FREQUENTLY ASKED QUESTIONS ABOUT CYBERSECURITY AND PRIVACY

April 2012

What cyber threats does the United States face and how can the country be protected?

- Pervasive and sustained cyber attacks against the United States could have potentially devastating effects – both physical damage and economic disruption – on federal computer systems and operations as well as on networks that control critical civilian infrastructure. The United States could potentially be attacked by hackers, terrorists, and foreign governments. For example, an attack could cause the failure of power-grids, transportation networks, or financial systems. In this increasingly interconnected era, an attack on one network could quickly spread through the entire Internet infrastructure.
- Although the United States is at risk from potential cyber attacks, the government has not adequately described to the public how severe this problem is, and what risks and consequences the nation faces if attacked. The Constitution Project's ("TCP") Liberty and Security Committee therefore urges Congress and the Executive Branch to clarify the nature and magnitude of the cybersecurity threat to the public so that the development and approval of comprehensive cybersecurity policies and public-private collaboration efforts are adequately shaped by the specific risks facing America's critical network infrastructure.

If the threats are really that significant, then why should we care about privacy rights and civil liberties?

- Privacy rights and civil liberties are fundamental protections guaranteed by the United States Constitution. We should not sacrifice basic constitutional safeguards in order to protect computer networks. Moreover, provisions designed to limit the amount of personally identifiable information and unrelated communications content that is shared with the government can help make cybersecurity programs *more* effective by focusing on actual threats and wrongdoers. Ultimately, while protecting our nation from cyber-attacks is vitally important, so too is protecting our privacy and due process rights. An effective cybersecurity program that also preserves civil liberties is a realistic goal that Congress can, and should, pursue.

People who follow the law have nothing to hide – why should we protect the privacy rights of criminals and hackers over protecting the nation?

- The right to privacy is a fundamental American value and is protected by the United States Constitution. People who follow the law may not have anything criminal to hide, but they legitimately may not want the government to be able to review and monitor their internet searches and private electronic communications, including political or religious leanings, medical aand private business transactions.

Given that it is an election year, what makes you think Congress will even consider cybersecurity legislation this year?

- Leaders in both houses of Congress and at the White House have announced that they plan to seek enactment of comprehensive cybersecurity legislation this year. *The Hill* reported in February that Senate Majority Leader Harry Reid (D-Nev.) plans to bring a cybersecurity bill straight to the Senate floor early this year, skipping any committee markups. Leaders in the House have also promised to consider such legislation following the Easter break. More than 50 legislative proposals dealing with cybersecurity, including one developed by the White House, were introduced in the Congress last year. Currently, there are two lead bills in the Senate (S. 2105 and S. 2151) and two lead bills in the House (H.R. 3674 and H.R. 3523).

When you talk about cybersecurity proposals that rely on information sharing between private networks and the federal government, what do these proposals entail? Specifically, what would trigger the transfer of private information to a government agency, and what information would the private network disclose?

- In general, these proposals would permit or require the sharing of cybersecurity related information between the private sector and the federal government, and vice versa. For example, in the Defense Industrial Base ("DIB") pilot program, originally operated by the Department of Defense and now transferred to the Department of Homeland Security ("DHS"), the federal agencies share classified threat intelligence with defense contractors. The defense contractors use these threat signatures to monitor their own private networks; if they come across the malicious signatures, then they notify the government that an attack has occurred. Under the White House's legislative proposal, private entities that already intercept, acquire, or otherwise obtain network communications may lawfully disclose that information to DHS for the purpose of protecting information systems from cybersecurity threats. The information shared currently in this pilot program may include sensitive personally identifiable information ("PII") or the contents of communications.
- Having the government share threat information with private industry does not raise civil liberties concerns, but it is critical that we incorporate privacy safeguards to cover the situation when private companies share information back with the federal government.

What are the risks caused by government monitoring of private networks?

- Government monitoring of private networks or review of private communications raises significant privacy and civil liberty concerns. If private companies share sensitive PII or the contents of communications with the federal government, this creates the risk that the receiving agency could share this information with other government agencies, including law enforcement. Without proper access, storage, and use restrictions, government agents could have the unfettered ability to review and use personal information and the content of private communications, and Americans would be subject to the equivalent of a perpetual "wiretap" on their private communications and web browsing behavior.

