The Role of Government in Commercial Cybersecurity

Public-Private Partnerships and Improvements in Government Data Security Rather Than Government Control As the Optimal Model

Christopher Wolf
Future of Privacy Forum
Washington, DC*
cwolf@futureofprivacy.org

Abstract— *Privacy consists of two components: (1) conforming one's collection, use, and sharing of personal data to existing laws and norms, and (2) securing the data against unauthorized access and use. Even with the best of intentions as to the treatment of personal data, there can be no privacy where there is no data security. With the interconnected Internet, cybersecurity is a critical component of privacy. Given the dramatic increase in cybersecurity incidents, including Advanced Persistent Threats, some look to government to take control of the cybersecurity problem. In the United States, there is recognition of both the legal restrictions on the government "taking charge" of the flow of information through network access, monitoring, and/or control, as well as the limitations of government technical capabilities. As a result, US cybersecurity policy is collaborative, with the government working with industry to develop flexible standards rather than prescribing complex regulations. The result is a process-oriented, thematic approach to commercial cybersecurity that is more likely to produce optimal business practices. Several distinctions can be drawn between cybersecurity law and policy approaches worldwide, particularly between the US and other countries. A significant difference between the US and other jurisdictions is the role of public-private partnerships in promoting cybersecurity. Countries vary widely in their use of public-private partnerships to address cybersecurity. After evaluating the global differences in approach, public-private partnerships appear to be the best arrangement to secure commercial cyberspace.*

Keywords- *privacy; cybersecurity; public-private partnership; CALEA; ECPA; Fourth Amendment*

Privacy consists of two components: (1) conforming one's collection, use, and sharing of personal data to existing laws and norms, and (2) securing the data against unauthorized access and use. Even with the best of intentions as to the treatment of personal data, there can be no privacy where there is no data security. With the interconnected Internet, cybersecurity is a critical component of privacy.

Given the dramatic increase in cybersecurity incidents, including Advanced Persistent Threats, some look to government to take control of the cybersecurity problem. In the United States, there is recognition of both the legal restrictions on the government "taking charge" of the flow of information through network access, monitoring, and/or control, as well as the limitations of government technical capabilities. As a result, US cybersecurity policy is collaborative, with the government working with industry to develop flexible standards rather than prescribing complex regulations. The result is a process-oriented, thematic approach to commercial cybersecurity that is more likely to produce optimal business practices. Several distinctions can be drawn between cybersecurity law and policy approaches worldwide, particularly between the US and other countries. A significant difference between the US and other jurisdictions is the role of public-private partnerships in promoting cybersecurity. Countries vary widely in their use of public-private partnerships to address cybersecurity. After evaluating the global differences in approach, public-private partnerships appear to be the best arrangement to secure commercial cyberspace.

I. THE UNITED STATES APPROACH

A. THE LEGAL RESTRICTIONS ON THE US GOVERNMENT'S ACCESS TO NETWORKS

To understand the United States government's approach to protecting networks from cybersecurity intrusions, it is instructive to review the significant legal restrictions on its right to intercept and to review electronic communications and information. The government is obligated to follow the law, and may not access or control private networks unilaterally in the name of commercial cybersecurity. While a network operator may consent to government monitoring, the circumstances in which that is possible are limited to actual instances of computer trespass, not for prophylactic reasons.

The primary legal restrictions on government access to networks come from two primary sources: the Fourth Amendment to the US Constitution and the Electronic Communications Privacy Act ("ECPA"). [1]

The Fourth Amendment is most relevant to cases involving search and seizure of evidence, and also applies to government acquisition of electronic signals. [2] As a practical matter, however, the general Fourth Amendment proscriptions are less relevant that the specific prohibitions of the Wiretap Act and its amendment, ECPA, that encompass or exceed Fourth Amendment standards.

ECPA has three main sections. The first section amends the Wiretap Act to expand the government's surveillance authority over new technologies under prescribed

circumstances. The second section, the Stored Communications Act ("SCA"), governs access to "stored wire and electronic communications and transactional records." The third section is the "Pen Registers and Trap and Trace Devices" statute ("Pen/Trap" statute), which places limitations on the government's ability to compel a service provider to disclose real-time non-content information.

In general, the Wiretap Act and the Pen/Trap statute regulate the government's ability to obtain communications and non-content information contemporaneous with transmission; the SCA regulates its ability to obtain communications and non-content information that is stored by the service provider before or after transmission.

