and one labor union.\(^69\) The indictment should be viewed against the larger context of a decade of intellectual property and trade secrets theft by hackers based in China—by government personnel, government-sponsored or affiliated personnel, or private groups. In 2013, a blue-ribbon panel of intellectual property experts stated that while the exact total of US losses from IP and trade secret theft was unknowable, they were comfortable in estimating that it was at least $300 billion annually.\(^70\) And they and others pointed out that the scope and size of such incursions—up to 80 percent of which originates from Chinese hackers—had steeply climbed over the past decade. While the Obama administration had repeatedly warned China that it would act, the Unit 61398 indictment was the first serious move against the rampant theft of US IP and trade secrets.

In the PLA indictment and since then, US officials have attempted to define what one cybersecurity expert has called “the precise (and narrow) limits of US economic espionage.”\(^71\) The US argues that there is a clear distinction between spying for national security goals and

---


commercial spying by governments for the benefit of individual corporations or sectors. As Attorney General Eric Holder stated in regard to the Chinese PLA indictment: “The alleged hacking appears to have been conducted for no reason other than to advantage state-owned companies and other interests in China, at the expense of businesses here in the United States. This is a tactic that the US government categorically denounces. As President Obama has said on numerous occasions, we do not collect intelligence to provide a competitive advantage to US companies, or US commercial sectors.”

Holder’s statement was underscored by James Clapper, the top US intelligence official: “What we do not do . . . is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of—or give intelligence we collect to—US companies to enhance their international competitiveness or increase their bottom line.”

In defending the US position, even some distinguished cyber experts have blurred or misstated key distinctions. James Lewis of the Center for Strategic and International Studies (CSIS) has stated: “There are unwritten rules that govern espionage, and China’s behavior is out of bounds. Where Beijing crosses the line is in economic espionage. . . . The United States, by contrast, does not engage in economic espionage.”

The problems with this assertion are twofold: first, there are no “rules” for economic espionage, written or unwritten; and second, the United States does indeed conduct economic espionage operations. It is just that, according to the repeated avowals of US officials, it does not pass along information so gained to private US companies.

This self-imposed restriction on US spying still leaves a large area of economic espionage for US intelligence agencies to exploit, including economic espionage on foreign governments and institutions, economic espionage on private companies as well as state-owned enterprises. It also permits penetration of company data to extract IP or trade secrets, with the stipulation only that such information not be passed on to US private firms. All of these actions are defended as essential elements of the broader goal of protecting US national security. Under this rubric, as the Snowden documents have shown, the United States has penetrated the corporate

---

communications of a number of companies in a number of nations, including the Brazilian state-run oil company Petrobras, which also led to the tapping of Brazilian President Dilma Rousseff’s phone.75 The US has also tracked firms’ internal communications, seeking to uncover support for sanctioned nations such as North Korea and Iran: one example is the German firm Siemens.76

Seeking information from governments is also fair game, as demonstrated by US attempts to ascertain economic or diplomatic policy negotiating positions. Examples here would include the EU antitrust commissioner, for information regarding potential actions against Microsoft, Intel, and Google77; Japanese officials during auto trade negotiations in the 1990s78; and French officials again for insight into their allegedly protectionist trade positions.79 And finally, of particular note given the current standoff with Beijing, US agencies penetrated deep into the corporate halls of China Telecom and the giant telecom company, Huawei (with the irony here that the US has excluded Huawei from major US contracts from the fear that it was a Trojan horse for Beijing).80

There are two final lessons from the US indictment of the PLA officers. First, and this can no doubt be remedied in future legal actions, the Chinese hackers actually stole little intellectual property of great importance, as described in the indictment. The potentially most significant technology cited related to an advanced civilian nuclear reactor, but Westinghouse, the parent company, had already agreed to transfer this technology to a Chinese joint venture partner several years before the case. Second, of greater import for future legal actions and charges, was the fact that the government, in its indictment, charged that the Chinese hackers had stolen corporate data that related to a trade remedy case against a Chinese company that involved several US companies (US Steel, Solar World) and a trade union as litigants. Though labeled

79 Ibid.
“ trade secrets” in the US indictment, the data basically included mostly pricing data and strategies to be invoked against Chinese companies in the trade remedy (antidumping) case. And the problem is that such espionage actions are clearly within the orbit of actions taken by (and vigorously defended by) US intelligence agencies.

