Before the Commission on Enhancing National Cybersecurity

Request for Information: Public Awareness and Education

Comments of Public Knowledge

Megan H. Stifel
Gene Kimmelman
Public Knowledge
1818 N Street, NW
Suite 410
Washington, DC 20036
(202) 861-0020

September 8, 2016

Public Knowledge respectfully submits the enclosed draft Best Practices to Advance Consumer Privacy in Cybersecurity Information Sharing to the category Public Awareness and Education.

Current and future trends and challenges

A recent Pew Research Center Study revealed that 91% of adults agree or strongly agree that consumers have lost control of how companies collect and use personal information. The same study found that Americans lack confidence in the security of everyday communication channels and the organizations that control them, and in the ability of collecting organization – government or commercial – in keeping the personal information collected about them secure.[1] This lack of faith may also frustrate efforts to improve cybersecurity.[2] The evolution of big data and the Internet of Things make it critically important for government and industry to address this deficit soon in order to make real progress on cybersecurity; collective efforts to address these concerns will enhance our ability to better secure intellectual property, personal privacy, and economic prosperity.

Progress to address the challenges

Transparency, or the lack thereof, about the types of information collected and the purposes for which it will be used may contribute to the ongoing challenge described above. There are some areas of progress, but more can be done. For example, a growing number of corporations, particularly those in the information and communications technology (ICT) space, produce transparency reports. These reports detail, among other topics, the number of government requests for information about the companies' customers. Other elements of these reports, such as Google's, depict the company's efforts to identify and inform users about malicious websites. Few transparency reports, if any, discuss a company's efforts to address cybersecurity, including whether the company shares information for cybersecurity purposes.

Yet companies have been sharing information for cybersecurity purposes for years. In 1998, Presidential Decision Directive 63 encouraged the creation of information sharing and analysis centers, through which companies began to pool information to address the evolving threat posed by greater connectivity. More recently, in early 2015 the Obama Administration issued Executive Order 13691 to support the creation of information sharing and analysis organizations. And in late 2015, the Cybersecurity Act of 2015 ("the Act") granted liability protection to companies that share information consistent with its authorization. Notwithstanding its prevalence, little transparency exists about private sector to private sector information sharing. Many see a need for greater transparency and accountability surrounding the activities the Act authorized.

[1] http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america/
[2] https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf, at 6.

The Cybersecurity Act does require the government to provide some transparency with respect to the information sharing it authorized. To that end, the Act requires the government to publish several sets of guidelines, including privacy and civil liberties guidelines for information obtained by the government in connection with the Act. The government also published guidelines to assist non-federal entities when they share information with the government. In addition, the Act requires the government to publish a number of reports concerning its activities authorized by the Act, including compliance issues and the impact the Act has on the privacy and civil liberties of United States persons.

It is too early to determine the Act's impact on cybersecurity. In the interim, industry can take steps to improve its transparency and raise additional awareness about cybersecurity, which may in turn improve consumer practice and confidence. Adopting best practices to protect consumer privacy in private sector cybersecurity information sharing is one such step.

Promising approaches to address challenges

Challenges in the ICT space are often best addressed through multistakeholder engagement and the adoption of best practices. The Framework for Improving Critical Infrastructure Cybersecurity is a recent example of such an approach. Using a similar approach, Public Knowledge is leading a multistakeholder effort to develop best practices to protect consumer privacy in private sector cybersecurity information sharing.

Public Knowledge is undertaking this effort to address several issues plaguing progress on cybersecurity, including insufficient consumer awareness and education, low levels of trust among stakeholders, and few meaningful opportunities to bridge these obstacles. In particular, Public Knowledge believes that the process to develop best practices, and the practices once final, will serve as a tool to foster enhanced dialogue among stakeholders. Conversations surrounding the practices to date have highlighted the need for more detailed discussion about how industry addresses cyber threats: the types of information that is most useful, the way it uses the shared information, and how it handles the information once received, to name but a few.

