In the Matter of Stakeholder Engagement on Cybersecurity in the Digital Ecosystem

U.S. Department of Commerce
National Telecommunications and Information Administration
Docket No. 150312253–5253–01
Submitted via email to securityRFC2015@ntia.doc.gov

May 28, 2015

Thank you for this opportunity to respond to the National Telecommunications and Information Administration's (NTIA) Request for Public Comment on the effort of the Department of Commerce Internet Policy Task Force (IPTF) to "identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers."[1] Access commends the IPTF on the development of inclusive, transparent cybersecurity processes that aim to defend the digital ecosystem. However, we believe the IPTF effort must do more to protect users while respecting the fundamental rights they exercise online.

Access defends and extends the digital rights of users at risk. We advocate for a holistic approach to cybersecurity that respects the end user as well as hardware and software. The IPTF multistakeholder process has the potential to ratchet up protections across the entire internet ecosystem, including the networks and channels that process and store user data. The IPTF should promote practices that protect the entire internet ecosystem without risking user privacy.[2]

The IPTF is seeking to develop a multistakeholder process "built on the principles of openness, transparency, and consensus." Outcomes could include "voluntary policy guidelines, procedures, or best practices." The IPTF's current work builds upon previous U.S. government cybersecurity efforts, including a 2011 Department of Commerce report, *Cybersecurity,*

[1] National Telecommunications and Information Administration, *Stakeholder Engagement in Cybersecurity in the Digital Age*, Dock. No. 150312253-5253-01, 14360, 14360 (Mar. 19, 2015), http://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf [hereinafter Request for Public Comment].
[2] *See, e.g.*, The Online Trust Alliance, *OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented* (Jan. 21, 2015), https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented.

Innovation, and the Internet Economy,[3] and Executive Order 13636 (EO 13636) issued in February 2013.[4]

Access encourages IPTF to consider the human rights impact of any best practices that it develops both domestically and internationally. Cybersecurity is collectively improved if policies are developed with an eye toward the security of all systems, not only those within the United States. While Access believes the efforts of the IPTF are preferable to current sweeping proposals for regulatory or legislative action, particularly those that ignore human rights or transfer responsibility for cybersecurity to military organizations, policies developed through the IPTF multistakeholder process or through other channels should not interfere with the openness of the internet.[5] Specifically, Access suggests that IPTF:

- evaluates the impact of any cybersecurity process on user rights, including privacy and freedom of expression;
- develops rules to support adoption of strong digital security tools and technologies, including end-to-end and device encryption;
- coordinates with companies on an education campaign instructing users on precautions to reduce the risk of malware and other malicious activities; and
- encourages international cooperation guided by principles such as due process, oversight, and transparency.

The relationship between security and human rights

As the IPTF has noted, "privacy and civil liberties implications may arise when personal information is used, collected, processed, maintained, or disclosed in connection with an organization's cybersecurity activities."[6] Privacy need not be sacrificed to achieve strong digital security. Many security solutions also protect privacy. For example, encryption tools improve security and protect privacy. However, the IPTF should avoid promoting security measures that undermine privacy or the neutrality of the internet.

The user-up approach to cybersecurity, which implicates strong encryption, user education, and rapid fixes for vulnerabilities that put users at risk, seeks to improve the entire security

[3] The Department of Commerce Internet Policy Task Force, *Cybersecurity, Innovation and the Internet Economy (The Green Paper)*, (June 2011), http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf (The Green Paper focuses on the security of businesses not classified as critical infrastructure and how the dynamic change of the digital ecosystem challenged the usefulness of "traditional regulation" and compliance).

[4] Required the National Institute of Standards and Technology (NIST) to create a voluntary framework in consultation with the private sector for improving the cybersecurity of critical infrastructure. EO 13636 also contained provisions designed to increase the volume and quality of shared cyber threat information.

[5] While the IPTF cybersecurity processes have factored privacy and user security, other cybersecurity proposals by the Obama Administration and bills introduced in Congress would create new risks to user security and privacy. For instance, the Administration's information sharing proposal would grant companies sweeping liability protection against privacy laws, removing the incentive for companies to protect user privacy; *see* President Barack Obama, Information Sharing Legislative Proposal, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-information-sharing-legislative-proposal.pdf.