The Snowden documents provide an abundance of evidence in this area. For instance, one set of documents revealed that in the US intelligence agencies’ “black budget” there is a section that states that the intelligence agencies will “directly support and strengthen” trade enforcement actions and the goals of US trade negotiations.81 More broadly, US intelligence leaders in the past have often spoken with great pride in the contribution of intelligence activities to the US economy. At the end of the Cold War in the early 1990s, US intelligence was recruited to perform economic intelligence, and then–CIA Director Stansfield Turner stated, “As we increase emphasis on securing economic intelligence . . . we will have to spy on the more developed countries—our allies and friends with whom we compete economically.” And in 1996, a National Research Council (NRC) report noted: “According to the National Security Agency (NSA), the economic benefits of SIGINT contributions to US industry taken as a whole have totaled tens of billions of dollars over the last several years.”82 The fundamental point here is that while US spy agencies do not pass along competitive information to individual US companies, the information they collect often does contribute to the overall success of US economic policy.

2.5.3. THE OPM DEBACLE

The discovery in the summer of 2015 that the Office of Personnel Management (OPM) had been the victim of a massive data breach that jeopardized the future careers of over 22.1 million US civil servants and civilian service applicants triggered large-scale political consternation and dismay.83 Some months later, in September, OPM further disclosed that the fingerprints of 5.6

---

million US civil servants had been stolen as a result of the cyber incursion. There were immediate calls for retaliation against the perpetrators of this cyberattack. The Obama administration has never formally named a culprit, but US intelligence officials, including Director of National Intelligence James Clapper, have informally pointed the finger at hackers based in China.

A common negative reaction to the US failure to respond came from Sen. Cory Gardner (R-CO), who noted the paradox of the United States’ invoking sanctions against North Korea when Sony’s private property was destroyed, but that “when the OPM is hacked, and millions of Americans, many of whom . . . are just common, everyday, private sector people have their private information stolen,” we refuse to name the culprits or take any action against them.

These sentiments were echoed in a Washington Post editorial, which stated that the Chinese attack was a “breach too far,” and later added: “Doing nothing is not an acceptable option. The United States needs to give cyberattackers real pause and a credible threat of certain retaliation, one that can be seen in public as well as felt in private.”

The US intelligence community, however, weighed in on the other side. While not precluding the possibility of a US response, they pointed out that the OPM breach represented an espionage action of the type undertaken by all nations. Further, it did not cross any of the red lines enumerated by the Obama administration: destruction of property or infrastructure, theft of IP, or disruption of national networks. Director of National Intelligence Clapper ruefully opined: “You have to kind of salute the Chinese for what they did.” And former CIA and NSA Director

Michael Hayden bluntly stated that OPM was a “legitimate foreign intelligence target. . . . This is not shame on China. This is shame on us.”

The key point of the responses by the intelligence community is that the United States and all other nations with cyberattack capabilities have practiced espionage such as that demonstrated in the OPM attack. Behind this warning also was the implicit argument that the United States would not forgo offensive opportunities similar to those exploited allegedly by the Chinese.

2.5.4. CRAFTING RESPONSES TO VARIEGATED CYBERATTACKS

In crafting responses to cyberattacks, the US faces the challenge of differentiating among a variety of potential incursions from individual states, state-backed hackers, and private operatives. It must also devise counteractions that are proportionate to the nature and scope of the attacks.

