

## **Cybersecurity: Ideas Whose Time Has Not Come—and Shouldn't**

GREGORY T. NOJEIM\*

Cybersecurity is a serious problem that Congress and the Executive Branch need better to address. Ideas about how to address this problem abound and are being put into legislation that members of Congress are eager to advance. Some are obviously needed, have little downside, and should have been enacted years ago. But, a surprisingly large handful cut the wrong way; while well-intentioned, these ideas for statutory changes to deal with the significant cybersecurity problems we face could backfire and make us less secure. Unlike administrative initiatives adopted entirely within the discretion of the executive branch—and which can be revised or repealed just as easily—policy choices embodied in statutes can be revised only through subsequent legislation, making such decisions very difficult to reverse even when their negative impact becomes apparent. Some would undermine cybersecurity instead of furthering it.

The negative effects of these policy proposals can be broken down into five categories:

- (i) an unexpected economic or systematic impact;
- (ii) poor decisions that result from moving the power to decide away from the best decision-maker;
- (iii) slowing down decision-making or information sharing necessary to making the right decision;

---

\* Gregory T. Nojeim is a Senior Counsel and Director of the Project on Freedom, Security & Technology at the Center for Democracy & Technology.

- (iv) creating perverse incentives; and
- (v) endangering civil liberties.

This paper identifies some of the most problematic cybersecurity policy ideas, explains how they could backfire, and offers in each case an alternative approach that could accomplish the goals of the policy proposal called into question. It explores proposals to: (i) empower the government to block or limit Internet communications on private networks; (ii) give the Department of Defense the lead cybersecurity role for civilian government and privately owned critical infrastructure information systems; (iii) have the government monitor private networks and communications for cybersecurity reasons; and (iv) increase the scope of what is lawful electronic surveillance by re-architecting new communications technologies and services to make them more wiretap ready. Each of these proposals would unjustifiably increase the federal government's ability to take unilateral action in networks otherwise (and more appropriately) subject to highly distributed governance.

#### I. PROPOSAL 1: EMPOWER THE GOVERNMENT TO BLOCK OR LIMIT INTERNET COMMUNICATIONS ON PRIVATE NETWORKS

Probably the most talked about cybersecurity measure in any legislative proposal is the “Internet Kill Switch”—governmental power to shut down or limit Internet traffic in an emergency. Giving the government kill switch authority would generate virtually all of the negative effects that characterize cybersecurity ideas that should be rejected. It would move the shut down decision away from the network operators who are the best decision-makers, slow decisions about whether to shut down a network, discourage network operators from sharing information with the government, create perverse incentives that undermine cybersecurity, and threaten civil liberties.

The “Internet Kill Switch” was first associated with the Cybersecurity Act of 2009. Section 18(2) of the bill as introduced would have empowered the President to declare a “cybersecurity emergency” and limit or shut down Internet traffic to any compromised system or network in the emergency.<sup>1</sup> Section 18(6) of

---

<sup>1</sup> Section 18(2) of the bill provided that the President “may declare a cybersecurity emergency and order the limitation or shutdown of Internet traffic to and from any compromised . . . critical infrastructure information system . . .” Cybersecurity Act of 2009, S. 773, 111th Cong. § 18(2) (as introduced, Apr. 1, 2009).

the bill as introduced went further: It gave the President the power “to order the disconnection of any . . . critical infrastructure information system[] or network[] in the interest of national security . . . .”<sup>2</sup> Proponents argue that critical infrastructure operators’ decisions to isolate their systems would be influenced inappropriately by pursuit of profit and fear of liability, instead of by protection of national security. They also argue that because the Internet has no “kill switch” the legislation cannot be interpreted to authorize the President to flip the switch.

However, the network “backbones” of major Internet providers are generally regarded as “critical infrastructure” because their disruption would have enormous and immediate economic effects. Though the Internet has no “kill switch,” if the President could shut down or limit Internet traffic to Internet backbone systems, he could, in effect, order significant elements of the Internet and significant amounts of Internet traffic to be shut down. When the government of Egypt did exactly that in early 2011—cutting off much of its population from Internet access for days during civil unrest—it magnified concerns in the U.S. about legislation that would extend such power to the President.<sup>3</sup>

The idea that the government should have the authority to shut down or limit Internet traffic in a cybersecurity emergency lives on in the comprehensive cybersecurity legislation introduced in the next Congress, the Cybersecurity and Internet Freedom Act (CIFA).<sup>4</sup> Concerned with distancing their bill from Egypt’s actions, CIFA’s lead sponsors included a provision that states that “neither the President . . . or any officer or employee of the United States Government shall have the authority to shut down the Internet”<sup>5</sup> and they released statements indicating that the Act would “explicitly prevent the President from shutting down the Internet”<sup>6</sup> and denying that their

---

<sup>2</sup> *Id.* § 18(6).

<sup>3</sup> Matt Richtel, *Egypt Cuts Off Most Internet and Cell Service*, N.Y. TIMES, Jan. 29, 2011, at A13, available at <http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html>.

<sup>4</sup> Cybersecurity and Internet Freedom Act of 2011, S. 413, 112th Cong. (2011).

<sup>5</sup> *Id.* § 2(c).

<sup>6</sup> Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, 112th Cong., Lieberman, Collins, Carper Introduce Bill to Address Serious Cyber Security Threats (Feb. 17, 2011), available at <http://www.hsgac.senate.gov/subcommittees/federal-financial-management/majority-media/-lieberman-collins-carper-introduce-bill-to-address-serious-cyber-security-threats>.

legislation was ever intended to “empower the President to deny U.S. citizens access to the Internet.”<sup>7</sup>

But the bill nonetheless retains a vaguely worded provision that enhances the government’s authority over the Internet and that authorizes the Department of Homeland Security (DHS), in an emergency, to shut down some elements of the Internet or to curb some Internet communications without adequate clarity and limitations. Despite the disclaimer of any authority to “shut down the Internet,” the open-ended emergency provision is problematic both for civil liberties and for owners and operators of the critical infrastructure that could be put under an emergency order.

Specifically, the CIFA would empower the President to declare a “cyber emergency”<sup>8</sup> that triggers authority in the DHS to “direct” the owners and operators of “covered critical infrastructure” to implement response plans approved by the government.<sup>9</sup> DHS is also authorized to “develop and coordinate” unspecified emergency measures “necessary to preserve the reliable operation” of covered critical infrastructure.<sup>10</sup> There is little doubt that the emergency powers that DHS would possess under the bill when the President declares a cybersecurity emergency include authority to shut down or limit Internet traffic. This is clear because the bill specifically calls out, and limits, this authority.<sup>11</sup>

---

<sup>7</sup> Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, 112th Cong., Lieberman, Collins, Carper Statement on Cybersecurity (Feb. 1, 2011), *available at* <http://lieberman.senate.gov/index.cfm/news-events/news/2011/2/lieberman-collins-carper-statement-on-cybersecurity>.