[6] Request for Public Comment at 14362.

ecosystem. It recognizes that no individual effort will provide a perfect solution, but instead that cybersecurity is a shared responsibility. Cooperation between users, companies, and the government is critical. The IPTF is well suited to work with all stakeholders to develop rules in line with the user-up approach to cybersecurity.[7]

Effective security solutions can and should promote user privacy. David Kaye, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, recently released a report highlighting the relationship between encryption and anonymity and the rights to privacy and freedom of expression:

> "Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."[8]

While the IPTF should be commended for considering privacy, it should ensure any cybersecurity process properly evaluates impact on user rights.

Protecting user data

Insecurity harms user privacy and risks trust in the internet ecosystem.[9] A study by the Pew Research Center illustrates that "[a]cross the board, there is a universal lack of confidence among adults in the security of everyday communications channels".[10] Users are concerned

---

[7] Instead, the Obama Administration has prioritized Information sharing. The President's information sharing legislative proposal would increase the government's role in transferring data and provide broad liability protections for companies handling personal information. In February, President Obama issued Executive Order 13691 "Promoting Private Sector Cybersecurity Information Sharing". Executive Order No. 13,691, 80 Federal Register 9347 (Feb. 13, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari. Based on the Executive Order, the Department of Homeland Security is undergoing a process of developing standards to guide Information Sharing and Analysis Organizations (ISAOs), organizations to promote sharing between the private sector and the government. Aaron Boyn, *DHS Offering $11M Grant for Info Sharing Standards*, (May 27, 2015), http://www.federaltimes.com/story/government/cybersecurity/2015/05/27/dhs-grant-info-sharing/28012873/. However, security experts have shown that companies do not need immunity. Existing privacy laws do not prohibit sharing the types of information useful for network security. Ben Adida et al., *Letter from technologists to Members of Congress* (Apr. 16, 2015), https://cyberlaw.stanford.edu/files/blogs/technologists_info_sharing_bills_letter_w_exhibit.pdf. Information sharing is a reactive policy solution, and fails to protect against the newest attacks.

[8] Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/29/32, 3, (May 22, 2015).

[9] *See* Center for International Governance Innovation and Ipsos, *Global Survey on Internet Security* (Nov. 14, 2014), https://www.cigionline.org/internet-survey (Finding that 36% of users believe their private information is very secure on the internet).

[10] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, Pew Research Center Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

with the impact of government surveillance programs on digital security as well as the potential for malicious actors to access their personal information.[11]

The companies that store and transmit personal information have not taken adequate measures to implement security protocols that protect users. While corporate financial losses from recent large-scale data breaches have been less than anticipated, the harm suffered by the billions of users impacted by these breaches extends beyond their monetary impact to also include inestimable intangible damages.[12] More needs to be done to ensure companies have the proper incentives to implement adequate security that protects all user information. Furthermore, companies need to take a pro-active approach toward notifying users when their information has been compromised, regardless of potential financial impact on users.

In recognition of some of the gaps in corporate digital security practices, Access developed the Data Security Action Plan.[13] The Plan, which was developed in consultation with technology experts and members of the private sector, consists of seven steps that companies can take to provide a minimum level of protection for user data. While increased security will not stop all data breaches, it would reduce the total number and minimize the impact by increasing the cost of unauthorized access to sensitive user data.

Promotion of security best practices

The IPTF should promote the adoption of security best practices. Efforts to protect critical infrastructure miss many of the most frequently used systems and services, leaving weak points in the security ecosystem.[14]

Encryption and other security measures

Strong digital security practices should be adopted as an element of any corporate comprehensive security plan. As we've noted,

> "[Increasing] digital security and reining in unauthorized access to data does not necessarily shut down legitimate access to data for law enforcement or national security purposes. There are several different approaches that may be taken for officials to appropriately compel necessary information. What data security will do is protect users