What can Congress do to protect Americans' privacy rights and civil liberties when implementing cybersecurity legislation?

- TCP's Liberty and Security Committee recently issued its "Recommendations for a Comprehensive and Constitutional Cybersecurity Policy." The report outlines 17 specific proposals that broadly recommend implementing effective privacy safeguards, establishing robust oversight, and limiting the scope of government access to or use of the content of communications.
- Specifically, TCP's Liberty and Security Committee recommends that any upcoming cybersecurity legislation that involves the sharing of information between the federal government and private parties have provisions that (1) require the anonymization of PII before data is shared with the federal government and (2) place use restrictions on the federal government for any data it receives from private industry to ensure that it is not used for any purposes other than detecting and preventing cyber-attacks, and prosecuting those who engage in such activity, or if there is probable cause of a non-cybercrime.

What privacy safeguards are needed?

- TCP's Liberty and Security Committee recommends that cybersecurity programs should rely upon private monitoring of private networks. To the extent that cybersecurity programs rely on partnerships between the government and the private sector, these programs should include specific procedures to limit the sharing of personally identifiable information ("PII") between the private sector and government actors. In most cases, data shared between the government and the private sector should have Americans' PII removed and sanitized.
- When private companies share cyber threat information with the federal government the information should be provided only to a civilian agency such as DHS. NSA and other military agencies should not be the recipients of private network information.
- Additionally, cybersecurity programs involving information sharing should require (1) strict time limits for data retention, (2) data anonymization whenever possible, and (3) policies to diminish the risk of inadvertent or improper disclosure of PII.
- TCP's report urges that any cybersecurity program should implement strict use restrictions for all data shared with or collected by the federal government. If federal agencies acquire content of private communications through cybersecurity operations, that information should only be used as necessary to implement the cybersecurity program and protect networks. Content and PII should not be shared with law enforcement officials or relied upon as evidence of a non-cybercrime, unless it was legitimately obtained as a necessary component of the data specifically flagged as a possible cybersecurity threat. All other data included in flagged communications should be unavailable for review by traditional law enforcement agencies without first obtaining a warrant.
- Cybersecurity initiatives and technologies that involve the interception of wire, oral or electronic communications should comply with the Wiretap Act and other statutes governing electronic surveillance by government agencies, again requiring government officials seeking to obtain the content of such communications to first obtain a warrant or order from an appropriate court. All existing exceptions to these statutory requirements, such as the exception for exigent circumstances that would necessitate immediate action would continue to apply.

How can the government be more transparent in its cybersecurity program and how can American citizens ensure that their privacy rights and civil liberties are not being violated by cybersecurity programs?

- Any federal agency developing new or expanded cybersecurity programs should first promulgate a Privacy Impact Assessment ("PIA") report, even if one is not required by the E-Government Act.
- Independent oversight must be established to ensure that constitutional safeguards are implemented and followed across federal agencies and private industry. First, the Privacy and Civil Liberties Oversight Board should be fully established and all five of the Board's seats should be filled; at present the Board does not exist. Second, legislation should require periodic mandatory audits by the Inspectors General of the relevant agencies and should require that the IG reports include a discussion of the nature and amount of information being shared with the federal government and how it is used. These reports should be submitted to all congressional committees of jurisdiction and each IG should also prepare an unclassified version that will be made available to the public.

How did the Liberty and Security Committee come to propose the recommendations included in the report?

- TCP is a constitutional watchdog that brings together policy and legal experts from across the political and ideological spectrum to reach a consensus on difficult constitutional issues. The Fourth Amendment in the Digital Age is one of the Liberty and Security Committee's ongoing interests, as too often, technology is developing more quickly than the law. The Committee has been working to develop new rules and best practices to ensure that Fourth Amendment protections continue to apply in the Digital Age. Recent Committee reports on applying the Fourth Amendment in the Digital Age include the following: 1) Liberty and Security Committee Statement on Location Tracking; 2) Suspicionless Border Searches of Electronic Devices; and 3) Principles for Government Data Mining. All three are available online at www.constitutionproject.org.

The Constitution Project released its report detailing the constitutional threats posed by current cybersecurity proposals—and its recommendations for addressing them—on January 27, 2012. The report is available at http://www.constitutionproject.org/pdf/TCPCybersecurityReport.pdf.