KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement for the Record of Gregory T. Nojeim
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology

Before the Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

CYBERSECURITY: EVALUATING THE ADMINISTRATION'S PROPOSALS

June 21, 2011

Chairman Whitehouse, Ranking Member Kyl, and Members of the Subcommittee:

Thank you for the opportunity to submit this statement for the record on behalf of the Center for Democracy & Technology[1] about the Administration's proposed cybersecurity legislation.[2] We applaud the Subcommittee for examining these proposals, critical parts of which implicate matters that are within the jurisdiction of the Judiciary Committee, including:

- Data breach notification;
- Amendments to the Computer Fraud and Abuse Act; and
- Cybersecurity information sharing provisions.

Today, I will briefly outline existing threats to our cybersecurity. I will then discuss some of the key distinctions that must be drawn in order to chart a path forward that provides for meaningful improvements in security while ensuring protection for America's cherished rights of privacy and free expression and encouraging continued innovation. I will examine the Administration's cybersecurity proposals in broad strokes, then focus on the three proposals that fit within the Judiciary Committee's jurisdiction. I will suggest an approach to information sharing more likely to protect civil liberties and promote security, explain why the Administration's data breach notification proposal is a good start but needs some modifications, and encourage you to address longstanding concerns with

---

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom. CDT coordinates a number of working groups, including the Digital Privacy and Security Working Group (DPSWG), a forum for computer, communications, and public interest organizations, companies, and trade associations interested in information privacy and security issues.

[2] Text of the White House cybersecurity legislative proposal: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill.pdf (hereinafter, "White House proposal") Section-by-section analysis of the proposal, prepared by the White House: http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/Law-Enforcement-Provisions-Related-to-Computer-Security-Full-Bill-Section-by-Section-Analysis.pdf.

the ambiguity and breadth of the CFAA before considering the penalty enhancements the Administration has proposed.

An overarching theme of our statement for record is that Congress should take a careful, nuanced approach when crafting cybersecurity authorities, avoiding overbroad legislation and the attendant unintended consequences to individual rights and technological innovation. In particular, CDT urges the Subcommittee to think carefully about the role of government in enhancing national cybersecurity. Government action is surely required in some areas, but in others government intervention would raise significant civil liberties concerns, could impede innovation, and might be counterproductive from a security standpoint.

The Cybersecurity Threat

The United States faces significant cybersecurity threats from state actors, from private actors motivated by financial greed, and from terrorists. Earlier this month, the International Monetary Fund (IMF) released news of a major attack on its network that may have given hackers access to the organization's collection of sensitive market data about struggling state economies worldwide.[3] The IMF's announcement came just weeks after one of the nation's largest defense contractors, Lockheed Martin, suffered a "significant and tenacious" cyber attack on May 21.[4] In 2010, the Stuxnet worm, allegedly designed with the involvement of the U.S. government, penetrated the control systems of centrifuges Iran was using to refine uranium, causing hundreds of the centrifuges to spin out of control and damage themselves.[5]

The GAO, among others, has repeatedly criticized the federal government for failing to respond adequately to this threat.[6] The scope of the federal response should not be dictated by the need to react to such criticisms, however, but instead by the actual problems that lie behind them.

---

[3] Sudeep Reddy and Siobhan Gorman, IMF Hit by Cyber Attack, *The Wall Street Journal* (June 11, 2011), http://online.wsj.com/article/SB10001424052702304259304576380034225081432.html.

[4] Gopal Ratnam, U.S. Offers Lockheed Help After 'Tenacious' Cyber Attack, *Bloomberg News* (May 29, 2011), http://www.bloomberg.com/news/2011-05-29/lockheed-offered-help-after-cyber-incident-u-s-government-says.html.

[5] William Broad, et al., Israeli Test on Worm Called Crucial in Iran Nuclear Delay, *New York Times* (January 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[6] *See, e.g.,* Testimony of David A. Powner, Director, Information Technology Management Issues, Government Accountability Office, before the Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity of the House Committee on Homeland Security, *Critical Infrastructure Protection: DHS Leadership Needed to Enhance Cybersecurity* (September 13, 2006), *http://www.gao.gov/new.items/d061087t.pdf*. In 2008, GAO reported that the Department of Homeland Security's U.S. Computer Emergency Readiness Team, which has significant responsibilities for protecting private and governmental computer networks, was failing to establish a "truly national capability" to resist cyber attacks. Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), http://www.gao.gov/products/GAO-08-588. In 2009, GAO testified that DHS had yet to comprehensively satisfy its cybersecurity responsibilities. Testimony of Gregory C. Wilshusen, Director, Information Security Issues, before the Subcommittee on Technology and Innovation of the House Committee on Science and Technology, Government Accountability Office, *Cybersecurity, Continued Federal Efforts Are Needed to Protected Critical Systems and Information (*June 25, 2009), http://democrats.science.house.gov/Media/file/Commdocs/hearings/2009/Tech/25jun/Wilshusen_Testimony.pdf. In 2010, GAO found continued shortcomings. *Cyberspace Policy: Executive Branch Is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership Is Needed*, GAO-11-24 (October 6, 2010), http://www.gao.gov/products/GAO-11-24.

