Testimony of Harriet P. Pearson
Partner, Hogan Lovells U.S. LLP

before the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Hearing on

Striking the Right Balance: Protecting Our Nation's Critical Infrastructure from Cyber Attack and Ensuring Privacy and Civil Liberties

April 25, 2013

Chairman Meehan, Ranking Member Clarke, and Members of the Subcommittee,

My name is Harriet Pearson and I am a partner in the Hogan Lovells law firm, where I focus on cybersecurity and privacy law.[1] From November 2000 until July 2012 I served as the IBM Corporation's chief privacy officer and security counsel.

Thank you for the opportunity to participate in this hearing on how we in the United States can protect our critical infrastructure from cyber-based threats while safeguarding individual privacy.

The relationship between cybersecurity and privacy is complex. On the one hand, cybersecurity that protects data from intrusion, theft, and misuse obviously is a significant privacy safeguard. On the other hand, cybersecurity measures that monitor access and use can implicate the collection of personal information (or data that can be linked to individuals), and thus raises privacy concerns.

Organizations of all types increasingly are taking steps to protect themselves and the people that rely on them from cyber-based threats. Cyber threats come from many different sources. The risk to information systems and the data that resides or travels on them can come from activists, criminals, or spies. Most of the time, these bad actors attack from outside the company; sometimes, they strike from within. Frequently they are enabled by the carelessness or inattention of otherwise well-meaning individuals who leave the digital analog of the front door open for easy entry. And sometimes there is no affirmative attack at all, as in case where a system malfunction occurs or sensitive data is lost or misdirected by accident—presenting risks that are still quite significant if such information gets into the wrong hands.

[1] My professional service includes membership on the advisory boards of the Future of Privacy Forum and the Electronic Privacy Information Center. I was a founding and long-time member of the board of the International Association of Privacy Professionals. I also serve on the American Bar Association President's Cybersecurity Legal Task Force, co-chair the Cybersecurity Law Institute of the Georgetown University Law Center, and was a member of the CSIS Commission on Cybersecurity for the 44th Presidency. The views I express are mine only, and are not offered on behalf of Hogan Lovells or its clients, or other organizations.

Since the critical infrastructure and the most valuable IP of our society are owned and managed largely by the private sector, the steps companies take to safeguard their most precious possessions and figuratively to lock their doors, close their windows, and make sure only authorized people and things cross the threshold are exactly the steps needed to improve cybersecurity for society at large. Sharing information about observed threat patterns and vulnerabilities with other companies and with appropriate authorities is also part of the mix. This is akin to participating in a neighborhood watch that involves proactive and collaborative engagement with law enforcement.

While adoption of cybersecurity defenses will, as I noted, serve to protect personal data (indeed, there can be no data privacy without sufficient security, including cybersecurity), some of the defense techniques may require the monitoring or collection of personal information, and thus implicate privacy concerns.

- *First, there is network and system monitoring.* Experts agree that in order to detect and defend against cyber attacks, organizations should be aware of how their information networks and IT systems are behaving. Such monitoring typically is focused on non-personal information such as malware indicators, bad IP addresses, and network flow data. Of course, the more specifically one monitors, and potentially records, activity, the more potential there is that personal data will be part of the information reviewed and/or collected.

- *The next issue is that of background checks.* Not all cyber-defense measures involve cyber tactics. Organizations frequently find it prudent to conduct background checks—at times quite extensive—on individuals with access to certain sensitive systems and data. By definition, background checks require the collection and use of personal information.

- *A new aspect of data security arises from the "Bring Your Own Device" phenomenon.* An increasing number of organizations are allowing their workforce to use personally owned smartphones, PCs, and other devices. The steps organizations take to secure such devices and the data that might be stored on them often involve access to personal data.

- *Steps taken to strengthen supply chain and vendor security may also raise privacy issues.* Security-conscious enterprises understand that the weakest link in their organization may lie outside their formal control. Measures imposed on their vendors and suppliers may require those third parties to conduct background checks and share other information that has privacy implications.

- *Information-sharing with third parties and government agencies means that personal information may be shared.* Finally, but importantly, experts agree that rapid and preferably automated cross-organizational sharing of cyber threat information is essential to help detect and defend against cyber attacks. And as Members well know, given the recent passage of H.R. 624, the Cyber Intelligence Sharing and Protection Act, there can be significant privacy issues raised by such sharing.

While each of these areas of cybersecurity techniques raises privacy concerns, those concerns can be addressed responsibly.

First, consistent with the well-known Fair Information Practice Principles,[2] data collection should be thoughtfully limited; used only for the purpose of security or other carefully considered and approved

[2] The U.S. privacy framework is based on underlying principles of fairness known as "Fair Information Practice Principles" or "FIPPs," which were first developed in the United States in the 1970s and have since

purposes; retained only for as long as needed for security and other legitimate purposes; and shared only with those that need the data for security or other carefully considered and approved purposes, with accompanying limitations on their sharing, use, and retention. These are concepts that privacy professionals in American business apply every day, and close collaboration between privacy professionals and security personnel at companies is essential to ensure that the security/privacy balance is correct and that Fair Information Practice Principles are applied to design privacy into cybersecurity programs.

Second, there should be transparency as to the cybersecurity measures that organizations, especially operators of critical infrastructure, increasingly are using. Transparency is fundamental to the Fair Information Practice Principles. When implemented, it reassures individuals that the processing of information that relates to them is not being done in secret, thus enabling them to pursue any recourse available if necessary.

As it relates to cybersecurity measures, transparency would include encouraging companies that are deploying network and systems monitoring to disclose their use of such measures (not in sufficient detail as to defeat their operations, of course, but in enough detail that individuals know about the systems monitoring the use of workplace technologies and the like). The more we inform and educate each other about how cybersecurity systems work, and how privacy considerations are addressed in their design and implementation, the more these measures are demystified.

Third, I endorse the development of voluntary codes of conduct for the privacy-sensitive deployment of cybersecurity measures and programs that are common enough to warrant such effort. Examples might include information-sharing codes of conduct, in which organizations that engage in information-sharing partnerships with each other and with governmental agencies develop and commit to adopting privacy-sensitive practices. Another example is new work by the National Institute for Standards and Technology as mandated by the recently-issued Executive Order on Improving Critical Infrastructure Cybersecurity, to develop a voluntary Cybersecurity Framework that includes consideration of privacy. As you know, NIST will be consulting with stakeholders in both government and industry as it develops the Framework. This Subcommittee can keep the focus on privacy issues by showing interest in, and requesting to see, how privacy is integrated into NIST's and others' cybersecurity efforts.

Finally, the expectations, responsibilities, and legal protections for privacy when data is shared with or requested by government need to be clear. Legislation that clarifies the rules surrounding information-sharing is a valuable first step, and it is encouraging to see that the privacy issues associated with information sharing have been discussed and that language addressing these issues has been included in the legislation proposed in this Congress. Further efforts by government and industry leaders, outside of new legislation, will also be useful to educate and enable stakeholders involved in these activities to design privacy into information-sharing and related activities.

Thank you for the opportunity to appear before you today and to present my thoughts on how we can achieve a meaningful balance between privacy and protecting the United States' critical infrastructure.

---

influenced every privacy law, regulation or code of conduct adopted in this and many other nations. The Fair Information Practice Principles focus on *empowering individuals to exercise control* over personal information that pertains to them, and on *ensuring that measures are taken to achieve adequate data security.*