Though it remains unclear whether the Obama administration will follow through on its own framework, the president’s April EO and the September summit agreement represent a reasonable foundation for future US responses. The administration did put forward a proportional response—increased sanctions on Kim Jong-un’s government—to the Sony attack, which both disrupted the company’s networks and destroyed vital data. The administration, however, would be well advised to reiterate and underscore that, in the future, any destruction of public or private data—from whatever source—will be met with retaliation.

With regard to the complex issues presented by economic espionage, the US should stick to its guns when it comes to responses to the theft of intellectual property or trade secrets. This is despite the fact that as a New York Times analysis noted: “While American officials are loath to admit it, Washington’s view has relatively few advocates around the world.” Though the US is open to the charge that such retaliatory rules are self-serving as the US outdistances other nations

---

in technological advancement, it is also true that negotiations in the World Trade Organization (WTO) have introduced IP and trade secrets obligations into the global trade regime. While WTO rules do not as yet include obligations for cyberspace (see below for more on WTO issues), the US is on solid ground when defending technologies that are fundamental to its international competitiveness.

For the foreseeable future, however, the US will have to turn to its own domestic IP and trade secrets legal framework, and to its criminal justice system to enforce that framework. There are, however, important criteria and due process standards that the US must uphold as it moves to unilaterally enforce its domestic regime. And these present particular difficulties in cyberspace. First, given the increased ability of both government and private marauders to hide their tracks on the Internet, US legal teams will have to assemble solid evidence identifying the alleged culprits of the cyberattacks, as was the case, for instance, in the indictment of the five PLA officials in 2013. Second, civilian and intelligence officials will have to make decisions regarding the government’s ability to make public the evidence behind the indictment, even if such evidence has been collected by intelligence activities. The public evidence problem will force a careful balancing of priorities that will vary case by case. Third, in charging theft of IP, the US government faces the complex task of tying the original IP theft to the exploitation of the fruits of that technological breakthrough by a company in the offending nation. As the United States has already indicated, penalties for conviction in these cases could include exclusion from US financial markets or import restrictions or exclusion from the US market.

There are also legal tactics that the United States should avoid. Particularly, future US indictments should not conflate charges that include the theft of intellectual property and trade secrets and material related to pending trade remedy cases. As this report has shown, the US itself has strongly defended surveillance and data collection by US intelligence agencies that involves trade negotiations, as well as trade infractions relating to US or WTO law. Continuing down this road in future indictments will open America up to valid charges of hypocrisy.
One final note: former NSA director Keith Alexander has called Chinese actions against US intellectual property “the greatest transfer of wealth in history.”\(^1\) Within the coffers of the Justice Department and the CIA, there are undoubtedly many spectacular examples of US technology that has been stolen from US companies and then adopted by Chinese companies. The US government would be well advised to cherry pick and disclose publically the top examples when it comes time to follow up on President Obama’s vows to punish cyber violations of US companies’ intellectual property.

2.6. CHINA’S HARDENING STANCE ON TRADE POLICY AND CYBERSECURITY INCURSIONS

Chinese trade and economic policy has fluctuated wildly over the past two decades. Throughout the 1990s, as the country attempted to put in place policies that would allow it to join the WTO, it steadily moved toward greater internal flexibility, a welcoming face to foreign direct investment, and reducing both external and many internal barriers to trade. Having successfully achieved WTO membership in 2001 under premier Zhu Rongji, Beijing for the next five years made a sincere effort to live up to its multilateral trade obligations. The private sector thrived, and attempts were made to curb the favoritism toward state-owned enterprises.