A Careful and Nuanced Approach Is Required for Securing the Internet

In developing a national policy response to cybersecurity challenges, a nuanced approach is critical. One size does not fit all. There are four important sets of distinctions to be drawn in any attempt to tackle the cybersecurity problem:

- First, a distinction must be drawn between those systems that are government-owned and those that are owned by the private sector.
- Second, distinctions must be drawn based on the degree to which the operation of particular systems is vital to the national well-being.
- Third, systems that support free speech and democratic discourse must be distinguished from those that do not.
- Fourth, threats to systems must be distinguished based on the capabilities and intentions of the originators of those threats.

Keeping these distinctions in mind when tailoring a cybersecurity policy to the needs of various systems is vital.

First, it is absolutely essential to draw appropriate distinctions between military government systems, civilian government systems, and systems owned and operated by the private sector. Policy towards government systems, both those in the military domain and those under .gov, can, of course, be much more "top down" and much more prescriptive than policy towards private systems.

Second, particularly with respect to private systems, it is important to remember that most networks are not critical infrastructure and should not be treated as such. While the Internet is a "network of networks" encompassing at its edges everything from personal computers in the home to servers controlling the operation of nuclear power plants, cybersecurity policy should not sweep all entities that connect to the Internet into the same regulatory basket. For example, while it is appropriate to require strong authentication of a user of an information system that contains classified information or controls a critical element of the electric power grid, it would not be appropriate to require authentication of ordinary Americans surfing the Internet on their home computers.

Third, when developing policy responses, appropriate distinctions should be made between the elements of critical infrastructure that primarily support free speech and democratic participation – most prominently the Internet – and those that do not. The characteristics that have made the Internet such a success – its open, decentralized, and user-controlled nature and its support for innovation and free expression – may be put at risk if heavy-handed cybersecurity policies are enacted that apply uniformly to all critical infrastructure. Policies that may be appropriate for the power grid or the banking system may not be appropriate for components of the Internet used for exercising First Amendment rights to speak, associate, and petition the government.

Fourth, any cybersecurity policy must recognize that networked system security is aimed at countering a broad range of threats, from national-level actors engaging in the theft of state secrets to organized criminals engaged in financial fraud to teenage hackers testing their skills. As one cybersecurity expert has noted, it is important to "break down attacks by attribution and

category."[7] Only then can the cybersecurity policy be appropriately tailored to a particular set of threats and not attempt to fit these diverse activities into the same policy framework.

For all these reasons, a sectoral, threat-specific approach is called for. Very careful distinctions – too often lacking in cybersecurity discourse – are needed to ensure that the elements of the Internet critical to new economic models, human development, and civic engagement are not regulated in ways that could stifle innovation, chill free speech, or violate privacy.

Top Line View of the Administration's Cybersecurity Proposals

The White House's legislative package of cybersecurity reforms is largely balanced and contains some appropriate nuance, but includes some troubling provisions.

As compared to the leading Senate cybersecurity bill (the Cybersecurity and Internet Freedom Act (CIFA), S. 413), the Administration's bill could subject more entities and assets to regulation as "critical infrastructure" but that regulation would have a lighter touch. The White House proposal defines critical infrastructure as those entities and assets whose incapacity or disruption would cause "a debilitating impact."[8] This vague language could encompass a broad swath of industry. CIFA does a better job, defining critical infrastructures as those systems whose disruption would cause "a mass casualty event which includes an extraordinary number of fatalities," "severe economic consequences," ''mass evacuations with a prolonged absence," or ''severe degradation of national security capabilities, including intelligence and defense functions."[9] On the other hand, CIFA would impose heavier regulatory burdens on those critical infrastructure owners and operators. CIFA would impose fines for non-compliance with key requirements, while the Administration bill would instead use transparency to encourage compliance, by requiring companies to report publicly their compliance failures. CDT favors the tighter definition of "critical infrastructure" in CIFA (though we would tighten it more) and the lighter regulatory hand of the Administration's bill.

Like CIFA, the White House bill properly makes the Department of Homeland Security (DHS) rather than the Department of Defense (DOD) responsible for securing civilian government systems and for working with the private sector to secure privately held critical infrastructure. The Department of Defense would continue to secure classified systems and the .mil domain. This is the best allocation of responsibilities. There is serious concern that if the National Security Agency or another DOD entity were to take the lead role in cybersecurity for civilian unclassified systems or private sector systems, it would almost certainly mean less transparency, less trust, and less corporate and public participation, thereby increasing the likelihood of failure and decreasing the effectiveness of the effort. The White House legislation draws the lines of authority appropriately.

---

[7] Scott Charney, Rethinking the Cyber Threat: A Framework and a Path Forward 7 (2009) http://download.microsoft.com/download/F/1/3/F139E667-8922-48C0-8F6A-B3632FF86CFA/rethinking-cyber-threat.pdf.

