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 OF GREGORY T. NOJEIM

SENIOR COUNSEL AND DIRECTOR OF THE FREEDOM, SECURITY AND TECHNOLOGY PROJECT

THE CENTER FOR DEMOCRACY AND TECHNOLOGY

HEARING BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE ON PROTECTING AMERICA FROM CYBER ATTACKS: THE IMPORTANCE OF INFORMATION SHARING

January 28, 2015

Chairman Johnson, Ranking Member Carper, and members of the Committee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy and Technology. CDT is a nonpartisan, non-profit technology policy advocacy organization dedicated to protecting civil liberties and human rights on the Internet, including privacy, free speech, and access to information. I direct the Freedom, Security and Technology Project at CDT. It works to develop and promote policies that safeguard individuals from overbroad government surveillance while preserving the government's ability to protect national security against evolving threats. We applaud the Committee for holding the first hearing of the 114th Congress on cybersecurity, an important issue that the Homeland Security and Government Affairs Committee has a key role in addressing.

Today I will explain how Congress can embrace cybersecurity information sharing policies with appropriate authorities and safeguards that enhance both privacy and security. I will first describe the cybersecurity threat and explain the role that information sharing can play in countering that threat. I will then identify different approaches to encouraging information sharing as well as the essential civil liberties attributes of a successful information sharing policy. I will also measure pending legislative proposals against those attributes.

Cyber attacks represent a significant and growing threat. Earlier this year, a study by the Center for Strategic and International Studies estimated that the global cost of cyber crime has reached over $445 billion annually.[1] According to an HP study released in October 2014, the average cost of cyber crime to each of 50 U.S. companies surveyed had increased to $12.7 million per company, up

[1] Center for Strategic and International Studies, *Net Losses: Estimating the Global Costs of Cybercrime* (June 2014), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

from $6.5 million per company just four years ago.[2] Frequency and intricacy of attacks has increased as well. The same study concluded that the number of successful attacks per company per year has risen by 144 percent since 2010, while the average time to resolve attacks has risen by 221 percent.[3]

Major cyber attacks represent an ongoing hazard to our financial and commercial sectors, with potential to harm both important institutions and individual online users. 2014 saw major attacks affecting large numbers of people against companies such as Target, J.P. Morgan Chase, Home Depot, and most recently, Sony Pictures.[4] In addition to direct harms – which are substantial – these large scale and highly publicized attacks threaten to chill use of online services.

Unfortunately, there is no "silver bullet" that will wipe away the danger of cyber attacks. Cyber attacks are constantly evolving, and defending against them requires a range of actions from both governmental and private entities. Most successful attacks could be stopped by basic security measures, such as frequently changing passwords, patching servers, detecting insider attacks, and educating employees about risks. Thus, while information sharing is an important tool for enhancing cybersecurity, it is also important to maintain a broad perspective and encourage other measures that would also increase digital hygiene.

I. Information sharing is an important component of an effective cybersecurity policy and must be accompanied by appropriate privacy protections at all levels.

There is widespread agreement that the sharing of information about cyber attacks, threats and vulnerabilities is a valuable component of an effective cybersecurity policy. As detailed by the National Institute of Standards and Technology's draft "Guide to Cyber Threat and Information Sharing," benefits of information sharing include: 1) Greater awareness of specific cyber threats, and of defenses against them, 2) development of more robust threat indicators, 3) enhanced defensive agility, 4) rapid notification to victims of cyber attacks, and 5) improved ability to efficiently process and preserve criminal evidence.[5]

While cyber attacks sometimes employ malware that exploits "zero-day" vulnerabilities – previously undiscovered vulnerabilities – many cyber attacks are repetitive. Cyber criminals often recycle previously used vulnerabilities, deploying old exploits on systems and software that were not previously attacked. Information sharing can limit the effectiveness of these "recycled" threats: the victim of the first attack can share information that can be used by other potential victims to defend against future iterations of the same attack. Further, by making cyber criminals take additional steps to modify their attacks rather than simply replicating attacks on previously used vulnerabilities, the cost of engaging in cyber attacks increases, thereby decreasing the incentive to engage in them.

---

[2] HP, *Ponemon Institute 2014 Cost of Cyber Crime Study* (September 2014), *available at* http://h17009.www1.hp.com/pub/msc/29FD917C-64F3-46A7-955C-EF9D2F8D9E3C.pdf.