Toward the end of the George W. Bush administration, however, forces gathered that swung the pendulum back toward greater state control along with increasing pressure to foster and protect native companies and key technological sectors. These trends have greatly accelerated under the new leadership of President Xi Jinping, starting in 2013. The “turning inward” has taken many forms. American and other foreign firms have been harassed through the use of fabricated business practices or antitrust complaints: Qualcomm, for alleged price fixing; Microsoft, for alleged abuse of market power; and Google, for refusing to knuckle under Beijing’s censorship demands.\(^2\) Under the unchecked zeal of China’s National Development and Reform


Commission, foreign company offices have been raided, computers and data collections seized, and local executives arrested. Over the past five years, the climate for foreign direct investment has become increasingly hostile.

On the other side of the policy equation, the Chinese government has mounted a widening campaign for “indigenous innovation” through which top Chinese political leaders hope and intend to foster local “Chinese” technologies that will, over time, replace foreign competitors. A variety of policy tools have been employed to achieve these goals, including identifying key technologies, subsidizing Chinese companies to compete against foreign companies, and closing off strategic sectors to foreign control or even investment. The Chinese government has also begun to develop national technical standards that differ substantially from internationally accepted product and process standards; American and other foreign companies have been forced to accept Chinese partners as a condition for operating in the Chinese market and, in many cases, also have been pressured—or forced—to transfer frontline production processes to the joint venture.93

2.6.1. THE NEW CHINESE SECURITY LAW AND ITS COMPANIONS

Over the past 12 months, the regulatory vise regarding foreign companies and competition has tightened steadily. Under the pretext of responding to the Snowden revelations, late in 2014 Beijing announced plans for new national security, cybersecurity, and antiterrorism laws. Beginning in the summer of 2015, the Chinese parliament passed the legislation.94

As with most Chinese legislation, the new national security law is couched in vague and sweeping terms. Within the scope and definition of national security are a daunting number of areas, including the military, political, and economic institutions and policy, the environment, religion, food safety, space exploration, and the Internet. The reach of the law goes far beyond China’s geographic boundaries, exerting authority over the seas, outer space, and most important

for this report, over cyberspace. The law also ties the Communist Party directly to the interests of the Chinese state, asserting that the new law is “to defend the people’s democratic dictatorship and the system of socialism with Chinese characteristics.” And it places a high priority on the need for China to assert “cyberspace sovereignty.”

The national security reviews prescribed in the law include not only traditional security analysis but also reviews of foreign investments that might infringe upon national security and reviews for investments involving key materials and technologies (particularly Internet and information technologies), construction projects, and “other major projects and events”\(^95\) that might implicate national security. The national security reviews of the technology industries are charged with producing technology that is “secure and controllable,”\(^96\) a phrase that is widely believed to provide grounds for forcing foreign technology companies to build so-called backdoors or hand over source code or encryption keys. Left unclear is how these new requirements would be administered or which agencies would be responsible.\(^97\)

Accompanying the national security law was also a law aimed specifically at cybersecurity. The new cybersecurity law fleshes out in more detail some of the rules in the overall national security law. The law commits the government to establishing new standards for the Internet and networks; mandates real-name registration on the Internet; mandates that Internet operators give “support and assistance” to the government in matters of criminal activity and national security; provides for timely notification of cybersecurity incidents; mandates that user data must be stored in China, though operators may apply for exceptions due to business necessity; provides for user permission before a company can use personal data; and grants large regulatory and enforcement powers to the Cyberspace Administration of China.\(^98\)

---


China has moved with dispatch to begin implementing important mandates in the law. Reports earlier this summer reveal that a number of US companies have received letters requesting that they pledge to fulfill key provisions of the national security law. The letter was issued by the China Information Technology Security Evaluation Center, most likely pursuant to instructions from the Cyberspace Administration. According to a New York Times report, the letter calls for the companies to commit not to harm Chinese security and to ensure that their products are “secure and controllable.” The specific language reads: “Our company agrees to strictly adhere to the two key principles,” which are listed as “not harming national security and not harming consumer rights.” As noted above, the repeated appearance of the “secure and controllable” language in official documents appears part of a coercive mandate that ultimately will present all foreign companies with two choices: either acquiesce, which would signal publicly that they were cooperating with Chinese plans for surveillance, or refuse to sign the declaration and thereby risk retaliation or cashiering from the enormous Chinese market.