[8] White House proposal, proposed Section 3(b)(1)(A) of the Cybersecurity Regulatory Framework for Critical Infrastructure Act.

[9] S.413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 254 of the Homeland Security Act and amendments to Section 210E of the Homeland Security Act.

The White House bill also wisely omits any provision that would give the President or DHS the authority to limit or shut down Internet traffic to a compromised critical infrastructure information system in an emergency or to disconnect such systems from other networks for reasons of national security.[10] This is good policy for many reasons. To our knowledge, no circumstance has yet arisen that could justify a governmental order to limit or cut off Internet traffic to a particular privately owned and controlled critical infrastructure system. Operators know better than do government officials whether their systems need to be shut down or isolated. In contrast, a new Presidential "shut down" power comes with a myriad of unexamined risks. Even if such power over private networks were exercised only rarely, its mere existence could enable a President to coerce costly, questionable – even illegal – conduct by threatening to shut down a system. It would make private sector operators reluctant to share information because it could be used to order them to shut down. Conversely, when private operators do determine that shutting down a system would be advisable, they might hesitate to do so without a government order, and could lose precious time waiting to be ordered by the government to shut down so as to avoid liability for the damage a shutdown could cause others. Finally, the grant of "shut down" authority to the President for cybersecurity purposes would set a precedent other repressive countries would cite when shutting down Internet services for other purposes, including the stifling of dissent. For all of these reasons, we believe it was wise for the Administration to leave this issue out of its bill.

Finally, the White House legislation honors the President's pledge, made in connection with the 2009 release of the Cyberspace Policy Review, that the federal government would not monitor private networks as part of its cybersecurity program.[11] Monitoring private communications networks is the job of the private sector communications service providers themselves, not of the government. Private sector operators already monitor their networks on a routine basis to detect and respond to attacks as necessary to protect their networks.

Nevertheless, caution must be exercised to ensure that government monitoring of private-to-private communications does not occur as an indirect result of information sharing between the private and public sectors or as an unintended by-product of programs put in place to monitor communications to or from the government.

I will now turn to the Administration's information sharing proposal and its other proposals that fall with the Judiciary Committee's jurisdiction.

White House Information Sharing Proposal Is Overbroad, Raising Privacy Concerns

There is widespread agreement that the current level of cybersecurity information sharing – sharing that is essential to a robust cybersecurity program – is inadequate. Private sector network operators and government agencies monitoring their own networks could better respond to threats if they had more information about what other network operators are seeing.

---

[10] The Cybersecurity and Internet Freedom Act includes such a provision. For an analysis, see http://www.cdt.org/blogs/greg-nojeim/does-senate-cyber-bill-include-internet-kill-switch.

[11] When the White House released the Cyberspace Policy Review on May 29, 2009, President Obama pledged that: *"Our pursuit of cybersecurity will not – I repeat, will not – include monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish as Americans."*

How to encourage more robust information sharing without putting privacy at risk is a central policy challenge that falls to the Judiciary Committee to resolve, because many of the statutes that would have to be amended or overridden are within the Committee's jurisdiction.

a. Information Sharing Between the Private Sector and DHS Under the White House Proposal

As a solution to this problem, the White House has proposed a sweeping information sharing regime that would permit any entity to share with DHS any information the entity may have, including communications traffic, no matter how it was acquired, no matter whether it is thought to include information about an attack or not, and *no matter how use and disclosure of that information would otherwise be restricted by law*, so long as the entity shares it for the purpose of protecting a system against a cybersecurity threat, makes reasonable efforts to remove irrelevant identifying information, and complies with as-yet-unwritten privacy protections.[12] The provision would permit a vast amount of personal information to flow to and from DHS and would effectively override protections in the Wiretap Act, the Electronic Communications Privacy Act, the Communications Assistance for Law Enforcement Act, the Foreign Intelligence Surveillance Act, the Freedom of Information Act, the Privacy Act of 1974, and the Sherman Antitrust Act – statutes within the jurisdiction of the Judiciary Committee.[13] In contrast, the leading Senate cybersecurity bill explicitly requires information sharing relating to cybersecurity to adhere to the statutory schemes governing electronic surveillance.[14]

In other words, this "hub and spoke" model of information sharing in the White House bill puts the Department of Homeland Security at the center. DHS would receive information, analyze it, and could share what it receives as well as the results of its analysis with other entities.

On the plus side, information sharing under the Administration proposal would be voluntary, not mandatory. This is commendable because giving a governmental entity mandatory authority to access private sector data that is relevant to cybersecurity[15] would completely eviscerate the electronic surveillance laws and would undermine the public-private partnership that needs to develop around cybersecurity. In addition, it is good to see that the proposal indicates that DHS's policies and procedures must require destruction of communications intercepted or disclosed for cybersecurity purposes that do not appear to be related to cybersecurity threats.