<sup>8</sup> Cybersecurity and Internet Freedom Act, *supra* note 5, § 249(a)(1). The bill authorizes the President to declare a cybersecurity emergency when there is an action by an individual or an entity that has the capability and intent to exploit a “cyber risk” that could disrupt a computer or software or hardware that is essential to the operation of covered critical infrastructure. *Id.* A “cyber risk” is any physical or virtual risk to a computer or related hardware or software, which, if exploited, would pose a significant risk of disruption to a computer, hardware, or software essential to the reliable operation of covered critical infrastructure. *Id.* § 241(5).

<sup>9</sup> *Id.* § 249(a)(3)(A).

<sup>10</sup> *Id.* § 249(a)(3)(B). The emergency actions DHS can direct must represent the least disruptive means feasible to the operations of covered critical infrastructure and hardware and software essential to the operation of covered critical infrastructure. *Id.* §§ 249(a)(3)(C), 4(8).

<sup>11</sup> Under the CIFA, communications traffic flowing over an Internet backbone system (or other critical infrastructure system) can be restricted or shut down when a DHS official determines that no other emergency measure will preserve the reliable operation of a

Of course, the Internet has no “kill switch” for the U.S. President to flip. Executing an Egypt-style Internet shut down in the U.S. to squelch dissent would be difficult to accomplish anyway. As compared to Egypt, the U.S. has significantly more Internet Service Providers (ISPs) and backbone systems, and many more connection points to the rest of the world, making it harder as a practical matter for the government here to achieve blanket compliance with an order that seemed politically motivated or otherwise illegal.<sup>12</sup>

Kill switch issues aside, is it wise to give the government authority to shut down or limit parts of the Internet or to selectively control communications over the Internet in an emergency? The Obama Administration seemed to think it unnecessary because it omitted any such authority from its cybersecurity legislative package, dealing the proposal a significant blow.<sup>13</sup> Additionally, there are ample reasons to reject such a proposal on the merits:

*Unintended economic and systematic impacts:* The potential list of unintended consequences to both the economy and to critical infrastructures themselves from even a limited shut down of some Internet traffic is long. Depending on the network involved, a shut down order could interfere with the flow of billions of dollars necessary for the daily functioning of the economy. It could deprive doctors of access to medical records. It could deprive manufacturers of critical supply chain information. Even if the power were exercised rarely, its mere existence would pose other risks. It could enable the government to coerce costly and unwise—even unlawful—conduct by threatening to shut down a system.

*Moving decision-making away from the best decision-maker:* Owners and operators of critical infrastructure already have control over their systems and strong financial incentives to protect them. They already limit or cut off Internet traffic to particular systems when they need to do so. They know better than government officials whether their systems need to be shut down or isolated. So far, a real

---

computer or related hardware or software that is essential to the operation of covered critical infrastructure. *Id.* § 249(a)(6)(a).

<sup>12</sup> Joshua Gruenspecht, *It Can't Happen Here? Why a Full-Scale American Internet Blackout Is Unlikely*, CTR. FOR DEMOCRACY & TECH. (Feb. 9, 2011), <http://www.cdt.org/blogs/joshua-gruenspecht/it-cant-happen-here-why-full-scale-american-internet-blackout-unlikely>.

<sup>13</sup> For the Obama Administration's cybersecurity legislative package, see OFFICE OF MGMT. & BUDGET, COMPLETE CYBERSECURITY PROPOSAL (2011), [http://www.whitehouse.gov/omb/legislative\\_letters](http://www.whitehouse.gov/omb/legislative_letters).

life circumstance has not yet been identified in which an owner or operator of a critical system kept it running when it clearly needed to be shut down. Government agencies' failures to date to protect their own systems<sup>14</sup> give reason to question the assumption that underlies the proposed authority: that the government knows best.

*Perverse incentives:* Giving the government the power to shut down or limit Internet traffic even in limited circumstances would backfire by creating perverse incentives. Private sector operators will be reluctant to share information if they know the government could use that information to order them to shut down. Shut down authority would thus undermine the very information sharing that the CIFA legislation encourages. Broadly speaking, it would also undermine the partnership that must develop around cybersecurity between the private sector and the government.

*Slowing decision-making:* Perhaps most importantly, giving the government shut down authority during an emergency would encourage delay when quick action is necessary. When private sector network operators determine that shutting down a system would be advisable, they could lose precious time waiting to be ordered to shut down so that they would be less likely to be held liable for the damage a shut down could cause others.<sup>15</sup>

*Endangering civil liberties:* Giving the government the power to block some Internet communications in an emergency for legitimate reasons creates a risk that such power will be abused or misused, to the detriment of civil liberties. One misuse would be to shut down some communications traffic to thwart a protest, as the government of

---

<sup>14</sup> *E.g.*, the Government Accountability Office recently found:

Weaknesses in information security policies and practices at 24 major federal agencies continue to place the confidentiality, integrity, and availability of sensitive information and information systems at risk. Consistent with this risk, reports of security incidents from federal agencies are on the rise, increasing over 650 percent over the past 5 years.

U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-137, INFORMATION SECURITY: WEAKNESSES CONTINUE AMID NEW FEDERAL EFFORTS TO IMPLEMENT REQUIREMENTS (2011), <http://www.gao.gov/new.items/d12137.pdf>.

<sup>15</sup> Limitations on liability for compliance with cybersecurity mandates permeate various legislative proposals. For example, CIFA provides that no civil action that is the direct consequence of actions taken in good faith to implement emergency cybersecurity measures may be maintained against an entity that owns or operates a critical infrastructure system. Cybersecurity and Internet Freedom Act, *supra* note 5, § 249(e)(4).

Egypt did, and as the Bay Area Rapid Transit (BART) system in San Francisco did. On August 11, 2011, BART shut down mobile phone service in a number of underground stations in an effort to head off a protest against an earlier shooting by BART police.<sup>16</sup> The normal restraint on government action in this context—judicial review to protect civil liberties—is often ineffective because it comes after the emergency that triggered the restrictions on communications.