[3] *Id.*

[4] Sharone Tobias, *2014: The Year in Cyberattacks*, Newsweek (December 31, 2014), *available at* http://www.newsweek.com/2014-year-cyber-attacks-295876.

[5] Chris Johnson et al, *Guide to Cyber Threat Information Sharing*, National Institute of Standards and Technology (October 2014), 7*, available at* http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf.

Many information sharing mechanisms are already in place, are providing benefits, and should be supported, improved, and built upon. They include sector-specific Information Sharing and Analysis Centers (ISACs) and the DHS Enhanced Cybersecurity Services Program.[6]

The cybersecurity proposal the Administration announced earlier this month[7] includes an important requirement for cybersecurity information sharing: Privacy protections should be applied prior to *any level* of information sharing. Privacy safeguards apply to 1) company sharing with the government, 2) company sharing with the private information sharing hubs the proposal would authorize, and 3) inter-agency sharing. The Administration proposal requires front-end protections prior to a company's sharing of cyber threat indicators – reasonable steps to remove personally identifiable information believed to be unrelated to the threat – as well as privacy guidelines to govern information sharing among government agencies.[8] This contrasts with the Cyber Intelligence Sharing and Protection Act (CISPA),[9] which does not require reasonable efforts to remove such PII prior to sharing, and requires instantaneous, real-time transfer of information, including communications content, from the Department of Homeland Security (DHS) to other government agencies – including the National Security Agency (NSA). While the Administration proposal has ambiguities and omissions that might render it less effective than it could be in protecting privacy,[10] it demonstrates that a viable information sharing policy can empower all players in the cybersecurity ecosystem to rapidly transmit cyber threat information with civil liberties protections built in.

Quite simply, the American public should not – and need not – be forced to choose between being hacked by cyber criminals and being snooped on by the government.

II. Information sharing among private entities avoids significant civil liberties concerns and should be encouraged.

In this section and the next, I describe two approaches to information sharing that we favor because they minimize civil liberties risks – 1) private-to-private information sharing and 2) information sharing facilitated by limited amendments to the surveillance statutes that do not necessitate creation of complex, new programs.

---

[6] US Dept. of Homeland Security, Enhanced Cybersecurity Services (September 8, 2014) http://www.dhs.gov/enhanced-cybersecurity-services

[7] The White House, Updated Department of Homeland Security Cybersecurity Authority and Information Sharing, Section by Section, Analysis (January 13, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/information-sharing-legislation-section-by-section.pdf.

[8] Some in industry contend that an obligation to endeavor to remove personally identifiable information before cyber threat indicators are shared would prove too burdensome, particularly for small companies. We believe that the same automated systems that would identify the threat information that could be shared because it meets the definition of cyber threat indicator would be configured to omit irrelevant PII, thus mitigating the burden. Under questioning by Rep. Adam Schiff (D-CA) at a 2013 House Intelligence Committee hearing, certain industry representatives confirmed that a requirement to remove PII irrelevant to a cyber threat prior to information sharing is reasonable and would not dissuade them from participating in a cybersecurity program. *See*, https://www.eff.org/deeplinks/2013/02/industry-experts-congress-we-can-remove-personally-identifiable-information.

[9] H.R. 234, 2015.

[10] See infra, Section VII.

The most important type of information sharing to incentivize is that between private entities. This is because entities in the private sector own and operate most of the critical infrastructure in the country that must be protected against cyber attacks. Information sharing can occur directly between private entities, without any government involvement. Threat analysis would occur more often at the private company level as opposed to within the government.

This not only makes the process more efficient, it does not raise many of the privacy and civil liberties concerns attendant to private-to-government information sharing. For example, private-to-private sharing of information does not convey communications content to the NSA, and does not raise concerns that this sharing of information could result in a new surveillance program through a backdoor, which Congress did not intend to authorize.

The White House proposal does little to encourage company-to-company information sharing – it extends no liability protection for this sharing – and this is a significant shortcoming. Instead, the Administration proposal encourages private-to-private sharing only through information-sharing hubs that the government has designated as such. This approach may have been taken because the Administration and industry have had difficulty in agreeing on a mechanism to ensure that companies play by the rules when they share information company-to-company. We believe such a mechanism is a pre-requisite to expanding such sharing.