What follows are descriptions of the government's abilities and limitations under ECPA and two additional statutes to secure the nation's information infrastructure: the Foreign Intelligence Surveillance Act ("FISA") and the Communications Assistance for Law Enforcement Act ("CALEA"). FISA regulates electronic surveillance of suspected foreign agents. CALEA governs the telecommunications industry's responsibility to assist the government in surveillance activities.

1. The Wiretap Act

The Wiretap Act [3] generally prohibits "any person" from intentionally (1) intercepting any (2) wire, oral, or electronic communication. "Intercept" means to acquire the contents of communications through the use of a device contemporaneously with transmission. Almost all Internet and telephone communications qualify as "wire" or "electronic" communications under the Wiretap Act. The Wiretap Act has many exceptions; two that are relevant here are the provider exception and the computer trespasser exception.

The Provider Exception: An agent or employee of a service provider may intercept and disclose communications "incident to the rendition of his service or to the protection of the rights or property of the provider of that service." This exception generally permits service providers to combat fraud, theft, or damage to the network. Notably, this exception does not permit "service observing or random monitoring except for mechanical or service quality control checks."

The Computer Trespasser Exception: In certain circumstances, a service provider acting under the government's direction ("under color of law") is permitted to intercept and monitor a computer trespasser's or hacker's wire or electronic communications "transmitted to, through, or from" a networked computer. The exception applies if the following requirements are met: (1) the owner or operator of the networked computer authorizes the interception; (2) the person acting under color of law is lawfully engaged in an investigation; (3) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (4) the interception does not acquire communications other than those transmitted to or from the computer trespasser. Importantly, this provision does not permit routine, ongoing monitoring of a network by the government, but only consented-to monitoring where permission is granted by the network operator.

2. The Pen/Trap Statute

The Pen/Trap statute [4] applies when the government seeks to compel a service provider to disclose real-time non-content information (i.e., dialing, routing, addressing, or signaling information) at the time of transmission. Pen registers capture outgoing information; trap and trace devices capture incoming information. In general, the government may install a pen/trap device through a court order. To get an ex parte court order, the government attorney must submit an application to the court that, among other things, must certify that the information likely to be obtained is relevant to an ongoing criminal investigation. In the alternative, the government can install a pen/trap device without a court order in certain emergency situations such as where there is an immediate danger of death or serious bodily injury or an immediate threat to national security. A pen/trap order requires the service provider to furnish the "information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device."

3. The Stored Communications Act

The SCA [5] regulates the circumstances under which the government can compel disclosure of (i) certain customer information stored by the service provider and (ii) certain communications stored prior to transmission and after receipt; as well as the service provider's ability to voluntarily disclose such information. The SCA assigns different levels of protection depending on the information and type of communication at issue; thus, the tools available to the government to compel disclosure depend on the type of information sought and the type of service provider. For example, the government can compel disclosure of basic subscriber and billing information using only a subpoena (a very low burden for law enforcement). Other non-content information, such as addressing information, requires a court order (a higher burden than a subpoena, but lower than a probable cause search warrant). And some communications, such as certain unretrieved emails and voice mails, require a court-issued search warrant (the highest burden, requiring a showing that there is probable cause to believe that the information sought is relevant to the investigation). Similarly, whether the government must provide notice of the subpoena, court order, or search warrant to the person to whom it was directed depends on the type of information or communication. Moreover, in certain circumstances a court may order the service provider to not disclose the existence of a subpoena, court order, or warrant to the person whose information or communications are sought, such as when disclosure would endanger the physical safety of an individual. The SCA shields a service provider from liability for complying with the terms of a "court order, warrant, subpoena, statutory authorization, or certification."

The SCA also governs when a service provider may voluntarily disclose certain information and communications to third parties, including the government in its law enforcement role. Absent an applicable exception, a service provider may not disclose communications to any third party or any records

to a governmental entity. However, the provider may make a voluntary disclosure to the government, among other reasons, if (1) such disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service"; (2) the information was "inadvertently obtained by the service provider and appear[s] to pertain to the commission of a crime"; or (3) "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."

Under the "counterintelligence" or "National Security Letter" ("NSL") provisions of the SCA, the government may require that a wire or electronic communications provider produce subscriber information and billing records information, upon a certification by certain high-level FBI officials that the records or information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." An NSL may prohibit the recipient service provider from disclosing the existence of the NSL to anyone, upon a certification by one of several specified FBI officials that disclosure may result in a danger to the nation's security, interference with an ongoing investigation, or danger to the life and physical safety of any person. Following several constitutional challenges to this provision, NSLs are now subject to judicial review, in which the provider may seek to set aside or modify the request for information and the non-disclosure provisions.

