Cyber Security Legislation Privacy Protections are Substantially Similar

By Rob Strayer and David Beardwood

The four most prominent cyber security legislative proposals – the Obama administration's legislative text; Cyber Intelligence Sharing and Protection Act (CISPA), H.R. 3253, sponsored by Congressman Mike Rogers; the Cybersecurity Act of 2012, S. 2105, sponsored by Senators Lieberman, Collins, Rockefeller and Feinstein; and the Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act (SECURE IT Act), S. 3342, sponsored by Senator McCain and several other Republican senators – all apply strict conditions to cyber security information sharing and have oversight measures to protect privacy and civil liberties. Each proposal establishes information-sharing mechanisms that would protect personal information from misuse and mandates ongoing oversight to ensure respect for privacy and civil liberties.

Caviling over minor differences with its proposal, the administration threatens to veto the House-passed CISPA, largely based on its privacy protections.[1] There is substantial common ground rather than major divergence among these proposals on how to protect privacy and civil liberties, as explained below.

PRIVACY AND CIVIL LIBERTIES PROVISIONS IN CURRENT PROPOSALS

The Obama Administration Proposal

The administration's proposal assigns the Department of Homeland Security with the responsibility of carrying out cyber security information sharing.[2] Private-sector information used by the government must be related to cyber threats to federal networks or critical infrastructure, personal information must be protected from unauthorized access or disclosure, and those using federal networks must be notified that their traffic may be monitored.[3] Shared information may also be used for law enforcement purposes with the approval of the attorney general if it is evidence of the past, current or imminent commission of a crime.[4] Private sector,[5] as well as state and

local,[6] cooperation with the federal government is protected from public disclosure. Finally, oversight of these measures would be provided by the chief privacy and civil liberties officers of DHS and DOJ through annual reports to Congress,[7] and separately by the Privacy and Civil Liberties Oversight Board (PCLOB), which would provide an initial evaluation to Congress within two years of enactment.[8]

CISPA

The Cyber Intelligence Sharing and Protection Act, H.R. 3523, passed the House by a bipartisan vote of 248-168.[9] It would allow the director of national intelligence (DNI) to establish intelligence-sharing mechanisms between the intelligence community and the private sector. CISPA grants more control to the private sector than the other proposals in limiting the use of information provided to the federal government or other private sector entities. It allows companies submitting information to set additional anonymization standards[10] and prohibit sharing of the information with specific federal agencies.[11] Shared information is protected from public disclosure[12] or use for unfair trade advantage.[13]

Data provided to the government may only be used for cyber security purposes, investigating and prosecuting crimes which could result or have resulted in death, serious bodily har m, or the exploitation of a minor, and in cases of threats to national security.[14] Personal records on library use, book sales and purchases, firearm sales, tax returns, education, and medical history are also excluded from use in intelligence sharing.[15] The inspector general of the intelligence community provides oversight through annual reports to Congress,[16] but the PCLOB is not required to participate in oversight under the bill.[17]

The Cybersecurity Act of 2012

The Cybersecurity Act of 2012, S. 2105, authorizes additional public-private information sharing with DHS, similar to the Obama administration's proposal, and among private sector entities. The bill requires that DHS establish guidelines for sharing cyber security threat and vulnerability information to protect privacy and civil liberties, in consultation with the attorney general and DNI.[18] It would also establish a full-time privacy officer to ensure compliance with the guidelines.[19] The federal government must also explicitly protect against the disclosure of personal information, and any cyber intelligence shared with the government would be protected from public disclosure.[2021]

The government may only use shared information against cyber threats[22] and to prevent, investigate, or prosecute the past, current, or imminent commission of a crime with the approval of the attorney general – with the attorney general weighing the value of any such law enforcement action against the need to protect personal information.[23] Businesses may share cyber intelligence as long as they follow these restrictions and do not use shared information to gain an unfair trade advantage.[24] Oversight would come from the chief privacy and civil liberties officers of DHS and DOJ through annual reports to Congress,[25] as well as the PCLOB, which would provide an initial evaluation to Congress within two years of enactment, as in the administration's proposal.[26] The inspector general of each relevant agency would also provide annual evaluations.[27]