*Alternative approach:* While the government often does not know best, sometimes it does know a key piece of information that the private sector operator may lack that would influence a decision about whether to isolate a system or throttle particular traffic. For example, the National Security Agency (NSA) may learn from its own signals surveillance activities of a concerted effort to attack one system that may be a harbinger of an attack on another. A good alternative to giving the government the authority to shut down traffic to the other system would be to encourage the NSA to share the information with the operators of the system so they can better protect it. When the information is classified, it would be shared only with those operators who are cleared to receive the classified information.<sup>17</sup> It may also be necessary for the government to share such information with the ISP that carries communications to the network at risk. Personnel at each entity may be required to obtain security clearances so they can receive classified information that may be involved in such a sharing arrangement.<sup>18</sup>

---

<sup>16</sup> Michael Cabanatuan, *BART Admits Halting Cell Service to Stop Protests*, S.F. CHRONICLE, Aug. 13, 2011, at A-1, [http://articles.sfgate.com/2011-08-13/news/29883195\\_1\\_bart-police-bart-service-downtown-san-francisco-stations](http://articles.sfgate.com/2011-08-13/news/29883195_1_bart-police-bart-service-downtown-san-francisco-stations). BART ultimately adopted a policy that severely limits the circumstances in which officials could interrupt mobile phone service on the BART system. *Extraordinary Circumstances Only for Cell Phone Interruptions*, BAY AREA RAPID TRANSIT (Dec. 1, 2011), <http://www.bart.gov/news/articles/2011/news20111201.aspx>.

<sup>17</sup> As an example of how this might work, the Cyber Intelligence Sharing and Protection Act would require the Director of National Intelligence to establish procedures to allow elements of the intelligence community to share information pertaining to network vulnerabilities and threats with cleared individuals and with entities that the DNI has determined can appropriately protect classified information. Cyber Intelligence Sharing and Protection Act of 2011, H.R. 3523, 112th Cong. § 2(a) (2011).

<sup>18</sup> For discussion of a pilot program through which Defense Department entities share classified cybersecurity information with communications service providers to help them better protect information systems of companies in the defense industrial base, see *infra* notes 54–59 and accompanying text.

This approach would increase the likelihood of making good decisions about whether to shut down or limit Internet traffic for cybersecurity reasons. It would put the decision in the hands of the network operators and owners who have the most knowledge about whether a system needs to be isolated, remove the liability-related disincentive to rapid decision-making, and diminish the risk that shut down decisions will be made for illegitimate reasons, such as to squelch speech. Moreover, it would rely on, rather than threaten, the sharing of information necessary to make the right decision.

## II. PROPOSAL 2: GIVE THE DEPARTMENT OF DEFENSE THE LEAD CYBERSECURITY ROLE FOR CIVILIAN GOVERNMENT AND CRITICAL PRIVATE SYSTEMS

The DHS bears responsibility for securing civilian government systems and for working with the private sector to secure networks associated with critical infrastructure, such as power production, generation, and distribution systems, and information technology and telecommunications systems.<sup>19</sup> However, it has been repeatedly criticized for failing to develop plans for securing key resources and critical infrastructure,<sup>20</sup> as required in the Homeland Security Act of 2002.<sup>21</sup> President Obama's national security and homeland security

---

<sup>19</sup> Homeland Security Act of 2002, Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2135, 2146 (2002).

<sup>20</sup> See, e.g., U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-1087T, CRITICAL INFRASTRUCTURE PROTECTION: DHS LEADERSHIP NEEDED TO ENHANCE CYBERSECURITY (2006), <http://www.gao.gov/new.items/do61087t.pdf>. In 2008, GAO reported that the DHS'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. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-588, CYBER ANALYSIS AND WARNING: DHS FACES CHALLENGES IN ESTABLISHING A COMPREHENSIVE NATIONAL CAPABILITY 47 (2008), <http://www.gao.gov/assets/280/279084.pdf>. In 2009, GAO testified that DHS had "yet to comprehensively satisfy its . . . cybersecurity responsibilities . . ." U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-09-835T, CYBERSECURITY: CONTINUED FEDERAL EFFORTS ARE NEEDED TO PROTECT CRITICAL SYSTEMS AND INFORMATION (2009), <http://www.gao.gov/assets/130/122877.pdf>. In 2010, GAO found continued shortcomings. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-24, CYBERSPACE POLICY: EXECUTIVE BRANCH IS MAKING PROGRESS IMPLEMENTING 2009 POLICY REVIEW RECOMMENDATIONS, BUT SUSTAINED LEADERSHIP IS NEEDED (2010), <http://www.gao.gov/assets/320/310967.pdf>.

<sup>21</sup> Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

advisors completed a cyberspace policy blueprint on April 17, 2009,<sup>22</sup> but implementation of those measures was slowed by the Administration's failure to timely appoint a cybersecurity official in the White House who could drive policy development and coordinate implementation of a government-wide plan.<sup>23</sup>

In the meantime, the NSA—an intelligence agency within the Department of Defense (DOD)—has continued to develop its own network monitoring capabilities and has worked to defend networks containing classified information. In addition, the DOD has set up its own Cyber Command to oversee the military's efforts to protect DOD's own 15,000 computer networks.<sup>24</sup> Cyber Command's top commander also heads the NSA and it is housed at Fort Meade alongside the NSA.<sup>25</sup> Cyber Command became operational on May 21, 2010, pulling together information operations expertise from components of the Army, Navy, and Air Force, and launching a program to recruit a cadre of cyber-warriors.<sup>26</sup> In this environment—a plodding DHS and a slowed-down White House, an emergent Cyber Command with expertise, and a complex threat environment with many actors and

---

<sup>22</sup> Exec. Office of the President of the U.S., *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure* (2009), available at [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf).

<sup>23</sup> Cybersecurity Coordinator Howard Schmidt was appointed on December 22, 2009. Macon Phillips, *Introducing the New Cybersecurity Coordinator*, THE WHITE HOUSE BLOG (Dec. 22, 2009, 7:30 AM), <http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator>.

<sup>24</sup> U.S. Cyber Command Factsheet, UNITED STATES STRATEGIC COMMAND, [http://www.stratcom.mil/factsheets/Cyber\\_Command](http://www.stratcom.mil/factsheets/Cyber_Command) (last visited Apr. 5, 2012). The United States Cybercommand is subordinate to the U.S. Strategic Command and is headquartered in Fort Meade, Maryland where NSA is also headquartered. *Id.* Its mission statement, from the U.S. Strategic Command Factsheet:

USCYBERCOM is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend the Department of Defense information networks and when directed, conducts full-spectrum military cyberspace operations (in accordance with all applicable laws and regulations) in order to ensure U.S. and allied freedom of action in cyberspace, while denying the same to our adversaries.

*Id.*

<sup>25</sup> *Id.*

<sup>26</sup> *Id.*

interconnected networks that all need to be defended—it is tempting to give Cyber Command and the NSA responsibility not only to defend the .mil domain, but to take the lead in defending the civilian .gov domain and privately-owned critical infrastructure systems as well.