4. The Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act ("FISA") [6] authorizes and regulates electronic surveillance of communications transmitted through the United States involving suspected agents of foreign powers, when a significant purpose of the surveillance is to obtain foreign intelligence information. To obtain authorization, the government must generally certify to a special court, the Foreign Intelligence Surveillance Court, that the target of the surveillance is a foreign power or agent of a foreign power and that a significant purpose of the surveillance is to obtain foreign intelligence information, among other things. The government must also propose certain "minimization procedures" designed to minimize inadvertent collection of unauthorized communications. Like the SCA, FISA shields a service provider from liability for assisting with a FISA order.

FISA applies both when foreign agents are physically located within the United States and when foreign agents' communications are routed through the United States. FISA does not apply to communications occurring wholly outside of United States territory. Moreover, if the surveillance involves communications exclusively between or among "foreign powers" (a term that includes groups engaged in international terrorism and foreign-based political organizations not substantially composed of United States persons), the United States Attorney General may authorize surveillance without a court order provided that, among other things, there is "no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."

5. The Communications Assistance for Law Enforcement Act

The statutes discussed above provide the legal boundaries within which the government can conduct electronic surveillance; CALEA [7] requires service providers to ensure that the government has the capability to conduct electronic surveillance. When the original Wiretap Act was enacted, law enforcement intercepted communications primarily through AT&T's telephone wires when that company enjoyed a monopoly position. The government's ability to conduct that surveillance was hampered due to the development of new methods of communication and the increased number of communications providers. In response, Congress enacted CALEA in 1994 in order to "make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes and for other purposes." CALEA requires "telecommunications carriers" to "ensure that its equipment, facilities, or services . . . are capable" of: (1) enabling the government to intercept communications content; (2) enabling the government to access call-identifying information; (3) delivering intercepted communications and call-identifying information to the government; and (4) facilitating authorized communication interceptions and access to call-identifying information, while protecting both the privacy of other communications and call-identifying information and information regarding the government's interception of communications or access to call-identifying information. The Federal Communications Commission is responsible for prescribing regulations necessary to implement CALEA, including which entities are subject to CALEA. Broadband providers and Voice over Internet Protocol providers are considered "telecommunications carriers" under CALEA.

6. Legislative Proposals Affecting ECPA and CALEA

There are currently two legislative proposals relevant to ECPA and CALEA. Legislation is proposed to extend the reach of ECPA to cloud computing providers, thus extending the strictures and prohibitions of that law beyond network operators to remote Internet hosts of user content. This would impose further restrictions on the government's ability to access information in the name of cybersecurity. At the other end of the spectrum is the FBI-backed proposal for legislation that would require operators of online services that serve as "virtual networks," such as social media companies, to have the technological means to permit the government access to communications under legally permissible circumstances.

B. The US Government's Role in Promoting Commercial Cybersecurity

Since the US government is limited in its ability to monitor commercial networks for cybersecurity issues, its principal roles in protecting cyberspace have been through (1) law enforcement, (2) improvements to its own cybersecurity and sharing its research and experience with industry and the public, and (3) engaging in a public-private dialogue about cybersecurity through which it has incorporated suggestions from industry into cybersecurity policy. There is no apparent support for these roles to change. This section explores each of

these three methods of promoting positive commercial cybersecurity practices.

1. Law Enforcement

US law enforcement in the cybersecurity area falls into two general categories: prosecuting hackers who break into private networks, and holding organizations responsible if they suffer data breaches due to a failure to adopt industry-standard data security protections.

The primary statute in the US used to prosecute computer hackers is the Computer Fraud and Abuse Act ("CFAA"). [8] The CFAA prohibits hackers from accessing a networked computer "without authorization" or by "exceeding authorized access," and thereby obtaining information, engaging in fraud, or causing damage or loss. It also prohibits individuals from transmitting computer viruses. The statute contains a private right of action, which permits network owners to sue and recover from hackers who damage their networks. Many states, in addition to enacting their own anti-hacking laws similar to the CFAA, have also enacted anti-spyware laws that prohibit individuals from loading software onto others' computers without their knowledge. [9]

In the second category, the Federal Trade Commission ("FTC") has the authority to bring enforcement actions against businesses that provide an inadequate level of data security under its jurisdiction to police "unfair or deceptive acts or practices in or affecting commerce" under Section 5 of the FTC Act. [10] Under this authority, companies found to lack industry-standard data security safeguards, or that misrepresent their data security safeguards, are subject to penalties and ongoing government audits. At the state level, laws parallel to the FTC Act also have been used to penalize companies suffering data breaches. In addition, most states have enacted breach notification laws that require entities maintaining certain types of personal information to report to affected individuals any breach of that information. The specter of a regulatory enforcement action or a potential breach notification has encouraged companies to voluntarily enhance their data security measures without any direct mandate from government.