The SECURE IT Act

The SECURE IT Act, S. 3342, would establish cyber intelligence sharing between the private sector and multiple cyber security centers throughout the federal government.[28] These centers must follow standards set by the secretaries of commerce and homeland security to protect personal information and trade information,[29] and those providing information would be protected from legal reprisal or public disclosure of shared content.[30] Additional control is provided to the private sector, as those sharing information must provide consent before information may be shared with state, local or tribal governments for any reason.[31]

Any shared information may again only be used for cyber security, national security, or law enforcement purposes, although this bill is the most permissive for law enforcement use by allowing any federal agency to use information against any crime codified in section 2516 of title 18 of the U.S. Code.[32] Oversight is carried out by the PCLOB and all agency and department heads overseeing cyber security centers who, together, must submit an initial evaluation to Congress within one year of enactment and biennial reports thereafter.[33] The inspector general of each relevant agency would also provide annual evaluations.[34] Additionally, the Council of the Inspectors General on Integrity and Efficiency is authorized to conduct oversight, though no requirements are placed on the frequency of their review.[35]

MEASURES IN COMMON TO PROTECT PRIVACY AND CIVIL LIBERTIES

- ***All four proposals allow a government agency to set enforceable guidelines for the sharing of cyber security information between the private sector and the government, as follows:***
    - Administration's Proposal: The secretary of homeland security, with review and approval by the attorney general.[36]
    - CISPA: The director of national intelligence, in consultation with the secretary of homeland security.[37]
    - Cybersecurity Act: The director of the Department of Homeland Security's cyber security center, in consultation with the attorney general, DNI, and the privacy officer of the DHS center.[38]
    - SECURE IT Act: The secretary of commerce, in consultation with the secretary of homeland security.[39]

- ***Personally identifiable information (PII) may not be included in the information shared, unless it is necessary to include that information for security purposes.***[40] Each proposal requires the protection of PII whenever it is not critical for security purposes. This keeps PII limited to the company entrusted to protect it, as well as relevant government investigators. There are also provisions in each bill that prevent the disclosure of personal information to the public in the critical circumstances when it is shared. CISPA also allows for providers to set additional requirements for anonymization.

- ***There must be continuous oversight of compliance with privacy and civil liberty measures, as well as evaluation of their impact.***[41] Oversight will help to prevent intentional or accidental abuse and identify developing needs in regulations. The Privacy and Civil Liberties Oversight Board's membership awaits Senate confirmation. Once its members are confirmed, the PCLOB will serve as an independent agency to oversee activity across the government, and each of the four initiatives, except CISPA, would include the Board in oversight,[42] though the originally filed version of CISPA included the Board.[43]

The three proposals that include the PCLOB also prescribe other groups of government officers to lead dual oversight, with the administration proposal and the Cybersecurity Act involving the chief privacy and civil liberties officers of DHS and DOJ,[44] the SECURE IT Act requiring reporting from the relevant agency or department heads and chief privacy and civil liberties officers[45] as well as the Council of the Inspectors General on Integrity and Efficiency,[46] and both the Cybersecurity and SECURE IT Acts requiring oversight by the inspector general of each agency using shared information.[47] CISPA would require the inspector general of the intelligence community to conduct multi-agency oversight.[48]

- ***Information shared with the federal government may only be used for cyber security, for national security purposes, and by law enforcement to prosecute a crime; and not regulatory action.***[49]

- ***Cyber intelligence provided to the federal government is protected from public disclosure through the Freedom of Information Act (FOIA) or other means.***[50] This condition is necessary for intelligence sharing, as disclosed exchanges could reveal vulnerabilities in private security or cause reputational harm – possibilities which currently may preclude more robust information sharing.

CONCLUSION

The four major proposals from the administration, House, and Senate establish common ground on many privacy protections. The bills vary to limited degrees on the mechanism of the sharing, control over the process by the private sector, and agency responsibilities, but the core provisions on privacy and civil liberties are largely agreed upon. These differences are of the type that typically can be worked out through the legislative process as bills move through the committees to floor action and eventual conference between the House and Senate, and do not amount to an issue that should pose an insurmountable obstacle to the enactment of cyber security legislation.

[1] Executive Office of the President, Office of Management and Budget, *Statement of Administration Policy: H.R. 3523 – Cyber Intelligence Sharing and Protection Act*. 25 April 2012.