In other regards, however, the White House proposal raises serious concerns. Most fundamentally, the White House information sharing proposal is based on an unsupported premise: the bill assumes that the government is in the best position to identify threats to private sector networks. Therefore, the proposal would permit the sharing of much Internet traffic with the DHS for analysis. We believe that there is no evidence that the government has either the expertise or the ability to act quickly enough to protect private sector networks better than the private sector can. A better approach is to build on and improve the current network security

---

[12] White House proposal, "Department of Homeland Security Cybersecurity Authority and Information Sharing, proposed Section 245 of the Homeland Security Act.

[13] It also supersedes any state statute that regulates interception, collection, use, and disclosure of communications.

[14] S. 413, Cybersecurity and Internet Freedom Act of 2011, proposed Section 246(c) of the Homeland Security Act.

[15] For an example of such a proposal, see Section 14 of S. 773, the Cybersecurity Act of 2009, as introduced in the 111th Congress.

activities of the private sector. As we explain below in our discussion of an alternative approach to information sharing, much more narrowly targeted changes can be made to the privacy laws. Such changes would promote private sector cooperation for cybersecurity without the risks associated with feeding large amounts of traffic to the government.

Under the White House proposal, DHS could use and retain the communications traffic and other information it receives from service providers, could further disclose that information to private entities and to state and local governmental entities for cybersecurity purposes, and could disclose it to law enforcement entities when it is evidence of a crime. Agencies receiving communications, records, and other disclosures from DHS could use them for cybersecurity and law enforcement purposes and could further disclose them to other entities that have agreed in writing to use them for cybersecurity and law enforcement purposes and to abide by the as-yet-unwritten privacy protections.

The privacy and civil liberties protections in the proposal are weak, difficult to enforce, and principally center on the purpose limitation: limiting information sharing to cybersecurity and law enforcement purposes. Sharing a vast amount of communications traffic could, however, fall within those broadly defined purposes. The legislation would draw no distinctions between sharing content and non-content. While DHS would issue policies and procedures designed to protect privacy and civil liberties, it would have substantial discretion about what to include and little legislative guidance. The proposed legislation does not require that those policies and procedures be subject to notice and comment rulemaking under the Administrative Procedure Act. Moreover, there is no effective way for an aggrieved party to enforce compliance with the policies and procedures because there is no private right of action for violations. Knowing and willful violations are misdemeanors that the Department of Justice has discretion to prosecute; they bring no prison time and fines can be no more than $5,000/incident. Companies and state and local governments that violate the law and share communications and other information for inappropriate purposes, or who fail to strip out irrelevant identifying information, or who violate the privacy policies and procedures, are immune from civil and criminal liability under *all other laws* if they relied in good faith on their own determination that their conduct was permitted in the proposed statute. Finally, the DOJ – a law enforcement agency – would decide which information could be disclosed for law enforcement purposes.

We urge you to assert jurisdiction over cybersecurity information sharing within the purview of the Committee, and to take a more nuanced approach.

b. An Alternative Approach

First, Congress should determine exactly what information should be shared that is not shared currently. Improving information sharing should proceed incrementally. It should start with an understanding of why existing structures, such as the U.S. Computer Emergency Readiness Team ("U.S. CERT")[16] and the public-private partnerships represented by the Information

[16] U.S. CERT is the operational arm of the Department of Homeland Security's National Cyber Security Division. It helps federal agencies in the .gov space to defend against and respond to cyber attacks. It also supports information sharing and collaboration on cybersecurity with the private sector operators of critical infrastructures and with state and local governments.

Sharing and Analysis Centers (ISACs),[17] are inadequate. The Government Accountability Office (GAO) has made a series of suggestions for improving the performance of U.S. CERT.[18] Those suggestions included giving U.S. CERT analytical and technical resources to analyze multiple, simultaneous cyber incidents and to issue more timely and actionable warnings; developing more trusted relationships to encourage information sharing; and providing U.S. CERT sustained leadership within DHS that could make cyber analysis and warning a priority. All of these suggestions merit attention.

Second, an assessment should be made of whether the newly-established National Cybersecurity and Communications Integration Center (NCCIC) has addressed some of the information sharing issues that have arisen. The NCCIC is a round-the-clock watch and warning center established at DHS. It combines U.S. CERT and the National Coordinating Center for Communications and is designed to provide integrated incident response to protect infrastructure and networks.[19] Industry is now represented at the NCCIC[20] and its presence there should facilitate the sharing of cybersecurity information about incidents.

Third, Congress must make a realistic assessment as to whether an information sharing model that puts the government at the center – receiving information, analyzing it, and sharing the resulting analysis and even the raw information itself with industry – could ever be the basis for a rapid-response center possessing adequate expertise to effectively protect an overwhelmingly diverse set of private systems and enough speed and flexibility to respond to fast-moving threats. We have serious doubts. An industry-based model, subject to strong privacy protections, might be able to act more quickly and would raise few, if any, of the Fourth Amendment concerns associated with a government-centric model.