The enclosed best practices are still evolving. They reflect preliminary input from civil society, government, and industry, and will benefit from upcoming engagements to ensure they are consistent with consumer privacy needs and meet industry's business needs. With private sector input, we will develop brief paragraphs to further explain the objectives of each practice and identify exemplary resources to achieve the stated objectives.

In this vein, the draft practices also offer an opportunity to raise awareness and educate a broad range of stakeholders. First, the practices' high level approach makes them accessible to entities at all levels of cybersecurity maturity. Second, from the very macro level to the finer details, the practices highlight the primary areas where personal information and cybersecurity information intersect, and outline approaches to minimize the privacy impact while maximizing the flow of information. Entities that choose to adopt the practices may elect to adopt additional elements

within particular practices to optimize the practices with the entities' business needs. They could also develop specialized practices for their business sector. In addition, the practices can be adopted regardless of an entities' primary place of business; they are globally applicable. By publicly pledging to follow these practices, entities will signal their commitment to consumer privacy and cybersecurity, thereby acknowledging the trust deficit the Pew Study identified.

Near and long term action to address challenges

As the cybersecurity threat evolves, so too will these best practices. Through the multistakeholder approach to develop the practices, participants are building relationships that will inform their current and future cybersecurity efforts, beyond information sharing. By facilitating these opportunities for dialogue, Public Knowledge believes a higher level of trust will develop that will support enhanced cybersecurity through improved education and greater awareness. Each of the practices presents an opportunity for industry and civil society to work together to champion its optimal implementation.

Public Knowledge recommends the Commission support the adoption of best practices to advance consumer privacy in cybersecurity information sharing. In doing so, the Commission would signal the importance of enhanced transparency as a tool to raise awareness and education on cybersecurity issues. Equally if not more importantly, the Commission would highlight the need to consider the privacy impacts of cybersecurity activities as they grow ever more sophisticated.

In submitting this contribution, we note its consistency with elements of Ms. Susan Grant's testimony to the Commission. We also highlight Mr. Eli Sugarman's testimony, which emphasized the importance of government and civil society partnerships in building trust to better address the evolving cybersecurity space.

About Public Knowledge

Public Knowledge promotes freedom of expression, an open Internet, and access to affordable communications tools and creative works. It works to shape policy on behalf of the public interest, including to ensure universal access to affordable and open networks; promote creativity through balanced copyright; advance government transparency and the public's access to knowledge; uphold and protect consumer rights; oppose policies that would slow technology, impede innovation, shrink the public domain, or limit fair use; educate the press, the public, and policymakers; and produce events that provide a forum for policymakers, the public, industry, and the press to exchange ideas about our core issues.

Draft Best Practices to Advance Consumer Privacy in Private Sector Cybersecurity Information Sharing

1. To the maximum extent practicable limit the effect on consumer privacy of cybersecurity information sharing

2. Publicly identify types of information that will be shared as cybersecurity information

3. Develop procedures to govern the receipt, use, retention, and dissemination of cybersecurity information

4. Disclose, retain, and use information shared for a cybersecurity purpose only for limited purposes, e.g., cybersecurity purposes

5. Remove information of a specific individual or that identifies, or is relatable to, a specific individual before sharing cybersecurity information, unless it relates directly to cybersecurity activities

6. As soon practicable destroy information that identifies a specific individual or is of a specific individual obtained through a cybersecurity program when such information does not directly support a cybersecurity activity

7. Use the Traffic Light Protocol or similar approach to limit cybersecurity information sharing consistent with these practices

8. Promptly notify a submitter or originator of information shared for a cybersecurity purpose that is not cybersecurity information

9. Apply to cybersecurity information appropriate protection from unauthorized access or acquisition

10. Regularly review cybersecurity information to ensure it remains useful for cybersecurity purposes

11. Update cybersecurity information repositories upon receipt of a notice and destroy erroneous cybersecurity information

12. Regularly audit the receipt, retention, dissemination, and use of cybersecurity information for compliance with these best practices

13. Discuss in transparency reports cybersecurity information sharing policies, practices, and audit results