This temptation to give the NSA and Cyber Command a lead role in securing civilian government systems and leading the government's efforts to help the private sector to secure private systems should be resisted. NSA must follow, for legitimate reasons, a policy of secrecy that is incompatible with the transparency necessary for the success of a civilian cybersecurity program. DHS operates transparently relative to the military agencies and issues some of the most informative Privacy Impact Assessments (PIAs) in government, making many of its operations more transparent than one might expect of a governmental entity with national security responsibilities.<sup>27</sup> If NSA, Cyber Command, or a related DOD entity were to take the lead role in cybersecurity for civilian unclassified 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 even in terms of security. It would diminish needed information sharing and threaten civil liberties.

*Slowing Information Sharing:* The vast majority of critical infrastructure information systems are owned and operated by the private sector, which also provides much of the hardware and software on which government systems rely, including the government's classified systems. The private sector has valuable information about vulnerabilities, exploits, patches, and responses. Private sector operators may hesitate to share this information if, as a result of the secrecy that often attends defense and intelligence matters, they do not know how it will be used and whether it will be shared with competitors. The public-private partnership upon which the U.S. cybersecurity strategy depends cannot function without trust. A lack of transparency undermines trust and has hampered cybersecurity efforts to date.

*Endangering civil liberties:* For other reasons that go beyond securing the cooperation and support of the private sector, openness is an essential aspect of any national cybersecurity strategy. Without transparency, there is no assurance that cybersecurity measures

---

<sup>27</sup> Privacy Impact Assessments, DEP'T OF HOMELAND SEC., [http://www.dhs.gov/files/publications/editorial\\_0511.shtm](http://www.dhs.gov/files/publications/editorial_0511.shtm) (last visited Apr. 6, 2012).

adequately protect privacy and civil liberties and adhere to Fair Information Practices<sup>28</sup> and due process principles.

Confidence that the NSA would adhere to these principles is undermined by its conduct in the Terrorist Surveillance Program (TSP) for approximately five years after the September 11, 2001 terrorist attacks on the Pentagon and the World Trade Center. The TSP<sup>29</sup> involved secret surveillance in the U.S. of people communicating internationally when one party to the communication was thought to be an agent of al Qaeda or an associated organization. The surveillance, at least to the extent it targeted persons in the United States, is widely thought to have been both unconstitutional and unlawful warrantless surveillance under the Foreign Intelligence Surveillance Act (FISA).<sup>30</sup> The program ended shortly after it was exposed in the *New York Times*.<sup>31</sup>

Transparency is essential if the public is to hold the government accountable for the effectiveness of its cybersecurity measures and for any abuses that occur. Conversely, the absence of transparency undermines public trust, arousing suspicions based on past conduct that rules intended to protect privacy and civil liberties are not being followed. As happened with the TSP, when such conduct is eventually exposed, the entire program can be threatened.

*Alternative approach:* Rather than undermining security and liberty by giving a DOD entity lead responsibility for securing civilian government and privately-owned critical infrastructure information systems, the Department of Homeland Security should play this role. Resources that should be made available to DHS so it can be effective go well beyond funding. Rather, its cybersecurity program should be

---

<sup>28</sup> Fair Information Practices are a series of principles, based on the Privacy Act, intended to protect informational privacy. For DHS's articulation of Fair Information Practice Principles, see Privacy Policy Guidance Memorandum, DEP'T OF HOMELAND SEC. (Dec. 29, 2008), [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

<sup>29</sup> See James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, available at <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all>.

<sup>30</sup> Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1871 (2006).

<sup>31</sup> Risen & Lichtblau, *supra* note 30. Following exposure of the TSP, Congress enacted legislation that strengthened the FISA requirement that intelligence surveillance of U.S. targets generally requires a court order and permitted surveillance in the U.S. of targets abroad with only blanket approval by the Foreign Intelligence Surveillance Court of the procedures under which the surveillance is conducted. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

structured to draw on the information, expertise, and human resources in DOD entities such as Cyber Command and the NSA.

Steps are already being taken toward this end. On September 27, 2010, DHS and DOD signed a Memorandum of Understanding setting forth the terms by which they would provide personnel, equipment, and facilities to increase inter-departmental collaboration, and support and synchronize each other's cybersecurity operations.<sup>32</sup> Under the agreement, DHS personnel go to the NSA to plan and collaborate on cybersecurity activities, learn about detecting threats, and bring with them expertise on civil liberties matters.<sup>33</sup> In turn, NSA personnel, such as cryptologists and other professionals go to the DHS network operations center to assist with cybersecurity operations.<sup>34</sup> NSA experts would work alongside DHS cybersecurity teams to help bring those teams up to speed quickly.

This kind of arrangement is a better way to take advantage of expertise and human resources in the DOD than is the alternative of giving a DOD entity operational control over civilian systems.<sup>35</sup> If DHS can operate with as much transparency as possible, consistent with its cybersecurity mission, this approach promotes needed information sharing and increases confidence that civil liberties are being protected. Building up the civilian cybersecurity capability by leveraging the expertise of the NSA can reduce pressure to put elements of DOD in control of civilian cybersecurity efforts. Once DHS has built the necessary expertise, the co-location of DHS and DOD personnel can be replaced by information sharing from DOD to DHS about cybersecurity threats, vulnerabilities, and attacks on an ongoing basis.

---

<sup>32</sup> Memorandum of Agreement Between the Dep't of Homeland Sec. and the Dep't of Def. Regarding Cybersecurity, at 5 (Sept. 27, 2010), available at <http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf>.

<sup>33</sup> *Id.* at 1–3.

<sup>34</sup> *Id.* at 3–4.

<sup>35</sup> Leslie Harris, *DHS-NSA in Cybersecurity Swap: Success to Be Named Later*, HUFFINGTON POST (Oct. 15, 2010), [http://www.huffingtonpost.com/leslie-harris/dhs-nsa-in-cybersecurity\\_b\\_764289.html](http://www.huffingtonpost.com/leslie-harris/dhs-nsa-in-cybersecurity_b_764289.html).