One barrier to company-to-company information sharing – antitrust concerns – was largely put to rest by a Department of Justice/Federal Trade Commission policy guidance issued last year.[11] The U.S. Chamber of Commerce correctly read the guidance as a positive step and as a statement, "…that antitrust concerns are not raised when companies share cyber threat information with each other…."[12]

In addition to sharing between private entities, sharing from governmental to private entities represents an area for opportunity. To the extent that the government has information that would be useful for private entities to defend themselves, it should declassify it as necessary and share it. It can do this under current law. As with private-to-private sharing, government-to-private sharing can augment cybersecurity without the same risks to privacy that private-to-government sharing creates.

III. Current law permits sharing to protect oneself, but not to protect others. This can and should be addressed with a narrow amendment.

The other approach to information sharing that we commend to you involves only limited amendments to surveillance statutes. Current law does allow some degree of cybersecurity information sharing, but it does not meet present cybersecurity needs. Communication service providers are permitted to monitor their own systems and to disclose to governmental entities,

---

[11] *Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information*, April 14, 2014, http://www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing.

[12] *See*, Ann M. Beauchense, *Agencies' Statement on Antitrust and Cyber Information Sharing is Encouraging*, The US Chamber of Commerce (April 11, 2014), *available at* https://www.uschamber.com/blog/agencies-statement-antitrust-and-cyber-information-sharing-encouraging.

and other service providers, information about cyber attacks for the purpose of protecting their own networks. In particular, the 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.[13] This includes the authority to disclose communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, the Electronic Communications Privacy Act (ECPA) permits providers to disclose stored communications[14] and customer records[15] to any governmental or private entity in order to protect its own systems. 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" 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 an investigation of the trespass.[16]

While current law authorizes providers to monitor their own systems and to voluntarily disclose communications 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 *other* service providers. Thus, there may be a need for an exception to the Wiretap Act and ECPA to permit disclosures to others about specific attacks.

Any such exception should be narrow so that routine disclosure of Internet traffic to the government or other service providers remains clearly prohibited. It should bar unrestricted disclosure to the government of vast streams of communications data, and permit only the disclosure of carefully defined cyber attack signatures, cyber attack attribution information, and the method or the process of a cyber attack. It should also include privacy protections such as those described below. 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. Companies that share information under such a narrow exception will enjoy the liability protections already built into theses statutes. As other statutes that limit information sharing for cyber security purposes are identified, Congress may consider additional exceptions.

We encourage you to embrace this focused approach to enhancing cybersecurity information sharing. If it proves inadequate to promote information sharing, broader, riskier approaches that operate "notwithstanding any law" can be considered. However, because all of the major cybersecurity information sharing proposals take what we believe to be the overbroad, risky approach of trumping all other laws, they are addressed in some detail below. The civil liberties protections we describe are an important part of any cybersecurity information sharing program, but are particularly important for the broader, riskier approaches.

[13] 18 U.S.C. § 2511(2)(a)(i).

[14] 18 U.S.C. § 2702(b)(3)).

[15] 18 U.S.C. § 2702(c)(5)).

[16] 18 U.S.C. § 2511(2)(i).

IV. Civilian control of cybersecurity activity involving the civilian private sector should be maintained.

For numerous reasons, it is critical that if private, civilian entities are authorized to share users' communications information with governmental entities for cybersecurity reasons, that information should flow to and be controlled by a civilian agency – DHS – rather than a military agency, such as the NSA or Cyber Command.

First, civilian agencies are more transparent; for understandable reasons, intelligence agencies are more opaque. Details about the scope and nature of civilian agency activities, privacy protections – such as minimization rules – and interpretation of relevant law are all more available from civilian agencies. The Snowden disclosures demonstrate the contrasting approach of military intelligence agencies. Until June 2013, the public was unaware that the PATRIOT Act had been interpreted to authorize bulk collection of metadata, and that domestic phone call and Internet activity records were being collected, used, and retained for years.

Second, DHS has a well-established, statutory, and well-staffed privacy office. The NSA's privacy office was established just last year, with a huge mandate and relatively tiny staff.

Third, the NSA has multiple missions that can create conflicts about how to treat the cyber threat and cyber vulnerability information that it receives. In addition to its mission of defending information security, the NSA is also tasked with gathering signals intelligence, including through use of vulnerabilities. If the NSA receives information regarding a cyber threat or cyber vulnerability, its intelligence-gathering mission may be prioritized, leading the agency to hide, preserve and exploit the vulnerability, rather than disclose it to the entity that could patch the vulnerability.[17] It is for this precise reason that the President's independent Review Group on Intelligence and Communications Technologies recommended moving NSA's information assurance mission into a separate agency in the Department of Defense.[18] Further, while information may be shared to respond to cyber threats, NSA may re-purpose it to support its intelligence-gathering mission, creating a new surveillance program operating under a cybersecurity umbrella.