Supplementing this generally flexible approach to data security enforcement and regulation, the US has implemented more granular data security regulations specific to the healthcare and financial sectors. [11] Some states also have recently implemented specific data security regulations that provide more prescriptive rules for compliance that are consistent with FTC precedent and are sector-neutral. [12] For the most part, however, the data security of businesses not in the healthcare or financial sectors is regulated primarily by the FTC Act and its state analogs.

2. Improvements to US Government Cybersecurity

Though the United States' approach to the security of its own internal government networks is outside the scope of this paper, it is relevant to the extent that the US government shares with industry some of its security standards. This, in turn, encourages commercial entities to follow the government's own rigorous standards. In some circumstances, commercial government contractors are required to follow those standards.

For example, in February 2011, as part of its broader effort to encourage cloud computing for federal agencies, the National Institute of Standards and Technology ("NIST") announced a new cloud computing Wiki to enable industry-NIST collaboration, [13] as well as the publication of three significant cloud computing documents. The documents separately addressed (1) security and privacy in public cloud computing; (2) the definition of cloud computing; and (3) a guide to security for virtualization technologies. For cloud providers, the most important is NIST's draft Guidelines on Security and Privacy in Public Cloud Computing (the "Guidelines"). [14]

The comprehensive, sixty-page Guidelines encourage federal agencies to take advantage of public cloud computing services and provide roadmaps for negotiating meaningful privacy and data security protections from cloud providers. The Guidelines focus on identifying trouble spots that arise from using cloud providers and articulating an analytical framework to address them. Four overarching themes emerge: (1) moving data to the cloud does not relieve an organization of its privacy or data security obligations; (2) cloud computing complicates security because it adds layers of technology (and thus complexity and new avenues of attack) and strips the data owner of control over its data; (3) to the extent practicable, organizations should seek the same or better security of the cloud as in-house; and (4) cloud computing therefore requires a deliberative approach by organizations and unprecedented levels of trust of cloud providers. Though prepared for federal agencies, the Guidelines could prove influential to the private sector as an increasing number of private businesses use cloud services.

All three documents have the potential to shape how federal agencies and private-sector companies approach cloud computing and negotiating terms of service with cloud providers.

3. Facilitating a Public-Private Dialogue About Cybersecurity

A key component of the US government's approach to commercial cybersecurity policy has been to facilitate a public-private dialogue that has enabled both government and industry to learn from each other's experiences. For example, the US Computer Emergency Readiness Team ("US-CERT"), the operational arm of the National Cyber Security Division at the Department of Homeland Security ("DHS"), is a public-private partnership that interacts with federal agencies, industry, the research community, state and local governments, and others to publish cybersecurity information. US-CERT also provides interested parties with the ability to communicate and coordinate directly with the United States government on cybersecurity. US-CERT is charged with providing response support and defense against cyberattacks for .gov websites (those of the Federal Civil Executive Branch) and information sharing and collaboration with state and local governments, industry, and international partners.

The Obama Administration further set the tone in 2009 when the President directed a sixty-day, comprehensive "clean-slate" review to assess US policies and structures for cybersecurity. The results of this review were embodied in the Administration's Cyberspace Policy Review, [15] in which it stated that "[t]he United States cannot succeed in securing cyberspace if it works in isolation," advocating that the government and private sector should work together on their "intertwined" interest of "ensuring a secure, reliable infrastructure."

In March 2011, a broad coalition of business, civil liberties, and Internet security groups including the US Chamber of Commerce, the Business Software Alliance, the Center for Democracy & Technology, the Internet Security Alliance, and TechAmerica released a white paper that supports the continued use of public-private partnerships to address cybersecurity rather than have the government play a more prescriptive and intrusive role. [16] The paper, entitled "Improving Our Nation's Cybersecurity through the Public-Private Partnership" emphasized the importance of collaboration between the private and public sectors but concluded that the complexities of the Internet and the sophistication of cyber-criminals made centralized control of the problem ill-advised.