The US corporate community has mustered a reasonably united front in protesting the scope and potential implications of the array of new laws that the Chinese government is moving to implement. Led by the US Chamber of Commerce, a number of major companies and trade associations—including telecom firms, motion picture producers, financial and agricultural companies—signed a protest letter charging that the proposed rules were “opaque,” “intrusive,” and “discriminatory.”

2.6.2. PROPOSED US GOVERNMENT RESPONSES

While they may sign letters of protest, US and other foreign multinationals cannot alone push back against the proposed new Chinese demands. Such a response can come only from governments, and specifically, the US government, either alone or in concert with other nations (Japan and Europe). And if the Chinese ignore protests and move forward with these proposals, the US should move beyond business as usual in cyber diplomacy with Beijing. The annual US-

---


China Strategic and Economic Dialogue (S&ED) has failed to produce solid results over the past years. For instance, the recently concluded S&ED came up with 127 conclusions, including such weighty topics as joint customs training, industrial boiler efficiency, and clean cookstoves.101

In a separate diplomatic/security initiative, the United States must insist that the Chinese first lay out the exact reach of the new legislation. And the US should make it clear that it would retaliate if Beijing uses the new laws as a pretext to exclude competition from US and other foreign firms in the Chinese market. This includes demands that foreign firms build cyber backdoors or hand over source codes to Chinese government officials.

In pressing its demands, the US has a strong lever: the huge US market and the desperate desire of the Chinese government to foster foreign investment by domestic Chinese companies around the world. With their own stock market tanking and with few prospects for internal investment, Beijing is pushing hard for its most competitive firms to move abroad—since 2005, China’s combined global investment and construction has totaled $1.1 trillion and could reach $3 trillion by 2025. Since 2013, the US has been the leading recipient of Chinese investment funds, with a grand total of $90 billion since 2005.102

Make no mistake, the US economy reaps great benefits from inward foreign investment, including investment from China. Furthermore, as a general rule, strict tit-for-tat reciprocity does not constitute good trade policy. As the noted 19th-century French free trade proponent Frédéric Bastiat wisely stated regarding reciprocal protectionist measures: if your neighbor insists on filling his harbor with rocks, it makes no sense for you to do likewise. But the drift of Chinese trade and investment policy over the past few years, combined with the specific threat to foreign competition embodied in the proposed pieces of legislation, demand a commensurate response. In future bilateral negotiations, the president and his aides should quietly but firmly convey the US intent to retaliate—and then act with dispatch if Chinese obduracy continues.

PART III: FINDING POLICY SOLUTIONS

3.1. MAJOR FORA FOR CYBER TRADE NEGOTIATIONS

There are a number of potential trade negotiating fora where the United States can exert its influence in crafting free market, competitive rules for the Internet. This report will highlight three pathways: the proposed mega-regional FTAs, the Trans-Pacific Partnership Agreement (TPP) and the US-EU Trade and Investment Partnership Agreement (TTIP); WTO Trade in Services (TISA) negotiations; and negotiations in a future WTO trade round.

3.1.1. TPP AND TTIP

Before analyzing the potential for new trade rules flowing from successful conclusions of the TPP and TTIP negotiations, a word on the precedent-setting Korea-US FTA (KORUS). While the US had negotiated some 9 FTAs that included reference to the digital economy, it was with the 2011 Korea FTA that a more complete set of rules were put in place. It built on general provisions in earlier FTAs, such as agreement that rules for services apply to services performed electronically; a prohibition of customs duties, or fees for digital products; and nondiscriminatory and transparent rules for digital products. KORUS added more specific rules for electronic authentication and signatures, consumer protection safeguards, and free data flows across borders. It also established special rules for financial institutions to transfer data across borders where this was necessary for the ordinary course of business. On all of the data flow provisions, however, there was no legally binding commitment: only the hortatory statement that “the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.”