[2] White House, *Comprehensive National Cybersecurity Initiative*, available at: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative; White House, *Cybersecurity Authority and Information Sharing Act of 2011* (Cybersecurity Authority Act)
[3] Cybersecurity Authority Act § 244(b)
[4] § 244(b)(3)
[5] White House, *Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act* § 7(d)
[6] Cybersecurity Authority Act § 245(f)
[7] § 248(e)
[8] § 248(f)
[9] Final Vote Results for Roll Call 192. 26 April 2012.
[10] **H.R. 3523 (RFS)** § 2 (50 U.S.C. § 1104(b)(3)(A))
[11] § 2 (50 U.S.C. § 1104(b)(3)(C)(iv))
[12] § 2 (50 U.S.C. § 1104(b)(3)(D))
[13] § 2 (50 U.S.C. § 1104(b)(3)(B))
[14] § 2 (50 U.S.C. § 1104(c)(1))
[15] § 2 (50 U.S.C. § 1104(c)(4))
[16] § 2 (50 U.S.C. § 1104(e)(1))
[17] H.R. 3523 (IH) § 2 (50 U.S.C. § 1104(c))
[18] **S. 2105 (PCS)** § 243(c)(5)
[19] § 242(j)
[20] § 704(d-f)
[21] § 704(g)(4)
[22] § 704(g)(1)
[23] §704(g)(2)
[24] § 702(b)
[25] § 704(g)(5)
[26] § 704(g)(6)
[27] § 201 (44 U.S.C. § 3556(c))
[28] **S. 3342** § 101(5): Cyber security centers that could conduct information sharing include the DOD Cyber Crime Center, U.S. Cyber Command Joint Operations Center and NSA/CSS Threat Operations Center, the ODNI Intelligence Community Incident Response Center, the FBI National Cyber Investigative Joint Task Force, the DHS National Cybersecurity and Communications Integration Center, and any subsequently established federal cyber security center.
Available at: http://www.hutchison.senate.gov/files/documents/S%20%203342%20SECURE%20IT.pdf
[29] § 201 (44 U.S.C. § 3553(a)(1))
[30] § 102(c)(3-7)
[31] § 102(c)(2)
[32] § 102(c)
[33] § 105(a)
[34] § 201 (44 U.S.C. § 3554(a)(4))
[35] § 106
[36] Cybersecurity Authority Act § 248
[37] H.R. 3523 § 2 (50 U.S.C. § 1104(b) (Procedures and Guidelines))
[38] S. 2105 § 243(c)(5)

[39] S. 3342 § 201 (44 U.S.C. § 3553)
[40] Cybersecurity Authority Act § 248(a)(2); H.R. 3523 § 2 (50 U.S.C. § 1104(b)(3)(A)); S. 2105 § 243(c)(1)(E)(i); § 702(b)(1); S. 3342 § 102(d)(1)(C)
[41] Cybersecurity Authority Act § 248; H.R. 3523 § 2 (50 U.S.C. § 1104(e)); S. 2105 § 704(g)(4-7); S. 3342 § 104; § 106; § 201 (44 U.S.C. § 3554 (a)(4))
[42] Cybersecurity Authority Act § 248(f); S. 2105 § 704(g)(6); S. 3342 § 105
[43] H.R. 3523 (IH) § 2 (50 U.S.C. § 1104(c))
[44] Cybersecurity Authority Act § 248(e); S. 2105 § 704(g)(5)
[45] S. 3342 § 105(a)
[46] § 106
[47] S. 2105 § 201 (44 U.S.C. § 3556(c)); S. 3342 § 201 (44 U.S.C. § 3554(a)(4))
[48] H.R. 3523 (RFS) § 2 (50 U.S.C. § 1104(e))
[49] Cybersecurity Authority Act § 244(b); Cybersecurity for Critical Infrastructure Act § 8(a)(1)(C); H.R. 3523 (RFS) § 2 (50 U.S.C. § 1104(c)); S. 2105 § 704(g)(1-2); S. 3342 § 102(c)(1)
[50] Cybersecurity Authority Act § 245(f); Cybersecurity for Critical Infrastructure Act § 7(d); H.R. 3523 § 2 (50 U.S.C. § 1104(b)(3)(D)); S. 2105 § 704(d); S. 3342 § 102(c)(3-7)