In June 2011, the US Department of Commerce ("DOC") issued a "Green Paper" preliminarily recommending a new framework for commercial cybersecurity entitled "Cybersecurity, Innovation and the Internet Economy." [17] The report discusses how to improve the cybersecurity practices of companies that operate online in the so-called "Internet and Information Innovation Sector," not including companies in "critical infrastructure" sectors that implicate national security interests such as the defense, energy, financial, healthcare, and core telecommunications sectors. This report may be paradigmatic of public-private cooperation on cybersecurity. In 2010, after several months of consultations with stakeholders, DOC convened a public symposium and published a formal Notice of Inquiry requesting that private entities provide input into the desired role of government in private cybersecurity efforts. The results of that public outreach led to the Green Paper.

To increase the security of businesses on the Internet, the Green Paper preliminarily recommended that DOC: (1) work with multi-stakeholder groups to develop, when necessary, nationally recognized and consensus-based cybersecurity standards and practices specific to the covered businesses; (2) work with industry to create, through public policy and public-private partnerships and other means, new incentives for firms to follow nationally recognized cybersecurity standards and practices as consensus around them emerges; (3) work with industry and other federal agencies to deepen private-sector and public understanding of cybersecurity vulnerabilities, threats, and responses in order to improve incentives, research and development, and education; and (4) continue to enhance DOC's international collaboration and cooperation activities regarding cybersecurity.

Specifically, the Green Paper called for improved commercial cybsecurity through the use of voluntary self-regulatory industry standards. It also contemplated the development of external incentives for businesses that institute strong cybersecurity practices, such as liability protection, improving the availability of cybersecurity insurance, and tax breaks. Notably, none of these methods would impose prescriptive regulations on businesses, as DOC concluded that the best way to increase the adoption of best practices would be through incentives and proactively working with industry rather than merely reacting to problems as they occur.

Keeping with the spirit of collaboration, DOC permitted interested parties to comment on the recommendations in the Green Paper. DOC plans on incorporating these comments into its recommendations to help build a more complete policy with respect to commercial cybersecurity.

C. Pending Cybersecurity Legislation Under Consideration in Congress Proposes a Limited Government Role

The Executive Branch is not the only government actor interested in pursuing public-private partnerships. Cybersecurity has become a priority in Congress this past session, with legislators working on a number of bills to encourage businesses to increase the security of their networks.

There have been so many legislative proposals relating to cybersecurity, with at least seven Senate committees claiming jurisdiction, that in July 2011 Senator John McCain called for the formation of a temporary "Select Committee on Cyber Security and Electronic Intelligence Leaks" to assume primary jurisdiction over cybersecurity legislation. This section discusses two of these recent proposals.

1. Cybersecurity and Internet Freedom Act

In February 2011, the chairman and ranking members of the Senate Committee on Homeland Security and Governmental Affairs introduced the "Cybersecurity and Internet Freedom Act of 2011." [18] The limited nature of the bill is a reflection of the sentiment among major industry leaders (as well as civil liberties groups), and as reflected in the recent reports described above, that the government's role in protecting cyberspace is limited.

The proposed bill would, among other things:

- Authorize the President to issue a declaration of a "national cyber emergency" if there is an "actual or imminent action by any individual or entity to exploit a cyber risk in a manner that disrupts, attempts to disrupt, or poses a significant risk of disruption to the operation" of certain "critical infrastructure." In such an emergency, the President would be obligated to notify the owners and operators of the infrastructure of the nature of the emergency, and direct them to implement appropriate response plans. Infrastructure operators and owners would be required to develop those response plans, in advance, under regulations to be promulgated by DHS.

- Establish within DHS a National Center for Cybersecurity and Communications ("NCCC"), led by a Director, which would coordinate with the private sector and lead the national effort to secure, protect, and ensure the resiliency of the national information infrastructure.

• Prohibit any federal entity from (1) restricting communications over critical infrastructure unless the Director of the NCCC determines that no other emergency action would preserve the reliable operation of such infrastructure or the national information infrastructure; (2) controlling critical infrastructure; or (3) intercepting or accessing wire, oral, or electronic communications or conducting electronic surveillance unless otherwise authorized by existing law.

• Establish in the Executive Office of the President an Office of Cyberspace Policy, to be tasked with development of a national strategy to increase the security and resiliency of cyberspace, oversee and coordinate federal policies related to cyberspace security and resiliency, and ensure that all federal agencies comply with DHS policies relating to those issues.

• Establish US-CERT within the NCCC. As noted, US-CERT already exists within DHS; it collects and disseminates information on risks to computer infrastructure, engages with the private sector on cybersecurity, and addresses instances of computer network breaches. The proposed legislation would move US-CERT to NCCC and formalize some of its responsibilities.