The US goal in the TPP negotiations is to write more comprehensive rules of the road for digital trade that would be legally binding and would be part of an overall dispute settlement mechanism. Further, in the trade authorization legislation passed by Congress in the spring of 2014, the legislators (who have final say over trade rules under the US constitution) directly instructed the president to achieve a specific set of goals with regard to digital trade, including

mandates on free data flows, nondiscrimination of digital goods and services, and combatting mandates for local data storage and processing.  

At this point, the TPP negotiations have been concluded, but the final text has not been made public. However, On May 1, 2015, Deputy US Trade Representative Robert Holleyman set forth the major US negotiating goals in the TPP for electronic commerce. He labeled them his “digital dozen,” with the most important including:

- Trading nations agree to the principle of a free and open Internet;
- Complete prohibition of customs duties on Internet products;
- Nondiscrimination between domestic and foreign competitors;
- Oppose requiring technology transfers as a condition of doing business;
- Minimization of barriers to cross-border data flows;
- Prevent trading nations from forcing companies to localize data services;
- Safeguard network competition;
- Ensure technologically neutral electronic signatures and authentication;
- Foster innovative and effective encryption products.

Moving on to the TTIP negotiations, it is difficult at this point to render any detailed judgments because the negotiations have lagged in the wake behind the TPP negotiations. Recently, European trade officials have complained that the United States is dragging its feet, leaving the talks “not even halfway complete” after almost three years of negotiations.

Though it will further complicate matters, the recommendation in this report is to utilize the more comprehensive TTIP negotiations to settle important looming questions and potential conflicts regarding the Internet. These would include several major issues described above, including the right to be forgotten and negotiations for a new Safe Harbor agreement. For both issues, the goals should be a binding legal settlement as a part of the final TTIP agreement.

### 3.1.2. WTO’s Trade in Services Agreement (TISA)

The WTO Uruguay Round, which concluded in 1995, created a separate discipline for trade in services that is now binding for all WTO members: the General Agreement on Trade in Services (GATS). GATS introduced two sets of obligations on member states. The first simply adds the existing most-favored-nation (MFN) principle to the services sector. The second group of rules includes the national treatment principle and a set of market access rules to ensure fair competition across and within borders. Examples would include a prohibition on limiting the number of service providers in a given sector. These rules, however, apply only to sectors where a member state has specifically committed to such liberalization. Among the sectors that have the highest WTO member commitments are professional, financial, and telecommunications services.\(^{107}\) Importantly, these sectors are central to Internet services.

After the Uruguay Round, separate negotiations were mounted for financial services and basic telecommunications services. In addition, as noted above, individual bilateral and regional FTAs have advanced services liberalization in general, as well as updated rules that include the Internet. In 2000, WTO members agreed to launch a new overall round specifically for services negotiations. Participation is voluntary, but at this point some 24 WTO members have joined the negotiations (this counts the 28 EU nations as one body: counting them separately would bring the total to more than 50). They encompass more than 70 percent of the world’s total services trade.\(^{108}\)

If successful, the negotiations would multilateralize many of the goals and provisions in existing FTAs, as well as those under negotiation. It is also assumed that gradually more of the current 161 members of the WTO would sign onto the updated services disciplines. As to substance, there is a good deal of overlap in the specific proposals being considered in the TPP and TTIP. From leaked documents, it is clear that the negotiators are tackling most of the priority issues, including restrictions on data flows, particularly with regard to financial data; balanced privacy protections; consumer protections; prohibitions on mandated technology transfers; intellectual

---


property rights protection for digital products and services; protection of source code; nondiscriminatory authentication and signature rules; and prohibition of customs duties.109