### III. PROPOSAL 3: HAVE THE GOVERNMENT MONITOR PRIVATE NETWORKS TO PROTECT THEM FROM MALWARE

This idea is so politically radioactive that it is seldom advocated openly and starkly. Some, however, insist that because the government has both cybersecurity expertise and information about threats, attacks, and attack signatures that the private sector lacks, the government should monitor private communications for cybersecurity reasons.<sup>36</sup> They argue that such monitoring—if done only by machine without a human ever seeing the traffic being monitored—would survive Fourth Amendment scrutiny.<sup>37</sup> As one Hill staffer said at a cybersecurity briefing in 2011, if the government and the private sector ISP would both be looking for the same types of problems and have to engage in the same level of communications scrutiny, and the government could do a better job, why not have the government perform this task?<sup>38</sup>

*Moving decision-making away from the best decision-maker:* Of course, this argument rests on the assumption that the government could do a better job, but the government's record of securing its own systems calls this assumption into question.<sup>39</sup> The privacy implications of such monitoring are profound, particularly when, in a time of crisis, there would be enormous pressure to dial up the intrusiveness of the monitoring. Moreover, it also ignores a key difference between governmental monitoring and the monitoring done every day by providers in the private sector: consumer choice. In one model, the government monitors communications whether the user chooses to allow that or not. In the private sector arrangement, the Internet user—whether as an individual or a company—makes a choice, even if from a limited universe: the user chooses an ISP to connect the user to the Internet. Sometimes that choice is driven in part by the provider's ability to protect the network and the users of the network. In a sense, users hire a company to perform this monitoring for them.

---

<sup>36</sup> See, e.g., Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

<sup>37</sup> See, e.g., *id.*

<sup>38</sup> Briefing on Cybersecurity White Paper, House of Representatives, Mar. 11, 2011.

<sup>39</sup> Federal agencies have been slow to implement cybersecurity reforms recommended by the Government Accountability Office. This has resulted in network vulnerabilities and breaches. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 15.

Mandatory governmental monitoring of private sector communications networks can also undermine the public/private partnership that must support any successful cybersecurity program. Few network operators would be comfortable with mandated governmental monitoring of their networks, particularly if security concerns dictate that they are not informed of what the monitoring governmental agency is doing with the data it collects. Such a program would undermine the trust that must develop between the private sector and the government.

Though unlikely to be mandated directly, governmental monitoring of private communications could arise as: (A) an unintended by-product of existing programs in place to monitor communications to or from the government; (B) an intentional extension of those programs to private-to-private communications; or (C) an indirect result of voluntary or mandatory information sharing from the private sector to the government for cybersecurity reasons. Programs that amount to ongoing government surveillance of private-to-private communications among consumers will backfire when exposed to the light of day: Public reaction would be so negative that the program would have to be abandoned even if it provided a security benefit.<sup>40</sup> Consequently, it is better to design cybersecurity monitoring programs to ensure that they do not result in government monitoring of private-to-private communications.

#### A. UNINTENDED SYSTEMATIC IMPACT FROM EINSTEIN'S MISTAKES

Each government agency already has in place a program to protect its networks by monitoring communications that pass over them. Einstein 2,<sup>41</sup> an intrusion detection system, is designed to supplement the information security efforts federal agencies already undertake. According to a May 19, 2008 Privacy Impact Assessment<sup>42</sup> and a

---

<sup>40</sup> The surveillance of communications to or from a network supporting a nuclear power plant or similar critical infrastructure would not raise the same level of concern.

<sup>41</sup> Einstein 2 is the successor of the original Einstein program. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT EINSTEIN PROGRAM: COLLECTING, ANALYZING, AND SHARING COMPUTER SECURITY INFORMATION ACROSS THE FEDERAL CIVILIAN GOVERNMENT (2004), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_einstein.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein.pdf) [hereinafter EINSTEIN Program 2004].

<sup>42</sup> DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR EINSTEIN 2 3 (2008), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_einstein2.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf).

January 9, 2009 opinion of the DOJ Office of Legal Counsel,<sup>43</sup> Einstein 2 is being deployed at federal agency Internet Access Points. It assesses network traffic against a pre-defined database of signatures of malicious code and alerts the United States Computer Emergency Readiness Team (US-CERT) to malicious computer code. US-CERT, in turn, passes on to intelligence and law enforcement agencies information it receives that would assist those agencies in carrying out their statutory missions.<sup>44</sup> While the signatures that Einstein assesses are not supposed to include personally identifiable information (PII) as defined by DHS, they do include Internet Protocol (IP) addresses and the alerts that Einstein 2 generates for US-CERT may include other PII.<sup>45</sup> In addition to using attack signatures, Einstein 2 also detects anomalous network traffic on a particular system and alerts US-CERT to those anomalies.

A successor, Einstein 3, is being tested with an undisclosed ISP and an undisclosed federal agency. It will have the added capability of intercepting threatening Internet traffic before it reaches a government system. According to the Privacy Impact Assessment DHS issued in connection with these tests,<sup>46</sup> Einstein 3 will use intrusion detection technology developed by the NSA and will adapt threat signatures developed by NSA in the course of its foreign intelligence work and by the DOD in connection with its information

---

<sup>43</sup> Stephen G. Bradbury, *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (Einstein 2.0) to Protect Unclassified Computer Networks in the Executive Branch*, 33 Op. Off. Legal Counsel 1 (2009), available at <http://www.justice.gov/olc/2009/e2-issues.pdf>. The memo concludes that operation of Einstein 2 does not violate the Constitution or surveillance statutes. *Id.* An August 14, 2009 opinion from the Obama Justice Department's Office of Legal Counsel affirms that conclusion. David J. Barron, *Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Executive Branch*, 33 Op. Off. Legal Counsel 1, 1 (2009), available at <http://www.justice.gov/olc/2009/legality-of-e2.pdf>.

<sup>44</sup> EINSTEIN PROGRAM 2004, *supra* note 42, at 8–9.

<sup>45</sup> EINSTEIN PROGRAM 2004, *supra* note 42, at 7. The PIA for Einstein 2 makes it clear that, for example, Einstein 2 will collect an email address when the source of malicious code it detects is attached to an email address. *Id.* Moreover, any “flow record” (a specialized summary of a suspicious communication) that Einstein routinely generates will generally include IP address and time stamp, which are widely regarded as personally identifiable. *Id.*

<sup>46</sup> DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE INITIATIVE THREE EXERCISE (2010), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_nppd\\_initiative3exercise.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf) [hereinafter INITIATIVE THREE EXERCISE].

assurance mission.<sup>47</sup> It will also use commercially available threat signatures.<sup>48</sup>

Einstein 3 operates on the network of an ISP providing service to the government instead of on the network of the federal agency that is being protected. One critically important question<sup>49</sup> is whether Einstein can reliably focus on communications with the government to the exclusion of private-to-private communications passing over the ISP's network. According to the Einstein 3 PIA, the participating federal agency will provide IP addresses to the ISP, which will use them to distinguish traffic to or from that agency from other traffic.<sup>50</sup> This is a logical, but by no means foolproof, method of identifying the targeted traffic. IP addresses can be re-allocated and become outdated. If Einstein were to mistakenly analyze private-to-private communications, it would likely be conducting an unlawful interception under the electronic surveillance laws.<sup>51</sup>

*Alternative approach:* The government has the power—and the responsibility—to monitor its networks to prevent intrusions and attacks and can contract that work out to an ISP. Thus, there is no quarrel with Einstein per se, just a need to prevent mistaken monitoring of communications that are not with a governmental agency. An independent audit of Einstein to ensure that it is not accessing private-to-private communications should be required to assess the system and to prevent mistakes.

