BEFORE THE DEPARTMENT OF COMMERCE

PROMOTING STAKEHOLDER ACTION AGAINST BOTNETS AND OTHER AUTOMATED THREATS

COMMENTS OF PUBLIC KNOWLEDGE

Megan H. Stifel
Dylan Gilbert
Public Knowledge
1818 N Street, NW
Suite 410
Washington, DC 20036
(202) 861 – 0020

February 12, 2018

I. INTRODUCTION

Public Knowledge ("PK") supports the overall approach of the Report, which recognizes the need to increase transparency, raise consumer and organization awareness, expand implementation of known best practices, modernize education, review liability limitations, and reevaluate incentives given the critical role they play in improving cybersecurity beyond the status quo. In particular, we applaud and encourage the consideration of cybersecurity as an issue of sustainability, which the Report emphasizes in Goal 1: "Identify a clear pathway toward an adaptable, sustainable, and secure technology marketplace." As our prior comments to the Department, forthcoming working paper,[1] and broader work on cybersecurity[2] highlight, Public Knowledge believes increased transparency about most aspects of cybersecurity will further two important policy goals. First, at a technical level, broader sharing of cybersecurity information can enhance the overall security of the internet ecosystem, which will preserve it as a tool for the future. For now, however, in many instances knowledge of such data remains in narrow trust circles, which effectively limits the ability for others to learn from it, and consequently constrains our overall ability to improve ICT security. Second, enhanced transparency by developers, vendors, and breach victims will foster civil engagement as consumers become empowered with greater knowledge and information, enabling them to make better choices that can improve ICT security.

To begin to enhance transparency, prior PK comments have urged organizations to make public aspects of their cybersecurity practices. In an important recommendation, the Report calls for "more public commitments to avoid carrying malicious traffic."[3] We support this recommendation and urge relevant stakeholders to expand public statements beyond not carrying malicious traffic to other aspects of their cybersecurity practices, including whether and how they share cybersecurity information, how they train their workforce on cybersecurity issues, whether they employ best practices in software development, etc. These and similar actions are incorporated in our forthcoming working paper that proposes cybersecurity as a matter of sustainability.

In addition, PK wholeheartedly supports the Report's Action 1.1 recommendation to continue to develop best practices through a multistakeholder process. Multistakeholder methods have been at the heart of cybersecurity standards and specifications development for decades.

---

[1] A forthcoming working paper will discuss cybersecurity as a sustainability issue.

[2] *See* https://www.nist.gov/sites/default/files/documents/2016/09/16/stifel-kimmelman_rfi_response.pdf; https://www.thegfce.com/news/news/2017/05/31/raising-cybersecurity-awareness-by-building-trust-through-transparency.

[3] The Secretary of Commerce and The Secretary of Homeland Security, *A Report to the President on Enhancing the Resiliance of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, Draft for Public Comment (Jan. 5, 2018) at 12 ("Draft Report").

Recent successes in government-convened best practices development further evidence the utility and benefit of multistakeholder cybersecurity policy evolution.

PK understands the thrust of this report concerns botnets and the role of technology in their creation. Nevertheless, we urge the Department to expand the scope of Goal 1 beyond the technology marketplace to the entire ecosystem, which would include users from enterprises, providers, and consumers. Goal 5 takes a broader view, but several actions--e.g., Action 5.3, which focuses on computer science programs and Action 5.4, which focuses on engineering--narrow Goal 5's scope.

II. ACTION 2.3: THE FEDERAL GOVERNMENT'S ROLE IN CREATING MARKET INCENTIVES FOR EARLY ADOPTERS

PK agrees that vendors must be incentivized to prioritize device security. A functioning market cannot exist without consumer trust,[4] and consumer trust can be fostered significantly by modifying vendor behavior. This behavioral modification must take place as far "up the chain" as possible. Market incentives should be designed, however, with all vendors, not merely bad actors, in mind. The 2016 discovery of privacy flaws in the Glow fertility tracker application illustrates well the fact that even good faith vendors can create privacy issues when market incentives are aligned to minimize cost and time to market.[5] While generating consumer-friendly market incentives may lead to some increased costs, ensuring consumer trust across the ecosystem must be the ultimate policy goal.

Imposing some degree of liability on upstream vendors for inadequate consumer data protection could provide the necessary market incentives to establish and maintain consumer trust. It may be helpful to consider the liability of distribution platforms and its potential analogy to vendor liability in the physical world. Generally, vendors are not held liable for selling products they have no reason to believe are defective. But it is worth considering the set of circumstances in which the policy has been changed in favor of vendor liability. For example, instances of drunk driving significantly declined when bars began to be held liable for willful blindness. Something similar with regard to distribution platforms like the Apple Store and Google Play Store could be a valuable market mechanism to address basic privacy and security issues in apps. These intermediaries could act in effect as trust brokers to assist consumers who might be confused or overwhelmed by complex privacy policies buried in the fine print.