An information sharing approach that relies on the expertise of network operators would be far less disruptive of the current legal framework. Current law already gives communications service providers authority to monitor their own systems and to disclose both to governmental entities and to their own peers information about cyberattack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose, or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider.[21] This includes the authority to disclose

[17] Each critical infrastructure industry sector defined in Presidential Decision Directive 63 has established an Information Sharing and Analysis Center (ISAC) to facilitate communication among critical infrastructure industry representatives, a corresponding government agency, and other ISACs about threats, vulnerabilities, and protective strategies. *See* Memorandum from President Bill Clinton on Critical Infrastructure Protection (Presidential Decision Directive/NSC-63) (May 22, 1998), http://www.fas.org/irp/offdocs/pdd/pdd-63.htm. The ISACs are linked through an ISAC Council, and they can play an important role in critical infrastructure protection. *See* The Role of Information Sharing and Analysis Centers (ISACs) in Private/Public Sector Critical Infrastructure Protection 1 (January 2009), http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf.

[18] *See* Government Accountability Office, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability* (July 2008), http://www.gao.gov/products/GAO-08-588.

[19] *See* DHS Press Release announcing opening of the NCCIC, http://www.dhs.gov/ynews/releases/pr_1256914923094.shtm.

[20] *See* DHS Press Release announcing that it has agreed with the Information Technology Information Sharing and Analysis Center (IT-ISAC) to embed a full time IT-ISAC analyst at the NCCIC, November 18, 2010, http://www.dhs.gov/ynews/releases/pr_1290115887831.shtm.

[21] 18 U.S.C. § 2511(2)(a)(i).

communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, under the Electronic Communications Privacy Act (ECPA), a service provider, when necessary to protect its system, can disclose stored communications[22] and customer records[23] to any governmental or private entity.[24] Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser"[25] if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to investigation of the trespass.[26]

These provisions do not, in our view, authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To interpret them so broadly would destroy the promise of privacy in the Wiretap Act and ECPA. Furthermore, the extent of service provider disclosures to the government for self-defense purposes is not known publicly. We urge the Subcommittee to consider imposing a requirement that the extent of such information sharing be publicly reported, in de-identified form, both to assess the extent to which beneficial information sharing is occurring and to guard against ongoing or routine disclosure of Internet traffic to the government under the self-defense exception.

While current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, the law does not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of those other service providers. Perhaps it should. There may be a need for a very narrow exception to the Wiretap Act, ECPA, FISA, and other laws that would permit disclosures about specific attacks and malicious code on a voluntary basis and that would immunize companies against liability for these disclosures.

The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited. It would thus need to focus on the categories of information that many believe are most important to share: cyberattack signatures and attribution data associated with suspected cyberattacks. Under the approach we envision, these narrowly defined categories of information could be shared more widely, permitting service providers to share directly with each other without going through the government. Rather than taking the dangerous step of overriding the surveillance statutes, such a narrow exception could operate within them, limiting the impact of cybersecurity information sharing on personal privacy. CDT is drafting such an exception and is seeking comment in an effort to ensure that it is effective, is not overbroad, and includes appropriate enforcement and reporting requirements in order to prevent misuse.

Moreover, we urge the Subcommittee, before making any amendments that weaken the

---

[22] 18 U.S.C. § 2702(b)(3).

[23] 18 U.S.C. § 2702(c)(5).

[24] Another set of exceptions authorizes disclosure if "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 [or information] relating to the emergency." 18 U.S.C. §§ 2702(b)(8) and (c)(4).

[25] A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. 18 U.S.C. § 2510(21).

[26] 18 U.S.C. § 2511(2)(i).

controls and privacy protections of the surveillance laws, to consider counterbalancing such changes with legislation to update ECPA by making its privacy protections more relevant to today's digital environment.[27] We would welcome the opportunity to work with the Subcommittee on such legislation.

c. Inter-agency Information Sharing To Prevent Intrusions Into Government Networks

Just as private sector network operators should, and do, monitor their systems for intrusions, the federal government clearly has the responsibility to monitor and protect its own systems. At the same time, such efforts must start with the understanding that citizens' communication with their government implicates the exercise of the First Amendment rights of free speech and petitioning the government, which will be chilled if communications between Americans and their government are routinely shared with law enforcement and intelligence agencies. While the Fourth Amendment may not be implicated in citizen-to-government communications (because those communicating with governmental entities necessarily reveal their communications – including content – to the government), the privacy and civil liberties inquiry does not stop there. Protecting privacy in this context is absolutely critical to giving Americans the necessary comfort to communicate with their government, whether to access services or to criticize government actions.

The White House proposal puts the responsibility to monitor government civilian networks right where it belongs: on the shoulders of the Department of Homeland Security. Under the bill, DHS is charged broadly with engaging in cybersecurity and information infrastructure protection for civilian government systems in what would become new Sections 243 and 244 of the Homeland Security Act. Among other things, DHS would conduct risk assessments of federal systems and maintain a cybersecurity center that would serve as a focal point for cybersecurity information flowing from other governmental agencies at the federal, state, and local level and from the private sector.