---

<sup>47</sup> *Id.* at 2.

<sup>48</sup> *Id.* at 11.

<sup>49</sup> For a fuller listing of open questions about the Einstein Intrusion Detection System, see CTR. FOR DEMOCRACY & TECH., EINSTEIN INTRUSION DETECTION SYSTEM: QUESTIONS THAT SHOULD BE ADDRESSED 3–6 (2009), available at [http://www.cdt.org/security/20090728\\_einstein\\_rpt.pdf](http://www.cdt.org/security/20090728_einstein_rpt.pdf).

<sup>50</sup> INITIATIVE THREE EXERCISE, *supra* note 47, at 4.

<sup>51</sup> The Wiretap Act prohibits interception of electronic communications without a court order, and defines “intercept” as the acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device. 18 U.S.C. § 2510(4) (1968). Section 336 of the Intelligence Authorization Act for FY 2010 requires reports to Congress about the privacy impact of Einstein and any other similar cybersecurity programs as well as information about the legal authorities for the programs and about any audits that have been conducted or are planned for the programs. Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, § 336, 124 Stat. 2654, 2689–92 (2010).

## B. ENDANGERING CIVIL LIBERTIES BY EXTENDING EINSTEIN MONITORING TO PRIVATE COMMUNICATIONS

Deputy Secretary of Defense William Lynn III has advocated extending the Einstein intrusion detection and prevention system from the civilian government systems it now protects to privately-owned networks through voluntary adoption by ISPs.<sup>52</sup> Einstein monitoring, as mentioned above, includes both analyzing communications to or from a governmental agency and reporting information back to other governmental agencies. When it comes to extending Einstein monitoring to private networks, and to private-to-private communications, it is the backhaul of information—the flow of information to US-CERT and then to intelligence and law enforcement agencies—that triggers civil liberties concerns. A person who is communicating with a government agency cannot complain that the government is reading his communication. A person who is not can. If extending Einstein to the private sector includes reporting personally identifiable information back to US-CERT and on to intelligence and law enforcement agencies, this backhaul function threatens civil liberties and could violate the Electronic Communication Privacy Act and the Fourth Amendment.<sup>53</sup> It also moves some network monitoring responsibility to the government and away from the private sector network operators best able to perform this task.

---

<sup>52</sup> *Defense Dept. Outlines New Infosec Approach: Cybersecurity Speech by DoD Deputy Secretary William Lynn*, GOV INFO SEC. (May 26, 2010), [http://www.govinfosecurity.com/articles.php?art\\_id=2580&opg=1](http://www.govinfosecurity.com/articles.php?art_id=2580&opg=1).

<sup>53</sup> Absent an exception (explained in some detail *infra* at footnotes 63–67 and surrounding text), ECPA generally prohibits providers of electronic communication service from disclosing to governmental entities communications content and information about communications such as email logs revealing who communicated with whom, without a court order. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (1986). The most significant exception to this rule is that communications content more than 180 days old can be obtained with a subpoena, but such content tends to be less useful for cybersecurity operations. To the extent that the backhaul to the government reveals communications content or other communications information protected by ECPA against disclosure to the government without a court order, it violates the statute unless an exception applies. For example, a provider's acknowledgment to the government that particular content has passed over its network necessarily discloses that content to the government. The Fourth Amendment analysis is similar, but for content only, as non-content is generally regarded as unprotected by the Fourth Amendment. U.S. CONST. amend. IV.

*Alternative approach:* The government should share the technology that powers Einstein and the cyber-attack signatures that it has and that the private sector lacks. It should permit critical infrastructure network providers to use this technology if they find it superior to alternatives. To avoid the negative impact on civil liberties, any extension of Einstein to the private sector should exclude the backhaul reporting of PII to US-CERT and to intelligence and law enforcement agencies. This approach would help private sector network operators do what they are hired to do to monitor their networks for malicious code, while protecting privacy. Instead of directly monitoring communications, the government would be equipping the private sector parties best able to perform this task.

One model for implementing this alternative approach can be seen in the program the NSA recently launched to help large communications service providers secure networks of defense contractors in the Defense Industrial Base (DIB) Cyber Pilot. Under this program, the DOD shares classified attack signatures and other cybersecurity information with ISPs or with the DIB companies themselves.<sup>54</sup> They use this information to protect the DIB companies' networks against intrusion. The initial pilot involved AT&T, Verizon, and CenturyLink, working with fifteen DIB companies that included Lockheed Martin, CSC, SAIC, and Northrup Gumman.<sup>55</sup> This arrangement, whereby the NSA helps private sector companies defend their own networks, is a far better solution<sup>56</sup> than having NSA itself access the communications traffic and apply classified signatures to clean it.

The Pentagon recently decided to make the DIB Pilot permanent, to extend it to other DIB companies, and to consider extending the

---

<sup>54</sup> William J. Lynn III, *The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack*, FOREIGN AFFAIRS (Sept. 28, 2011), <http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later>. See also DEP'T OF DEF., PRIVACY IMPACT ASSESSMENT (PIA) FOR THE DEFENSE INDUSTRIAL BASE (DIB) CYBER SECURITY/INFORMATION ASSURANCE ACTIVITIES 5 (2011), available at [http://dodcio.defense.gov/Portals/o/Documents/DIB%20CS-IA%20PIA\\_FINAL\\_signed\\_30jun2011\\_VMSS\\_GGMR\\_RC.pdf](http://dodcio.defense.gov/Portals/o/Documents/DIB%20CS-IA%20PIA_FINAL_signed_30jun2011_VMSS_GGMR_RC.pdf).

<sup>55</sup> Ellen Nakashima, *NSA Allies with Internet Carriers to Thwart Cyber Attacks Against Defense Firms*, WASH. POST, June 16, 2011, [http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH\\_print.html](http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_print.html).