Finally, public trust in military intelligence agencies was severely compromised in both the U.S. and abroad by the NSA activities that Edward Snowden disclosed. Mass collection of sensitive communications and communications information pertaining to individuals not suspected of

---

[17] Exploitation of vulnerabilities is regularly used by the NSA for signals intelligence purposes. *See e.g.*, Ryan Gallager and Glenn Greenwald, *How the NSA Plans to Infect Millions of Computers With Malware*, The Intercept (March 12, 2014), available at https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/; *see also*, Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post (October 30, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[18] *See*, *The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, (Dec. 12, 2013), 185, *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("Those charged with offensive responsibilities still seek to collect SIGINT or carry out cyber attacks. By contrast, those charged with information assurance have no effective way to protect the multitude of exposed systems from the attacks. The SIGINT function and the information assurance function conflict more fundamentally than before. This conclusion supports our recommendation to split the Information Assurance Directorate of NSA into a separate organization.")

wrongdoing has led to strong demands for greater protections. If NSA or Cyber Command were to serve as the government entity receiving cyber threat information from communications service providers, it would almost certainly mean less trust, and therefore less corporate participation. Indeed, in the wake of revelations regarding the PRISM program, many major tech companies stated that they would not voluntarily share users' information or private communications with the NSA.[19] Thus, preserving civilian control by putting a civilian agency in charge of cyber threat indicators shared by the civilian sector with the government will not only enhance civil liberties, it would increase the effectiveness of this effort to promote security.

Main cybersecurity proposals have inadequately addressed this issue. While the Administration proposal requires application of privacy guidelines before information shared with DHS is sent to military agencies including the NSA, it is not clear that the guidelines will offer sufficient protections.[20] CISPA is even more problematic. It requires real-time sharing from DHS to NSA,[21] effectively creating the same concerns as company information sharing directly to the military. The Senate Intelligence Committee's Cybersecurity Information Sharing Act (CISA), reported out in 2014 takes the same problematic approach as does CISPA.[22]

V. Use restrictions should ensure that information shared for cybersecurity purposes is only used for cybersecurity, with narrow exceptions.

Cybersecurity legislation should not be warped into a backdoor wiretap, whereby communications shared to respond to cyber threats are provided to law enforcement agencies that use them for investigation of unrelated offenses, or to intelligence agencies that use them for national security purposes other than cybersecurity. Doing so undermines the privacy protections built into the Wiretap Act, ECPA, and the Foreign Intelligence Surveillance Act, and the critical role of an independent judiciary in authorizing surveillance for criminal and foreign intelligence investigations. For example, the user communications information that a company shares with the government could be stored, then mined for information relevant to crime or national security using identifiers of U.S. persons. Instead of applying for the court order that would permit access to such information under a surveillance statute when the information pertains to a US person or a person in the U.S., the government could simply pull the information from "the corporate store" as the NSA does for the telephone call records it collects in bulk under Section 215 of the PATRIOT Act.[23] Overbroad use permissions also create a perverse incentive for government to retain communications content, and even pressure companies into providing it more frequently than is necessary for cybersecurity.

---

[19] *See*, Gregory Ferenstein, *Report: NSA Collects Data Directly From Servers of Google, Apple, Microsoft, Facebook and More*, Tech Crunch (June 6, 2013), *available at* http://techcrunch.com/2013/06/06/report-nsa-collects-data-directly-from-servers-of-google-apple-microsoft-facebook-and-more/; *see also*, Chenda Ngak, *Apple, Google, Facebook, Yahoo, Microsoft, Paltalk, AOL issue statements of denial in NSA data mining*, CBS News (June 7, 2013), *available at* http://www.cbsnews.com/news/apple-google-facebook-yahoo-microsoft-paltalk-aol-issue-statements-of-denial-in-nsa-data-mining/.

[20] See infra, Section VII.

[21] H.R. 234, Sec. 2(b)(4), 2015.

[22] S. 2588, Sec. 5(c)(1)(C), 2014.

[23] See Patrick Toomey, ACLU, "Let's Lock Down the NSA's Shadow Database," https://www.aclu.org/blog/national-security/lets-lock-down-nsas-shadow-database.