We are concerned, though, about the vast scope of the information that could flow to the DHS cybersecurity center from other federal agencies under the White House proposal. The center would be authorized, notwithstanding any law, to intercept, retain, use, and disclose communications traffic to, from, or on any federal system and to deploy countermeasures that block or modify data packets on an automated basis, for cybersecurity purposes.[28] Communications content could be retained, used, and disclosed for cybersecurity purposes when associated with a known or suspected threat, and disclosed to law enforcement when it constitutes evidence of a crime. Users of federal systems would have to be given notice of the monitoring and potential for onward disclosure, but such blanket, mandatory "consent" is not true consent and does not address the First Amendment and privacy concerns. DHS would issue its own privacy and civil liberties policies and procedures in connection with this program, but there would be no independent oversight or auditing to ensure that only traffic to and from

[27] Specifically, the Judiciary Committee should take up the reforms proposed by the Chairman in the Electronic Communications Privacy Act Amendments Act of 2011 (S. 1011) introduced on May 17. There is widespread support for updating ECPA. Digital Due Process, a coalition of technology companies, communications service providers, academics, think tanks, and advocacy groups spanning the political spectrum, has recommended targeted, reasonable updates to ECPA. *See* www.digitaldueprocess.org. The Center for Democracy & Technology is a leading member of DDP.

[28] White House proposal, proposed Section 244(b) of the Homeland Security Act.

government systems is accessed and that ECPA is not being violated through access to purely private communications. Instead, the Secretary of DHS would annually certify the department's compliance with these provisions. No penalty is specified for violations.

While we recognize the right and responsibility of the federal government to monitor its networks for intrusion, the scope of this authorization and lack of independent oversight give us pause because the legislation appears to authorize significantly more activity than is necessary to facilitate operation of DHS's Einstein intrusion detection and prevention system.[29] At a minimum, Congress should consider requiring information collected by the center to be disposed of after a set period; requiring independent audits to ensure that only communications traffic with the government is acquired, retained, and used; and requiring DHS to provide an assessment of the federal laws that are being overridden to permit this monitoring program.

White House Data Breach Notification Proposal A Good Starting Point

The White House proposal would require business entities that hold "sensitive personally identifiable information" (SPII) about more than 10,000 people to notify such persons when the business entity suffers a cybersecurity breach that results in disclosure of SPII, unless the breach involves no reasonable risk of harm to the individual. The White House data breach notification proposal is similar in many respects to the data breach notification provisions in the Personal Data Privacy and Security Act (S. 1151) that Senator Leahy introduced on June 7, 2011.[30] Both contain the same coverage threshold (business entities holding SPII of at least 10,000 people), the same harm standard that obviates notice only when there is no reasonable risk of harm, and similar enforcement schemes.

Data breach notification serves cybersecurity purposes by encouraging large business entities that hold personally identifiable information to better protect that information. It also helps defend against the theft of identity, a problem that can undermine cybersecurity in some contexts. Because most states have already adopted data breach notification laws, breach notification is already effectively the law of the land.[31] The White House proposal would pre-empt those laws and therefore warrants special scrutiny to protect against eliminating current protections or other unintended consequences. It would wisely permit enforcement by state attorneys general and includes an innovative provision to authorize the Federal Trade Commission to adjust the categories of SPII it is intended to protect.

---

[29] The Einstein system is designed to detect and interdict malicious communications traffic to or from federal networks. It assesses network traffic against a pre-defined database of malicious signatures and detects and reports anomalies in network traffic. Einstein operates on the network of an ISP providing service to the government instead of operating on the network of the agency being protected, creating a risk that Einstein could monitor communications traffic that is not to or from a government entity. More about the program can be found in the Einstein 2 Privacy Impact Assessment (PIA) (May 19, 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf, in the PIA for the Einstein Initiative Three Exercise (March 18, 2010), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf, and in legal opinions issued by the Department of Justice concluding that the Einstein program operates lawfully: http://www.justice.gov/olc/2009/e2-issues.pdf (January 9, 2009), and http://www.justice.gov/olc/2009/legality-of-e2.pdf (August 14, 2009).

[30] The data breach notification provisions in the Personal Privacy and Security Act are in Sections 311-322 of the bill, S. 1151.

[31] *See, e.g.,* http://www.cdt.org/policy/congressional-committee-revives-data-security-legislation.

Data breach notification, however, is primarily a consumer privacy matter that CDT believes should be part of comprehensive consumer privacy legislation. We urge that you not miss the forest for the trees: what is needed is legislation to protect consumer privacy in the online and offline world that incorporates the full range of Fair Information Practice Principles. The effort to adopt data breach notification should not undermine the push for baseline consumer privacy legislation. That said, we believe that if Congress does enact federal data breach notification legislation, the White House proposal is a good starting point, although it should be improved as outlined below.

Definition of Sensitive Personally Identifiable Information. The definition in the White House proposal of "sensitive personally identifiable information" should include health data tied to a name or another identifier. Unless this change is made, the bill would pre-empt several state breach notice laws – such as California's[32] – that cover health data linked to the individual's name. The provision empowering the FTC to modify the definition of sensitive information in rulemaking should be retained to help keep the statute up to date as technology evolves, new categories of sensitive data are put at risk, and new identifiers are developed.