Market incentives must be tailored to reduce costs and barriers to entry. One solution could be to impose different standards based on the sensitivity of the personal information with

---

[4] *See generally*, George A. Akerlof, *A Market for "Lemons": Quality Uncertainty and the Market Mechanism*, The Quarterly Journal of Economics, Vol. 84, No. 3 (Aug. 1970), available at https://www.iei.liu.se/nek/730g83/artiklar/1.328833/AkerlofMarketforLemons.pdf.

[5] *See, e.g.,* Jerry Beilinson, *Glow Pregnancy App Exposed Women To Privacy Threats, Consumer Reports Finds*, Consumer Reports (Jul. 28, 2016), available at https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/.

which the vendor engages. So, for example, a vendor that engages in broad data practices or that processes sensitive personal information could be subject to strict liability. A less stringent liability standard such as negligence could be imposed if vendors process non-sensitive personal information.

Any approach to intermediary liability must minimize the risk of intermediary censorship. This can be accomplished by developing a basic set of standards that define what distribution platforms should expect of an application prior to distribution and what circumstances under which the platforms will stop distributing. In this regard, any liability on distributors should be consistent with a set of guiding principles such as the Manila Principles on Intermediary Liability.[6]

The Report suggests that the U.S. Government can establish market incentives for early IoT adopters by developing compliance guidelines for federal procurement.[7] As a threshold matter, procurement requirements are necessary. We support the government practicing what it preaches by adopting and implementing best practices and requiring the same of those who support it. The government should not knowingly support the acquisition of software that does not follow best development practices. To the extent that procurement requirements can be a market incentive, we believe such measures can be potentially helpful but note that government procurement excludes a large number of products.

Any federal standard must be open and reasonably accessible to everyone. Standards should also be set by a neutral body that can easily certify new products or applications. We support the nascent cybersecurity work of Underwriters Laboratories ("UL"), which is a well-known seal of approval in the traditional appliance market. Efforts such as UL's and the Digital Standard under development by Consumer Reports can serve as tools to translate complex software privacy and security design processes into features and capabilities a consumer understands, just as today many consumers look to symbols to know if a product is energywise, can be recycled, or is cruelty or conflict free. More formally, one potential approach to standards setting may be to expand the Consumer Product Safety Commission to cover new technologies that may be vulnerable to botnets and other distributed threats. While such an approach would not cover all devices vulnerable to such threats, properly implemented it could reduce the attack surface.

III. ACTION 2.4: INDUSTRY AND GOVERNMENT COLLABORATION TO STANDARDIZE INFORMATION-SHARING PROTOCOLS

PK supports information sharing consistent with the Cybersecurity Information Sharing Act of 2015, which requires the removal of sensitive personal information unless it is necessary to understand the shared information. To enhance privacy protections in cybersecurity

[6] *See* Electronic Frontier Foundation, *Manila Principles on Intermediary Liability*, EFF.org (Mar. 24, 2015), available at: https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.
[7] *See* Report at 29.

information sharing, in 2017 the Information Sharing and Analysis Organization published ISAO SP4000 on Protecting Consumer Privacy in Cybersecurity Information Sharing. PK led the development of these practices, and we encourage their adoption throughout the ecosystem. Furthermore, as noted above and in our submission to the President's Commission on Enhancing Cybersecurity, we highlighted the need across the ecosystem for enhanced transparency around organizations' cybersecurity practices.

IV. ACTION 2.5: NETWORK MANAGEMENT BEST PRACTICES

As a civil society organization frequently engaged with the Federal Communications Commission, Department of Justice, and state courts on matters involving competition and communications platforms, PK has a particular interest in the development of traffic management best practices and expertise in what impact these actions may have on competition. PK welcomes the opportunity to participate in such discussions.[8]

V. GOAL 4: COALITIONS BETWEEN SECURITY, INFRASTRUCTURE, AND OPERATIONAL TECHNOLOGY COMMUNITIES

PK supports this laudable goal but notes that it currently overlooks the role of civil society organizations in building such relationships. For example, in 2017, PK worked with the Organization of American States to strengthen the legitimacy and political robustness of government cybersecurity strategies and policies by incorporating the perspective of civil society groups. We recommend the Report include civil society in building these coalitions, including working directly with such organizations to support adoption of best practices by, among other things, translating best practices into local languages and facilitating opportunities for training and implementation, as further described infra at IX.