Some law enforcement use of cyber threat information is appropriate. For example, the goal of improving cybersecurity is promoted by prosecuting those who propagate attacks. Permitting information shared with government for cybersecurity reasons to be used for investigation and prosecution of cybersecurity crimes is logical, if those crimes are carefully described. Allowing information to be used by law enforcement to prevent imminent risk of death or serious bodily harm is also a sensible limitation.

Thus, cybersecurity legislation should make it clear that information shared under the bill can be used for cybersecurity purposes (to protect computers against cyber attacks and to mitigate such attacks), to investigate and prosecute people for engaging in such attacks, and to prevent imminent risk of serious bodily harm or death.

VI. Congress should not authorize countermeasures that amount to "hacking back" and should not extend liability protection to "hacking back."

In considering new cybersecurity policies, Congress should be careful to provide no authority to engage in countermeasures against cyber attacks that amount to "hacking back" against entities believed to have perpetrated the original cyber attack. Allowing such countermeasures – or providing liability protection for them – risks opening a Pandora's Box of unintended results that could do far more harm than good for Internet infrastructure and security.

The recent cyber attack against Sony Pictures highlights two of the greatest problems that authorization for such countermeasures would raise: attribution and escalation. It can be extremely difficult to reliably ascertain the source of a cyber attack and to finger the responsible party.[24] Hackers can not only obscure the source of their attack, but also leave a "false trail" that will lead to misattribution.[25] Authorizing companies to use countermeasures that compromise data that is not on their own networks risks harm innocent third parties. Limiting liability for causing such harm would only encourage it.

Private "hacking back" also risks escalation with national security implications that go far beyond the interests of the company engaging in the hack back. As computer security expert Bruce Schneier notes, "The blurring of lines between individual actors and national governments has been happening more and more in cyberspace."[26] Authorizing hacking back risks companies engaging in hostile acts against foreign nations and their agents, potentially leading to a series of increasingly damaging cyber attacks, or even kinetic attacks. The possibility of misattribution significantly heightens the escalation problem.

---

[24] *See*, Bruce Schneier, *Attributing the Sony Attack*, Scneier on Security (Janary 7, 2015), *available at* https://www.schneier.com/blog/archives/2015/01/attributing_the.html ("When it's possible to identify the origins of cyberattacks -- like forensic experts were able to do with many of the Chinese attacks against US networks -- it's as a result of months of detailed analysis and investigation").

[25] *See*, Jack Goldsmith, *How Cyber Changes the Laws of War*, EJIL (2013), Vol. 24 No. 1, 129–138, 132, *available at* http://ejil.oxfordjournals.org/content/24/1/129.full.pdf ("A thoughtful adversary can hide its tracks by routing attacks or exploitations through anonymizing computers around the globe. In 2009, a denial-of-service attack – a massive spam-like attack that clogs channels of communication – brought down some American and South Korean websites. Early reports said that the attack came from North Korea, but a few weeks later it was learned that the attack originated in Miami (and possibly, before Miami, elsewhere) and was routed through North Korea. It is still not known for sure who launched the attack, or from where.")

[26] Bruce Schneier, *Attributing the Sony Attack*, Schneier on Security (January 7, 2015), *available at* https://www.schneier.com/blog/archives/2015/01/attributing_the.html.

A foreign country could engage in a cyber attack against a U.S. company and leave a false trail leading to another nation – something that has been discussed as a viable possibility for the Sony attack[27] – with the goal of provoking an international incident between that nation and the United States. An activity with this level of risk is not something a private company should be authorized to engage in.

Despite the serious concerns about countermeasures that could affect data not on one's own network, authorization of countermeasures and liability protection for using them has received increased attention in recent years. CISA and the 2012 SECURE IT Act would have explicitly authorized countermeasures without adequate limitations,[28] while CISPA strongly risks authorizing problematic countermeasures.[29] The Administration's proposal does not include new authority for engaging in problematic countermeasures.

VII. The privacy provisions of the Administration cybersecurity proposal offer a path forward on some issues, but not on others.

The Administration's cybersecurity proposal wisely requires application of privacy protections prior to all levels of sharing. On the front-end, companies are required to make reasonable efforts to strip out information that can be used to identify specific persons prior to sharing with the government. Within government, inter-agency sharing is to be regulated by privacy guidelines, which must establish rules for 1) destruction of irrelevant information, 2) anonymizing information retained, 3) law enforcement use, and 4) the possibility of disciplinary measures against government employees and agents for privacy violations.