<sup>56</sup> Jim Dempsey, *Don't Mess with Success*, CTR. FOR DEMOCRACY & TECH. (June 17, 2011), <http://www.cdt.org/blogs/jim-dempsey/dont-mess-success>.

pilot to other critical infrastructure sectors.<sup>57</sup> Special attention should be paid both to the types of critical infrastructure companies to which the DIB Pilot would be extended and to the flow of information from ISPs to DOD.<sup>58</sup>

### C. ON-GOING INFORMATION SHARING AS A BACK-DOOR TO GOVERNMENTAL MONITORING

There is a well-founded belief that information sharing is an important aspect of any cybersecurity program. Different players in a networked environment detect different threats and vulnerabilities at different times and an exchange of information about them can help all. There is also a perception that cybersecurity information sharing as practiced is inadequate and there is some concern that the provisions of the Wiretap Act<sup>59</sup> and the Electronic Communications Privacy Act (ECPA)<sup>60</sup> are impediments to information sharing. Any discussion of information sharing must begin with an assessment of the information that must be shared, but that is not, and with an understanding of the extent to which the law already allows information to be shared.

Current law gives providers of communications services substantial authority to monitor their own systems and to disclose to governmental entities, and to their peers, information about cyber-attack incidents for the purpose of protecting their own networks. In particular, the federal Wiretap Act provides that it is lawful for any

---

<sup>57</sup> Aliya Sternstein, *Defense to Grow Industrial Base Cyber Program, DHS May Expand to Other Programs*, NEXTGOV (Sept. 19, 2011), [http://www.nextgov.com/nextgov/ng\\_20110919\\_6730.php](http://www.nextgov.com/nextgov/ng_20110919_6730.php).

<sup>58</sup> Consent is the legal underpinning of the current pilot: The DIB company that is the destination of a communication consents to its ISP sharing with the government the “hits” the ISP observes on the attack signatures the government has provided. Like electronic surveillance, this reporting discloses routing, addressing, and signaling information about communications, and may disclose communications content. The recipient has consented to this disclosure. A consent-based model might be appropriate for other critical infrastructure entities, such as a company operating a nuclear power plant. However, if the critical infrastructure company to be protected is itself a communications service provider for Internet users at large, its consent to disclosure to the government does not bind its users and its extraction of consent from its users through provisions tucked away in terms of service would create grave civil liberties concerns.

<sup>59</sup> Wiretap Act, 18 U.S.C. §§ 2510–2522 (1968).

<sup>60</sup> Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2006).

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.<sup>61</sup> 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, under the ECPA, a service provider, when necessary to protect its system, can disclose stored communications<sup>62</sup> and customer records<sup>63</sup> to any governmental or private entity.<sup>64</sup> 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"<sup>65</sup> 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.<sup>66</sup>

These provisions do not authorize ongoing or routine disclosure of traffic by the private sector to any governmental entity. To amend them to broadly allow the routine disclosure of communications traffic to the government for cybersecurity purposes would destroy the promise of privacy in the Wiretap Act and ECPA. The privacy these laws protect fosters the growth of the Internet and the economic activity that depends on it. Gutting them could backfire by discouraging the growth of technologies, such as cloud computing, that rely on the privacy of communications.

The Obama Administration has advanced such a proposal.<sup>67</sup> It envisions a sweeping information sharing regime that would override

---

<sup>61</sup> *Id.* at § 2511(2)(a)(i).

<sup>62</sup> *Id.* at § 2702(b).

<sup>63</sup> *Id.* at § 2702(c).

<sup>64</sup> 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), (c)(4) (2006).

<sup>65</sup> A "computer trespasser" is someone who accesses a computer used in interstate commerce without authorization. *Id.* at § 2510(21).

<sup>66</sup> *Id.* at § 2511(2)(i).

<sup>67</sup> OFFICE OF MGMT. & BUDGET, DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY AND INFORMATION SHARING: LEGISLATIVE PROPOSAL (2011), *available at*

contrary provisions in every state or local law without exception to permit any entity to share with a new collection center at DHS any information the entity may have, including communications traffic, so long as the information was shared for cybersecurity purposes.<sup>68</sup> It would not matter how it was acquired and it would not matter how use and disclosure would otherwise be restricted. Sharing entities would only have to undertake “reasonable” efforts to strip out identifying information that was irrelevant to the cybersecurity purpose, thus permitting all relevant identifying information, and the irrelevant identifiers that are difficult to filter out, to be shared.<sup>69</sup> The information sharing would be done under privacy rules yet to be written.<sup>70</sup>

Likewise, proposals to solve the information-sharing dilemma by simply expanding government power to compel disclosure of privately held data should be rejected, such as proposals to give a governmental entity wide-ranging authority to access private sector data that is relevant to cybersecurity threats and vulnerabilities.<sup>71</sup> Such an approach would be dangerous to civil liberties and would undermine the public-private partnership that needs to develop further around cybersecurity. Collecting large quantities of sensitive information into a common database can also undermine security because such a database could, itself, become a target for hackers.

*Alternative approach:* Properly viewed, implemented, and carefully controlled information sharing is an alternative to governmental monitoring of private communications. It leaves the monitoring responsibility where it belongs; with the private sector system operators. It supplements their existing abilities by better equipping them to do the monitoring that needs to be done. While current law authorizes providers to monitor their own systems and to disclose voluntarily communications and records necessary to protect their own systems, there might be a need for a very narrow exception to the Wiretap Act and ECPA that would permit disclosures about

---

<http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/dhs-cybersecurity-authority.pdf>.

<sup>68</sup> *Id.* at 8, 10.

<sup>69</sup> *Id.* at 8.

<sup>70</sup> *Id.* at 10.

<sup>71</sup> For an example of such a proposal, see Cybersecurity Act of 2009, S. 773, 111th Cong. § 14 (2009) (as introduced, Apr. 1, 2009).

specific attacks and malicious code on a voluntary basis. The exception would have to be narrow so that routine disclosure of Internet traffic to the government or other service providers remained clearly prohibited.

#### IV. PROPOSAL 4: IMPOSE DESIGN MANDATES ON NEW COMMUNICATIONS TECHNOLOGIES TO FACILITATE ELECTRONIC SURVEILLANCE

The Communications Assistance for Law Enforcement Act (CALEA)<sup>72</sup> was enacted in 1994 to require telecommunications carriers to design specific wiretapping capabilities into their networks. In 2005, the FCC extended these requirements to providers of broadband Internet access and interconnected Voice Over IP (VOIP) services.<sup>73</sup> Now, according to press accounts,<sup>74</sup> the FBI wants similar requirements to be imposed on communications applications and services. The Federal Bureau of Investigation, fearing that its surveillance capabilities will be eroded by new communications technologies, has floated the idea that those technologies should be made subject to design mandates that would facilitate surveillance of communications utilizing those technologies.<sup>75</sup> Among others, the FBI has mentioned Skype, which provides encrypted VOIP services, and RIM, which makes the popular BlackBerry and offers the BlackBerry enterprise service to business customers.<sup>76</sup> Apparently, they would be compelled to design their services to ensure government access to unscrambled communications.<sup>77</sup>

While this is not a cybersecurity proposal in its own right, the FBI justifies the electronic surveillance its proposal would facilitate by

---

<sup>72</sup> Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001–1010 (1994).