Preemption. The White House proposal would override any provision of state law relating to notification by a business entity "of a security breach of computerized data," but it only requires notice of a subset of such breaches: breaches of data containing specifically defined "sensitive personally identifiable information." As a result, for example, given the definitional problem we noted above, notice of breaches involving personally identifiable health data appears to be outside the scope of the proposed notice requirement but within the scope of the preemption section. That one example can and should be fixed in the statute, but the broader problem of the disconnect between coverage and preemption would remain. Preemption of state law should be limited to the data covered by the federal law, permitting states to develop their own laws to address breach of information categories not covered under the proposal.

Notification Trigger. Businesses must notify consumers of data breaches involving SPII under the White House proposal unless the business determines that there is "no reasonable risk of harm or fraud to consumers." Under this formulation, once a company reasonably determines that a breach has occurred, notice is the default and must be given *unless* there is an affirmative finding of no risk. "Harm" should be construed to include reputational harm or embarrassment, and some disclosures of personally identifiable information, such as health information, should be considered harmful per se; with such a construction, the proposal's trigger appears to be effective while avoiding notification regarding truly inconsequential data breaches. We would caution against requiring notification only where harm has occurred or is likely to occur, or only where there was a determination of a significant risk of harm. If a business determines that there is no reasonable risk of harm and that it is not obligated to notify consumers of a breach, the proposal would require the business to submit its risk assessment to the FTC – a critical safeguard for which CDT has advocated.[33]

---

[32] California's data breach law can be found in its Civil Code at Sections 1798.25-1798.29, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29. The White House proposal could also be modified to include an exception, such as is found in California law, specifying that notification is not required for instances of good faith unauthorized access or acquisition of the data by employees or agents of the data holder, provided the data was not further used or disclosed in an unauthorized manner.

[33] http://www.cdt.org/copyright/20090505_data_p2p.pdf.

Delays for Law Enforcement. Under the White House proposal, federal law enforcement agencies can require businesses to delay notification of a breach if the agencies determine that notification would impede a criminal investigation or national security activity. While such a provision is appropriate, it should limit the duration of the periods of delay (e.g., 30 days) and require written authorization by a senior law enforcement official.

Computer Fraud Law Needs Tightening Before Increased Penalties Are Considered

The White House proposal includes various amendments to the Computer Fraud and Abuse Act (CFAA).[34] The White House seeks to further broaden the reach of the CFAA, eliminate its first-time offender provisions, make CFAA violations RICO predicates, impose for conspiracies and attempts the same penalties imposed for completed acts that violate the CFAA, impose mandatory minimums for some violations, and add real property to the assets that can be forfeited in civil or criminal proceedings for conduct prohibited in the CFAA.

The CFAA has served as an important component of the online trust framework, giving the federal government authority to pursue cybercrimes including hacking and identity theft. However, vague terms in the law have fueled troubling civil actions that have stretched the application of the law well beyond that which Congress intended. That stretching of the law has spread to criminal cases under the CFAA as well, and a number of activities having little to do with the kinds of computer "trespasses" that originally motivated Congress to pass the CFAA are now potential crimes. Before it is further expanded or its penalties increased, the statute needs to be tightened and limited to the type of computer hacking activity it was intended to penalize so that it more clearly focuses on conduct that threatens cybersecurity. Only then should any expansion of CFAA penalty provisions be considered.

The CFAA imposes liability when a person accesses a computer without authorization or in excess of authorization. Courts have differed significantly on the definitions of "access" and "authorization." Some courts have interpreted unauthorized access so broadly that companies, when setting the terms of service few users will ever read, effectively determine what user conduct is "criminal." In *U.S. v. Nosal*,[35] the Ninth Circuit held just two months ago that a company's former employee violated the CFAA when he acquired information from the firm's computer network and then repurposed it for his own use, because the employer had not authorized that type of access to information on its network. This prompted one online publication to headline a story about the case "Appeals Court: No Hacking Required to Be Prosecuted as a Hacker."[36] While such activity might constitute theft, or a breach of an employment contract, it is certainly not the kind of conduct that should be addressed in a cybersecurity statute.

Similarly, in the 2008 Lori Drew case, a Missouri mother who impersonated a teenage boy on MySpace in order to taunt her daughter's teenage rival was charged in California under the CFAA after the girl committed suicide. The prosecutor's theory was that Drew exceeded authorized access because the MySpace Terms of Service did not allow users to create

[34] 18 U.S.C. § 1030.

[35] C.A. 9, 10-100038, April 28, 2011

[36] David Kravetz, Appeals Court: No Hacking Required to Be Prosecuted as a Hacker, *Wired: Threat Level* (April 29, 2011), http://www.wired.com/threatlevel/2011/04/no-hacking-required.

accounts under a false name. A federal judge overturned Drew's conviction under the CFAA.[37] While Drew's actions were reprehensible, they did not constitute "hacking" in any meaningful sense. Indeed, if violations of terms of service were per se violations of the CFAA, literally millions of otherwise law-abiding Americans could be subject to criminal prosecution for signing up for a service using a false name, misrepresenting their ages, or exceeding limits on storage capacity. Given that the Ninth Circuit called the result in *Drew* into question with its decision in *Nosal*, further prosecutions for this kind of terms of service violation may well happen.