Responding to criticism faced by a predecessor version of the bill introduced in 2010, the new bill explicitly states that neither the President nor any officer or employee of the US government would have the authority to "shut down" the Internet (or provide a so-called "Internet kill switch"). This language would bring clarity to Section 706 of the Communications Act of 1934, which grants the President sweeping war powers to regulate communications. That provision allows the government to "cause the closing of any facility or station for wire communication" and "authorize the use or control of any such facility or station" after having declared that a state of war, or the threat of one, exists.

The sponsors of the bill specifically envisioned that government and business would work together to develop optimal standards. In a commentary, they wrote: "This framework would produce cybersecurity 'best practices' that would then be available as a model for the private sector. While such use would be voluntary, the development of better security techniques and the creation of industrywide standards of care would lead commercial networks to install them as a way to keep customers and draw in new ones." [19] The sponsors clearly felt that incentives, and not prescriptive rules, would serve best to improve cybersecurity in the private sector.

2. Executive Cyberspace Coordination Act

In March 2011, federal legislation was introduced that would reform the way IT security would be monitored and managed within the federal government. The legislation also would overhaul the Federal Information Security Management Act of 2002 ("FISMA"), [20] which has important implications for private-sector government contractors. The bill, known as the "Executive Cyberspace Coordination Act of 2011," [21] comes on the heels of a report indicating that the federal government has "not yet fully implemented key actions that are intended to address threats and improve the current U.S. approach to cybersecurity." [22] The legislation has received bipartisan support and is similar to a bill introduced in the Senate in February.

Since this bill would affect the security standards to which private-sector federal government contractors would be required to adhere, many of these contractors are watching this legislation carefully. The bill includes a proposal to establish minimum information security requirements for procurement of IT products and services, and a proposal to adopt policies for evaluating and mitigating supply chain security risks associated with products or services acquired by federal agencies. Data security conditions (including FISMA terms) increasingly are incorporated into federal agreements, catching some contractors and grantees off guard. Moreover, as the private sector moves toward a cloud computing platform, the evolving federal cybersecurity policies likely will affect how organizations use cloud services in the performance of contracts and grants. Organizations may need to start treating cloud service providers as subcontractors, and contractually impose federal data security requirements on these providers. It is too early to tell how these and other important issues ultimately will play out, but if the legislation is enacted, a number of private-sector government contractors would be subject to more granular data security requirements.

The legislation includes other provisions limiting the government's role in cybersecurity and encouraging interaction between the public and private sectors. It would establish a Federal Chief Technology Officer, appointed by the President and confirmed by the Senate, to work across agencies and the private sector on information technology considerations with regard to federal budgets and research and development programs. While it would provide DHS with authority to issue measures for the protection of information systems that control critical infrastructure, it would not give DHS or the President an "Internet kill switch" or related control over private systems. The bill also has a collaborative component, as it would establish a "Cyber Challenge Program" to engage students and the workforce in skill sets relevant to advanced cybersecurity capability.

II. GLOBAL APPROACHES TO CYBERSECURITY

EU member states have implemented privacy and data security laws pursuant to several directives of the European Parliament and Council. The 1995 Data Protection Directive (95/46/EC) [23] and the 2002 E-Privacy Directive (2002/58/EC) [24] contain requirements pertaining to the processing and safeguarding of personal data and the confidentiality of electronic communications, which the member states have transposed into national law.

While the directives contain detailed and extensive privacy and confidentiality requirements, their treatment of data security is less comprehensive. Article 17 of the Data Protection Directive compels the member states to require entities that control personal data to "implement appropriate technical and organizational measures to protect personal data against . . . unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network." Similarly, Article 4 of the E-Privacy Directive states that an electronic communications provider must take "appropriate technical and organizational measures to

safeguard security of its services." In both directives, organizations must ensure "a level of security appropriate to the risks presented," taking into account factors such as cost of implementation. In addition, Article 5 of the E-Privacy Directive provides that member states "shall ensure the confidentiality of communications," and that "[i]n particular, they shall prohibit listening, tapping, storage, or other kinds of interception or surveillance of communications," except under certain circumstances.

Apart from these general principles, the directives says little with respect to data security. Given the generality of these requirements, the EU member states have had considerable flexibility in implementing the directives' security mandates according to their individual circumstances and existing legal systems.