However, the privacy protections have ambiguities and omissions that could severely undercut their effectiveness. While companies would be required to make reasonable efforts to remove personal information prior to sharing, this only includes information that is " reasonably believed to be unrelated to [a] cyber threat." Personally identifiable information about a *victim* of a cyber attack will often include information "related to a cyber threat." Depending on the circumstances, such information may, or need not, be shared to describe or counter the threat. Thus, reasonable efforts to remove personally identifiable information that is "not necessary to describe or counter the cyber threat" should instead be required.

It is difficult to evaluate how effective the privacy guidelines called for in the Administration's proposal will be as they are, of course, not yet written. The bill should provide more guidance about what should be included in the privacy guidelines. In addition to the four specific requirements set forth in the draft, Congress should require that the privacy guidelines comport

---

[27] *See*, Jack Goldsmith, *The Sony Attack: Attribution Problems, and the Connection to Domestic Security*, Lawfare (December 19, 2014), *available at* http://www.lawfareblog.com/2014/12/the-sony-hack-attribution-problems-and-the-connection-to-domestic-surveillance/ ("much more importantly, it is at least possible that some other nation is spoofing a North Korean attack. For if the United States knows the characteristics or signatures of prior North Korean attacks, then so too might some third country that could use these characteristics or signatures – "specific lines of code, encryption algorithms, data deletion methods, and compromised networks," and similarities in the "infrastructure" and "tools" of prior attacks – to spoof the North Koreans in the Sony hack").

[28] S. 2588, Sec. 4(b), 2014; S. 3342 Sec. 102(a), 2012.

[29] H.R. 234, Sec. 3(a), 2015.

with the Fair Information Practice Principles that the DHS promulgated in 2008,[30] during the George W. Bush Administration. Subjecting any privacy guidelines to a public notice and comment process would also be wise. Legislation should also require a timeline for implementation of the privacy guidelines that ensures that newly authorized information sharing occurs only after the guidelines are in place. There is no timeline in the Administration's proposal, and as a result, information sharing could be conducted for a time without privacy guidelines.

There are also significant concerns regarding the law enforcement use restrictions in the Administration's proposal. They permit use to investigate, prosecute, disrupt, or otherwise respond to "computer crimes," a threat of death or serous bodily harm, a serious threat to a minor, and an attempt or conspiracy to commit such offense. The term "computer crimes" is undefined, inviting an overbroad interpretation, such as any crime perpetrated in part through use of a computer, which would sweep in many crimes having nothing to do with cybersecurity. Instead, use of cyber threat indicators to investigate and prosecute violations of the Computer Fraud and Abuse Act, 18 USC 1030, and state law counterparts, should be permitted. Because the CFAA is so broad, an even better approach would permit use of cyber threat indicators only to investigate crimes an element of which is cyber threat conduct defined in the proposal if engaged in intentionally.[31] The Administration's proposal also permits law enforcement use in responding to threats of serious bodily harm, but does not require the threat be imminent. This could allow law enforcement to retain and use electronic communications based on suspicion of a vague or unsubstantiated threat.

Finally, the proposal counts on the government to enforce, against the government, the privacy guidelines the government itself authored. This is a weak enforcement mechanism. Instead, cybersecurity legislation should authorize a private right of action, with liquidated damages and attorney's fees, for those who suffer harm if a governmental entity does not abide by the privacy guidelines. CISPA authorizes such a private right of action;[32] the Administration proposal does not.

VIII. Federal data breach notification legislation should properly account for corresponding state laws.

Data breach notification is an area of cybersecurity where significant progress has been made at the state level. Currently, forty-seven states have laws requiring companies to notify consumers or regulatory agencies when breaches occur and personally identifiable information is disclosed. Because many businesses holding sensitive consumer data operate nationwide, they tend to follow the highest breach notification standard for simplicity's sake, and as a result, consumers across the country tend to benefit from the most robust state laws. Thus, while a

[30] Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, *Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 29, 2008*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[31] Under this approach, cyber threat indicators shared "notwithstanding any law" could be use to investigate and prosecute a crime an element of which involves intentionally "damaging or impairing the integrity, confidentiality, or availability of an information system or unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system," with certain exceptions.