VI. ACTION 4.1: INFORMATION SHARING WITH LAW ENFORCEMENT

PK supports cybersecurity information sharing between and among public and private sector organizations, provided that organizations responsibly collect, maintain, and disclose such information. To that end, we note that last summer the ISAO SO published relevant guidance.[9]

---

[8] Some have expressed concern that sharing cybersecurity information via peering agreements could trigger anti-competitive/antitrust issues. In 2014, the FTC and DOJ issued a policy statement on the sharing of cyber-security information stating that, properly designed, cyber threat information sharing is not likely to raise antitrust concerns and can help secure the nation's networks of information and resources. *See, e.g.,* https://www.ftc.gov/news-events/press-releases/2014/04/ftc-doj-issue-antitrust-policy-statement-sharing-cybersecurity.

[9] *See* https://www.isao.org/products/isao-sp-4000-protecting-consumer-privacy-in-cybersecurity-information-sharing-v1-0/.

VII. ACTION 4.2: INTERNATIONAL ADOPTION OF BEST PRACTICES

PK supports the development of a public and private sector engagement strategy for international standards bodies. In particular, government, private sector, and civil society collaboration in such an effort can support incorporation of U.S. values including the protection of privacy and human rights into developed standards. PK also supports greater private sector support to enhance technology law and policy capacity abroad, which could leverage in part existing sales and distribution networks to ensure that when new users and devices come online they do in a more safe and secure manner.

VIII. ACTION 4.3: NON-DECEPTIVE MARKETING AND SECTOR-SPECIFIC SECURITY REQUIREMENTS

PK agrees with the need to ensure that companies participating in the IoT market, along with traditional technology markets, do so in a responsible manner and not deceive customers and consumers with false or unsubstantiated representations regarding a product's data privacy and security capabilities. Developing marketing requirements assumes a parallel process that validates software and hardware privacy and security capabilities, which at this time is still very nascent and may require additional incentives to reach initial operating capability. In addition, PK concurs with the need to be cautious to avoid creating "static and ineffectual compliance requirements."[10] Liability regimes can develop gradually and in a case-by-case manner, taking into account the role of each player, economic considerations, and changing facts. Indeed, this is how tort law, including product liability, initially developed. A liability-based regime in the IoT and cybersecurity areas can proceed similarly, allowing a set of broad principles and evolving precedent to provide a framework for industry actors.

IX. ACTION 5.4: CYBERSECURITY EDUCATION

Establishing cybersecurity as a fundamental requirement in the engineering disciplines is an important first step to enhance cybersecurity. However, given the growing role data plays throughout the digital economy, PK submits there is an immediate need for a wholesale revision to cybersecurity education requirements in the United States. We encourage the Departments of Commerce and Homeland Security to consult with the Department of Education and other relevant stakeholders to strengthen and jump start the National Initiative for Cybersecurity Education to ensure age appropriate cybersecurity education and training beginning in Kindergarten.

[10] Draft Report at 23.

X. ACTION 5.5: GOVERNMENT SPONSORED PUBLIC AWARENESS CAMPAIGN

As noted above, PK supports efforts to raise awareness, enhance transparency, and strengthen trust throughout the ecosystem. To that end, PK supports efforts such as the Digital Standard that will inform consumers of important features in a comprehensible fashion. This and other efforts will help to build market demand for products that are safe and secure, where consumer product companies and organizations across the ecosystem recognize their role as stewards of consumer data.[11]

XI. CONCLUSION

Public Knowledge applauds the Departments of Commerce and Homeland Security for the important concepts outlined by the Draft Report. As our comments have highlighted, as implementation of the identified actions begins, it is critical to include civil society organizations where appropriate, particularly where the actions impact consumers. PK is available and interested in working with stakeholders to ensure the final Report and its recommendations advance cybersecurity and protect consumers.

[11] PK emphasizes that awareness campaigns and the underlying best practices should be developed with user behavior in mind. For example, early in the Draft Report there are several references to unpatched, pirated software. Rather than focus on one reason (pirating), we note that there are non-pirate reasons why people might disable software updates—and some vendors do distribute software updates to anyone but will disable features if they detect the software is pirated. But there might be performance reasons. People might be able to tweak just one version of software, updates may break compatibility with some software, or they might just be too difficult to install—patching the firmware on a TV or a router can be very technically challenging. We support the Draft Report's efforts to consider the lifecycle of devices and consumer behavior in product development and support.