Meanwhile, plaintiffs in civil cases continue to argue for an *even broader* understanding of unauthorized access. In one recent case, a pregnant mother who sued her employer for pregnancy discrimination was countersued under the CFAA for what the company asserted was unauthorized access to its computer systems: "excessive Internet use" in violation of its acceptable use policy.[38] In another, Sony sued users of its PlayStation devices under the CFAA for tinkering with their own lawfully purchased video game consoles without authorization from the in-box license.[39] Just as early civil cases on contractual authorization led to the questionable prosecutions in Nosal and Drew, so too do these cases point the way to additional dubious uses of the CFAA.

Instead of addressing this vexing problem of overbreadth, the White House proposal would enhance CFAA penalties, encouraging more questionable prosecutions. Penalties for first-time offenders would be increased and in some cases more than doubled. A new mandatory minimum three-year sentence would be imposed on those who, as a component of a felonious violation of the CFAA, damage or attempt to damage a critical infrastructure computer, as long as such damage would "substantially impair" the operation of that computer. The CFAA used to have mandatory minimum sentences, but they were repealed in Section 814(f)[40] of the USA PATRIOT Act in a section captioned "Deterrence and Prevention of Cyberterrorism." Before considering new mandatory minimums, an assessment should be made as to why the old ones were repealed.[41]

The White House proposal also makes the CFAA a RICO predicate – adding it to the list of crimes that can be used to demonstrate a "pattern of racketeering activity" to which severe criminal penalties could be applied. Notably, listing a crime under RICO allows civil plaintiffs to sue for triple damages for violations of that crime.[42] Because of the vagueness of the law, making the CFAA a RICO predicate could have the unintended consequence of making

---

[37] The brief in which CDT joined in the Lori Drew case can be found here: http://www.eff.org/files/filenode/US_v_Drew/Drew_Amicus.pdf.

[38] *Lee v. PMSI, Inc.*, 2011 WL 1742028 (M.D.Fla. 2011).

[39] Orin Kerr, Today's Award for the Silliest Theory of the Computer Fraud and Abuse Act, *The Volokh Conspiracy* (January 13, 2011), http://volokh.com/2011/01/13/todays-award-for-the-lawyer-who-has-advocated-the-silliest-theory-of-the-computer-fraud-and-abuse-act/.

[40] This section required the U.S. Sentencing Commission to "amend the Federal sentencing guidelines to ensue that any individual convicted of a violation of [18 U.S.C. § 1030] can be subjected to appropriate penalties, without regard to any mandatory minimum term of punishment." It also increased potential maximum penalties under the CFAA and broadened the conduct to which it applied.

[41] Orin Kerr, Congress Considers Increasing Penalties, Adding Mandatory Minimum Sentences to the Computer Fraud and Abuse Act, *The Volokh Conspiracy* (May 24, 2011), http://volokh.com/2011/05/24/congress-considers-increasing-penalties-adding-mandatory-minimum-sentences-to-the-computer-fraud-and-abuse-act/.

[42] 18 U.S.C. § 1964(c).

legitimate businesses subject to civil RICO suits for routine and normal activities. While such lawsuits may be legally groundless, their reputational impact and the prospect of treble damages and attorneys fees will often drive legitimate businesses into settling unsustainable charges. Moreover, such lawsuits would intensify the feedback loop between civil and criminal law that has led to the current overbreadth on the criminal side: as civil plaintiffs, newly incentivized to sue under the CFAA, continue to take novel theories to court, the set of activities which are considered criminal will likely continue to expand.

Finally, the proposal adds "real property" to items subject to civil forfeiture, as long as that property was used or was intended to have been used to commit or facilitate the crime. This would subject to forfeiture the house of the parents of a teenage hacker who has used a computer to attempt to break into someone's network if the parents were aware of this conduct.

The conduct constituting a violation of the CFAA must be narrowed before Congress considers legislation to extend the statute and enhance the penalties under it. As Professor Orin Kerr has suggested, the statute would be significantly improved by clarifying the definition of "authorization" to state that only actions exceeding *code-based* authorization are sufficient to constitute a violation.[43] Clarifying the meaning of "access" and "damage" under the statute would help as well. Even with such changes, however, some of the administration's proposals, such as mandatory minimum sentences for certain CFAA violations, would continue to raise concerns.

Conclusion

We appreciate the opportunity to testify about the White House cybersecurity proposals. They raise critical issues that fall squarely within the Judiciary Committee's jurisdiction and within the jurisdiction of the Subcommittee. We urge you to assert jurisdiction where appropriate, and we look forward to working with you to make progress on these important matters, while at the same time protecting the privacy rights of Americans.

[43] Orin S. Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, 78 *N.Y.U. L. Rev.* pp. 1596-1668 (November, 2003) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740.