Non-European countries have also addressed data security matters through regional agreements. The 2004 Asia-Pacific Economic Cooperation (APEC) Privacy Framework [27] establishes a common set of data privacy and protection principles for jurisdictions in the Asia-Pacific region. Similar to the EU Data Protection Directive, the APEC Framework states generally that personal information should be protected with appropriate safeguards that are proportional to the sensitivity of the information held and the likelihood and severity of any threatened harm. However, unlike the Data Protection Directive, the APEC Privacy Framework is non-binding and does not compel APEC members to implement the principles of the Framework into their national laws. Given the non-mandatory nature of the Framework, it is unlikely to eliminate the significant discrepancies that exist between countries in the Asia-Pacific region with respect to cybersecurity-related laws and practices.

That being said, APEC members have, to varying degrees, transposed the Privacy Framework's principles into national law. For example, in 2010 Taiwan revised its privacy law to include data security and breach notification requirements, as well as financial sanctions for data protection violations. In February 2011, comprehensive data protection legislation advanced in the Philippines House. The proposed legislation, which is consistent with APEC Privacy Framework's principles, would require Filipino businesses and government agencies to implement reasonable data security measures to protect personal information and provide breach notice to affected individuals. In July 2011, data protection legislation based upon the APEC Framework was signed into law in Peru. The law is designed to allow Peru to meet commitments in free trade agreements with the US and Canada, which specifically required Peru to adopt personal data protection legislation.

III. COMPARATIVE APPROACHES TO GLOBAL CYBERSECURITY POLICY

Several distinctions can be drawn between cybersecurity law and policy approaches worldwide, particularly between the US and other countries. In a number of jurisdictions, such as the EU, national data protection laws are derived from broad principles set forth in overarching regional frameworks. While such an approach can serve to establish baseline norms and promote regional cooperation, it can also lead to differing implementations across jurisdictions, which may in some cases frustrate the purpose of the underlying measure or framework.

For example, the EU directives have given little guidance to member states on how they should implement the directives' broad data security mandates, which in turn has led to varying interpretations of the directives. As noted in recent reports by the European Network and Information Security Agency (ENISA)—an EU agency established in 2004 to enhance the capability of the member states and their business sectors to prevent, address, and respond to network and information security threats—this variance is not without costs in terms of addressing transnational issues such as cybersecurity.

In a March 2011 report on the threat posed by "botnets" (which are networks of compromised, remotely controlled computer systems), [25] ENISA found that that the diversity of the member states' legal frameworks in the context of cybercrime was a "key factor" affecting the fight against botnets. The report also noted that the detection and mitigation of cybercrime was limited by conflicts between the member states' data protection and IT security laws. Among other recommendations, the report called upon regulators to harmonize European laws in order to facilitate mitigation processes and cooperation at an international level.

In June 2011, ENISA issued updated versions of its "Country Reports" on network and information security (NIS) in the EU member states and certain other European countries. [26] In its overview report, ENISA found that "there is no consistency in the observed European countries with respect to the presence of a NIS national strategy or cyber-security strategy." The report found that while the government in each state usually played a central and active role, "the level of involvement from other stakeholders (industry, academic, NGOs, etc.) is not consistent throughout Europe." The report observed that the cross-border interconnectedness of critical information systems raised the need to address their security with a "systemic perspective" as the frontline of defense against failures and attacks.

Another significant difference between the US and other jurisdictions is the role of public-private partnerships in promoting cybersecurity. As discussed earlier, such collaborations are a key element of the US approach, and help both government and private stakeholders optimize their approaches to cybersecurity. Other countries vary widely in their use of public-private partnerships to address cybersecurity.

For instance, the recent ENISA report identified inconsistencies throughout Europe in the level of involvement by non-governmental stakeholders in the development of cybersecurity policy. In one example, in the context of network resilience, the report found that in some countries, "no mechanism exists where authorities, telecom providers and infrastructure owners would meet on a regular basis to address eCommunications resilience and/or security issues," while in others there were "bilateral mechanisms" for addressing such matters. The ENISA report also discussed the "interesting trend" of more countries establishing centralized cybersecurity authorities, which seems at variance with the US strategy of empowering industry to deal with cyber threats.

The ENISA report specifically highlighted recent developments regarding national cybersecurity strategies in France, Germany, the Netherlands, and Estonia. According to the report, France's national strategy, released in February 2011, includes objectives such as being a global power in cyber-defense and reinforcing the cybersecurity of vital national infrastructure. The German national cybersecurity strategy, announced in early 2011, addresses enhanced protection of critical infrastructure, protection of IT systems in Germany, an effective joint effort across Europe and the world, and the creation of a "National Cyber Defence Centre." The Netherlands is in the process of developing a national strategy, which will address combating cybercrime, improving network and information security, cyber defense, and cyber warfare. Estonia's national strategy concentrates on the responsibilities of state and private organizations, vulnerability assessments of critical national information infrastructure, the response system, domestic and international legal instruments, international cooperation, and training and awareness-raising issues. Notably, with the exception of Estonia—which in 2007 suffered a wave of cyber attacks on government and private sites—none of these national strategies appear to address the role of private entities in the mitigation of cybercrime or the establishment and promotion of public-private partnerships of the kind described in the DOC Green Paper or the Administration's Cyberspace Policy Review.