<sup>73</sup> In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, 20 FCC Rcd. 14989 (2005), available at <http://www.askcalea.net/archives/docs/20050923-fcc-05-153.pdf>.

<sup>74</sup> Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1, available at <http://www.nytimes.com/2010/09/27/us/27wiretap.html>.

<sup>75</sup> *Id.*

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

arguing, among other things, that it helps the FBI combat identity theft<sup>78</sup> that is a product of data breaches that result from cybersecurity failures and would also help it combat other crimes. However, there is a risk that the vulnerabilities that would have to be built into communications technologies and services under such a mandate to facilitate law enforcement surveillance could be exploited by identity thieves, hackers, foreign spies, and foreign governments seeking competitive advantage. In other words, this policy proposal to enhance surveillance capabilities could backfire by undermining cybersecurity at the same time enormous efforts are being made to improve it.

This initiative is part of a program the FBI calls “Going Dark,” so named out of concern that as communications technologies evolve, the FBI will be unable to listen in. In reality, the digital age has been a boon for government surveillance. As cell phones and the Internet have become deeply entwined in consumers’ daily lives, more and more personal and proprietary data is being transmitted and stored on digital services, ranging from location, to one’s associations, purchases, and online interests. Electronic surveillance is already at record levels and it is increasing. In 2010, 3,194 federal and state wiretaps were authorized for criminal purposes, more than in any prior year,<sup>79</sup> and an additional 1,506 intelligence intercepts were authorized in 2010.<sup>80</sup> On average in 2010, 3,199 communications were intercepted in every criminal wiretap, yet 81% of monitored communications were non-incriminating, according to the government’s own data.<sup>81</sup> At the same time, the legal restraints on surveillance have been steadily relaxed—especially since the

---

<sup>78</sup> See, e.g., *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 3, (2011) (statement of James A. Baker, Associate Deputy Att’y Gen., stating that electronic surveillance laws protect privacy by helping law enforcement obtain evidence used to prosecute privacy related crimes such as identity theft and hacking).

<sup>79</sup> ADMIN. OFFICE OF THE U.S. COURTS, WIRETAP REPORT 2010 31 tbl. 7 (2011), available at <http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2010.aspx> [hereinafter 2010 WIRETAP REPORT].

<sup>80</sup> Dep’t of Justice, Office of Legislative Affairs, Annual Foreign Intelligence Surveillance Act Report to Congress 2010 (2011), available at [http://www.justice.gov/nsd/foia/reading\\_room/2010fisa-ltr.pdf](http://www.justice.gov/nsd/foia/reading_room/2010fisa-ltr.pdf) (letter from Ronald Weich, Assistant Attorney General, to Joseph Biden, President, United States Senate, dated Apr. 29, 2011).

<sup>81</sup> 2010 WIRETAP REPORT, *supra* note 80, at 31 tbl. 7.

September 11 attacks. Examples include the 2001 PATRIOT Act,<sup>82</sup> the 2008 FISA Amendments Act,<sup>83</sup> and the steady addition of relatively minor crimes to the list of offenses for which wiretapping is permitted.

*Unintended systematic impacts:* Such a mandate could backfire in several ways.<sup>84</sup> First, it could stifle innovation because it would apply to the application layer of the Internet, where the greatest innovation and economic development are occurring. The next great application might never be built because an innovator working with limited resources would be hard pressed to meet the design mandate. Some current applications would have to change so drastically that they would become unrecognizable to current users and others might be outlawed altogether. Second, it could undermine U.S. competitiveness by spurring innovators to market their new products overseas, instead of in the U.S., so they could avoid the mandate. Third, it would be cited by foreign countries that are human rights abusers as a justification for their own surveillance design mandates, which would be used to monitor dissidents and thwart democratic movements, undermining U.S. policy abroad.

Perhaps most important, the FBI proposal might actually harm cybersecurity. In essence, the FBI is asking that applications have a built-in backdoor to facilitate government wiretapping. However, such backdoors can also be exploited by hackers and identity thieves. More backdoors means less secure networks.

At Congressional hearings<sup>85</sup> on the FBI's Going Dark program, the cyber-insecurity that could result from such a mandate became a key issue. Dr. Susan Landau, a Fellow at Harvard University's Radcliffe Institute for Advanced Study, explained how a similar mandate had resulted in unauthorized eavesdropping on the Prime Minister of

---

<sup>82</sup> USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

<sup>83</sup> Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

<sup>84</sup> Industry associations and NGOs released a February 15, 2011 Statement of Concern about Expansion of CALEA urging cautious appraisal of any such proposal and outlining several ways in which it could have harmful effects. *Statement of Concern about Expansion of CALEA*, CTR. FOR DEMOCRACY & TECH. (Feb. 15, 2011), [http://www.cdt.org/pr\\_statement/statement-concern-about-expansion-calea](http://www.cdt.org/pr_statement/statement-concern-about-expansion-calea).

<sup>85</sup> *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. (2011), available at [http://judiciary.house.gov/hearings/hear\\_02172011.html](http://judiciary.house.gov/hearings/hear_02172011.html).

Greece, cabinet ministers, and others.<sup>86</sup> In that case, Vodafone Greece had purchased switches from Ericsson that were designed with backdoors to allow interception authorized by law.<sup>87</sup> Parties unknown to this day exploited those backdoors to eavesdrop on government officials and others.

*Alternative approach:* Rather than require that communications applications and services be designed with vulnerabilities that can be exploited, Congress could support the Domestic Communications Assistance Center that the FBI is establishing to leverage surveillance research and development efforts at the federal, state, and local levels. This would allow all levels of law enforcement to gain the benefit of surveillance techniques employed by any. It might also help the FBI enhance its own ability to exploit communications devices themselves. It also avoids the unintended consequences to innovation, U.S. competitiveness, and cybersecurity itself that could result from imposing design mandates to facilitate electronic surveillance of new communications technologies.

## V. CONCLUSION

Washington is awash with cybersecurity policy ideas for Congress to choose among. Some policies are “low hanging fruit” that should have been adopted long ago. But others, including those outlined in this article, could do more harm than good by undermining civil liberties and necessary information sharing, slowing down decision making and moving decision-making authority from the best decision makers, and creating perverse incentives and unexpected economic and systematic impacts, all of which would undermine cybersecurity. Picking the right policies will involve careful consideration of options and the foresight to look beyond promised security benefits to account for unintended effects.

---

<sup>86</sup> *Id.* at 23 (statement of Susan Landau, Ph.D., Radcliffe Institute for Advanced Study, Harvard University).

<sup>87</sup> *Id.*