[32] H.R. 234, adding Section 1104(d) to the National Security Act of 1947.

preemptive federal law might add only *some* simplicity for business, it could actually *weaken* protection for consumers by superseding stronger state laws.[33]

In fact, the preemption clause of the Administration's data breach notification proposal is particularly troubling. This provision is overly broad, pre-empting all state laws that are related to data breach notification— even notification laws that cover data sets not covered by the Administration's proposal. At the very least, federal data breach legislation should only preempt state laws that address the same areas that as a federal law — any exemptions to federal regulation should also apply to preemption. The Administration proposal also fails to include a private right of action, which would preempt the 17 state laws that offer this enforcement mechanism, removing an important incentive to companies to ensure that personally identifiable data is protected.

If federal legislation on the issue is to be considered, it should introduce new protections not present in state law, such as requiring access to information maintained by data brokers, which would allow consumers to more effectively monitor potential risks and the effects of a breach.

IX. Recent events and disclosures should prompt Congress to encourage cybersecurity measures beyond information sharing.

The Snowden disclosures and major cyber attacks conducted in the last year demonstrate that although new information sharing authority has value, other cybersecurity measures should be a high priority for Congress as well. While information sharing would not have averted the Sony or Target attacks as well as other prominent attacks, improved employee education and application of best practice internal security measures might have.[34] Government's best means of preventing attacks like these may be to develop incentives that encourage companies to practice better digital hygiene.

Last year, a number of companies, security experts, and civil society groups with expertise in tech policy – including CDT – issued a letter outlining several of these measures.[35] First, the government should offer incentives to companies that adopt strong security practices, including resolving known vulnerabilities in a timely fashion, making systems more resilient against attacks, and improving security architecture by design. Second, Congress should empower a civilian federal agency to perform the government's information assurance function for the civilian sector, thereby ensuring that conflicting offensive missions would not override information assurance objectives. Third, all administrative agencies that collect or handle personal information should be required to have a Chief Information Officer, Chief Privacy Officer, and Chief Technology Officer, tasked with establishing and publishing responsible disclosure policies and processes for vulnerability reporting. Fourth, government should offer resources to educate users, companies, and other actors on best practices for avoiding and

[33] Gautam Hans, Center for Democracy & Technology, "White House Data Breach Legislation Must be Augmented to Improve Consumer Protection," https://cdt.org/blog/white-house-data-breach-legislation-must-be-augmented-to-improve-consumer-protection/.

[34] Mark Jaycox, *Congress Should Say No to "Cybersecurity" Information Sharing Bills*, The Electronic Frontier Foundation (January 8, 2015), *available at* https://www.eff.org/deeplinks/2015/01/congress-should-say-no-cybersecurity-information-sharing-bills.

[35] Available at https://www.accessnow.org/page/-/Veto-CISA-Coalition-Ltr.pdf.

mitigating cybersecurity threats.[36] Fifth, the United States should foster greater international dialogue on cyber conflict standards to discourage foreign attacks. Sixth, government should establish strong transparency obligations that provide access to both oversight bodies and the public.

Congress should also consider the impact on Americans' cybersecurity of NSA stockpiling of vulnerabilities to support offensive cybersecurity operations. Any vulnerability that is left undisclosed and unpatched could also be discovered and used by a bad actor, as shown by recent reports that the Sony hack employed a zero-day vulnerability.[37] In order to promote better cybersecurity and reduce attacks against the United States, the Review Group on Intelligence and Communication Technologies recommended that the government avoid stockpiling zero-days, and instead disclose vulnerabilities to the parties that can patch them."[38] Congress should embrace this recommendation.

X. Conclusion.

The year ahead offers a promising opportunity to move forward in development of new measures that will improve cybersecurity, including information sharing. Despite the scope of the threat, cybersecurity information sharing should be incentivized with care due to the significant risk of harm the privacy of average Internet users. We look forward to working with the Committee and the Congress in pursuit of both security and privacy, and ensuring that the Internet continues to be a vibrant force for innovation, individual empowerment, and prosperity.

---

[36] *See*, Joseph Lorenzo Hall, *Improve Digital Hygiene*, The New York Times (February 23, 2013), *available at* http://www.nytimes.com/roomfordebate/2013/02/21/should-companies-tell-us-when-they-get-hacked/improve-digital-hygiene.

[37] Arik Hesseldahl, Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability, Re/Code (January 20, 2015), available at http://recode.net/2015/01/20/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability/.

[38] *The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, (Dec. 12, 2013), 219, *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.