Whatever the differences between national cybersecurity models, cybersecurity clearly is a global issue, as the interconnectedness of modern communications networks allows cyber-criminals to launch attacks from beyond a nation's borders. Cooperation between governments—as well as engagement between the public and private sectors—is therefore essential to ensuring the security of cyberspace.

* Mr. Wolf also is director of the Privacy and Information Management Practice at the international law firm Hogan Lovells US LLP. Special thanks to his Hogan Lovells colleagues Bret Cohen and Michael Epshteyn for their assistance in the preparation of this paper.

[1] Pub L. 99-508, 100 Stat. 1848 (1986).

[2] The Fourth Amendment declares that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[3] 18 U.S.C. §§ 2510-2522.

[4] 18 U.S.C. §§ 3121-3127.

[5] 18 U.S.C. §§ 2701-2712.

[6] 50 U.S.C. §§ 1801-1885c.

[7] 47 U.S.C. §§ 1001-1010.

[8] 18 U.S.C. § 1030.

[9] *See* National Conference of State Legislatures, State Spyware Laws (last updated 8 Feb. 2011), http://www.ncsl.org/default.aspx?tabid=13452.

[10] 15 U.S.C. § 45.

[11] *See* Health Insurance Portability and Accountability Act Security Rule, 45 C.F.R. Parts 160, 164; Financial Services Modernization Act Safeguards Rule, 15 U.S.C. §§ 6801-6809.

[12] *E.g.*, Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts, 201 CMR 17.00.

[13] NIST Cloud Computing Collaboration Site, http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing.

[14] NIST, GUIDELINES ON SECURITY AND PRIVACY IN PUBLIC CLOUD COMPUTING, Draft Special Pub. 800-144 (2011), *available at* http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

[15] CYBERSPACE POLICY REVIEW: ASSURING A TRUSTED AND RESILIENT INFORMATION AND COMMUNICATIONS INFRASTRUCTURE (2009), *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[16] IMPROVING OUR NATION'S CYBERSECURITY THROUGH THE PUBLIC-PRIVATE PARTNERSHIP (2011), *available at* http://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf.

[17] U.S. DEP'T OF COMMERCE INTERNET POL'Y TASK FORCE, CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY (2011), *available at* http://www.commerce.gov/sites/default/files/documents/2011/june/cybersecurity_green_paper_finalversion.pdf.

[18] Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

[19] Joe Lieberman, Susan Collins, & Tom Carper, *A gold standard in cyber-defense*, WASH. POST, July 7, 2011, *available at* http://www.washingtonpost.com/opinions/a-gold-standard-in-cyber-defense/2011/07/01/gIQAjsZk2H_story.html.

[20] 44 U.S.C. §§ 3541-3549.

[21] Executive Cyberspace Coordination Act of 2011, H.R. 1136, 112th Cong. (2011).

[22] GOV'T ACCOUNTABILITY OFFICE, CYBERSECURITY: CONTINUED ATTENTION NEEDED TO PROTECT OUR NATION'S CRITICAL INFRASTRUCTURE AND FEDERAL INFORMATION SYSTEMS 5 (2011), *available at* http://www.gao.gov/new.items/d11463t.pdf.

[23] DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 24 OCTOBER 1995 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[24] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 12 JULY 2002 CONCERNING THE PROCESSING OF PERSONAL DATA AND THE PROTECTION OF PRIVACY IN THE ELECTRONIC COMMUNICATIONS SECTOR, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML.

[25] ENISA, BOTNETS: DETECTION, MEASUREMENT, DISINFECTION & DEFENCE (2011), available at http://weblog.leidenuniv.nl/media/blogs/106178/Summary_ENISA_report.pdf.

[26] ENISA, NIS COUNTRY REPORTS OVERVIEW DOCUMENT (2011), available at http://www.enisa.europa.eu/act/sr/files/country-reports/enisa_country_reports_introduction.pdf .

[27] APEC PRIVACY FRAMEWORK (2005), available at http://publications.apec.org/publication-detail.php?pub_id=390.