3.2. THE INTERSECTION OF SECURITY AND TRADE LAW

As the potential conflict between the US and China over cybersecurity incursions has risen over the past decade, calls have periodically arisen for the US to invoke the rules of the WTO at least against economic espionage, such as the theft of intellectual property and trade secrets. Richard Clarke, a former security adviser to Presidents Bush and Obama, has argued that “victims of Chinese economic espionage should seek to establish clear guidelines and penalties within the World Trade Organization system.”110 Another noted cybersecurity expert, James Lewis of CSIS, has also suggested invoking WTO rules against China. Two means of utilizing WTO law are at issue: first, whether the theft of intellectual property or trade secrets by China or Chinese-directed hackers is a violation of China’s obligations under the WTO’s Intellectual Property agreement (TRIPS); and second, whether the US could invoke the WTO’s “national security exception” to retaliate against alleged Chinese espionage.

There are problems with both of these routes to retaliation. Regarding the TRIPS agreement, the specific challenge stems from the fact that WTO TRIPS rights are granted on a territorial basis: that is, China must grant national treatment (that is, equal treatment to that given its domestic companies) to the nationals or companies of other nations operating within its territories (Article 31). With regards to economic cyberespionage, however, what the US and other countries are seeking is protection of IP or trade secrets outside of China’s territorial boundaries: that is, theft by the PRC or PRC-controlled hackers in the US or other foreign territories. TRIPS does not mandate that China (or any other country) forbear from conducting IP or trade secrets theft in another country, nor does it mandate that China forbid its citizens from such activity. Neither China—nor the US—has made a commitment under TRIPS to avoid economic espionage outside its own territory. Thus, the US would have no WTO legal recourse to institute trade

countermeasures against alleged Chinese theft of IP or trade secrets within its US boundaries. It should be added, however, that this does not preclude the US from taking action under its own IP and trade secrets regime. It did so in 2014, when it indicted five members of China’s PLA for infractions of US (not WTO) law.

As to the recommendation that the US invoke the national security exception to WTO law, that course, too, raises important problems. Article XXI of the General Agreement on Tariffs and Trade (GATT) allows nations to levy trade actions against another country if such action is justified to protect essential national security interests—or, in GATT-speak, in response to an “emergency in international relations.”

Since this national security clause is self-justifying, it cannot be challenged effectively by other WTO members. And therein hangs the problem. Aware of the slippery slope nature of the national security exception, nations in both the GATT and WTO eras have largely refrained from invoking Article XXI. Should the US now suddenly invoke the exception to restrict Chinese trade or investment it would represent a WTO legal thunderclap and a break with long-standing practice. Further, China would certainly not stand still in the face of such action. It would retaliate, most likely also citing national security imperatives. And in the wake of the Snowden revelations, the US could not count or much legal or moral support even from some of its closest trading partners. In the end, this is not a fruitful path to take.

3.3. A US STRATEGY IN THE TRADE FORA

The United States should aggressively press forward with its stated digital trade policy goals in all fora. This means pinning down the priorities listed above first in the TPP negotiations, followed hopefully by a successful conclusion of the TISA and TTIP negotiations within the next several years.

Down the road, rules for digital trade should become a central element of the next WTO round of negotiations. The United States will certainly not achieve all of its goals for digital trade rules. But among the top priorities in the list of goals should be the extension of time-honored GATT/WTO rules regarding nondiscrimination and national treatment. In digital trade terms, this will mean lowering data flow barriers on an MFN basis, ensuring technological neutrality so
that goods and services supplied electronically receive the same treatment as traditional modes of
delivery, holding domestic and foreign service providers and Internet-related businesses to the
same rules, adopting rules to avoid data localization requirements, and adhering to a prohibition
of mandated technology transfers as a condition of doing business in a country.

Future US administrations must continue to uphold the vital digital agenda that both the Bush
and Obama White Houses have adopted to foster and maintain a free and open Internet. In such a
world, the United States will certainly thrive and prosper.