[11] *See* Center for International Governance Innovation and Ipsos, *Global Survey on Internet Security* (Nov. 14, 2014), https://www.cigionline.org/internet-survey (Finding that 61% of users are concerned that government agents from their own countries are monitoring their online activities and that 77% of users are concerned about someone hacking into their accounts to steal their personal information).
[12] Benjamin Dean, *Why Companies Have Little Incentive to Invest in Cybersecurity*, The Conversation (Mar. 4, 2015), http://theconversation.com/why-companies-have-little-incentive-to-invest-in-cybersecurity-37570 (Reporting that 2014 network breaches of Sony Pictures, Home Depot, and Target cost each company an estimated 1-2% of their annual sales).
[13] Access, Data Security Action Plan, https://encryptallthethings.net/docs/EATT.pdf.
[14] For example, the NIST Cybersecurity Framework was developed for critical infrastructure: the systems the incapacitation or destruction of which would debilitate security, economic security, public health, or public safety.

and their financial, legal, and professional interests from unlawful or unauthorized third-party or government access.[15]

The IPTF should develop rules to support adoption of strong digital security, including end-to-end and device encryption. Special Rapporteur Kaye noted that companies also have responsibility to protect human rights and ensure a positive impact of their work.[16] As he makes clear in his report, security measures are critical for the exercise of human rights. Proper security measures protect against potential snoopers, and increase protections for worldwide users facing more acute threats.[17] The IPTF, as part of the multistakeholder process, is well situated to determine effective security measures.

The IPTF can build upon existing efforts to identify industry standards. For instance, as discussed above, Access has identified minimum security-enhancing steps applicable to every internet platform in the Data Security Action Plan. The seven steps of the Action Plan include: (1) Implement strict encryption measures on all network traffic; (2) execute verifiable practices to effectively secure user data stored at rest; (3) Maintain the security of credentials, and provide robust authentication safeguards; (4) initiate a notification and patching system to promptly address known, exploitable vulnerabilities; (5) use algorithms that follow security best practices; (6) enable or support use of client-to-client encryption; (7) provide user education tools on the importance of digital security hygiene.[18]

The Data Security Action Plan is not meant to be exhaustive, nor is it intended to address unique challenges of particular services. The IPTF should utilize the multistakeholder process to expand upon the Action Plan to create a flexible set of best practices that can be tailored to particular industries and updated as the security landscape evolves.

Malware and botnets

Any initiatives to counter the spread of malware must adequately protect privacy and the integrity of the internet. Solutions must target the companies that can take measures to limit exposure to malware and users who can better understand risks. Industry best practices should be paired with an increased focus on user education, highlighting the risks of unknown apps and advertisements.

[15] Amie Stepanovich, *Fool's Gold: Data Security is Vital to User*, Access (Oct. 16, 2014), https://www.accessnow.org/blog/2014/10/16/fools-gold-data-security-is-vital-to-users.
[16] In the future, Special Rapporteur Kaye plans to focus on the human rights responsibilities of companies relating to security; A/HRC/29/32 10-11.
[17] *See* Andrea Peterson, *Today's Internet Users are Still Being Hurt by 990s-era U.S. Encryption Policies* (May 28, 2015), http://www.washingtonpost.com/blogs/the-switch/wp/2015/05/28/todays-internet-users-are-still-being-hurt-by-90s-era-u-s-encryption-policies/.
[18] Access, Data Security Action Plan, https://encryptallthethings.net/docs/EATT.pdf.

The 2015 Symantec Internet Security Threat Report showed increased prevalence of ransomware and "malicious advertising."[19] Such attacks pose particular threats to users, especially users without knowledge of basic digital security. Malicious advertisements can operate on major, trusted platforms. The number of parties, including the platform, advertising agency, and company advertising, permits the diffusion of responsibility and creates an additional challenge for attribution.[20]

Existing efforts to counter malware and botnets, including a voluntary botnet code of conduct for internet service providers, have not adequately protected privacy and the integrity of the internet.[21] The IPTF should coordinate with companies on an education campaign instructing users on precautions reducing the risk of malware. With fewer devices susceptible to control, the accessibility of botnets decreases. In addition, the voluntary botnet code should be strengthened to better protect privacy and make clear that blocking and direct monitoring are invasive to users and their use should be discouraged. There must also be some incentive for service providers to protect users — potentially through an increased role for CERTs, which may aid in companies failing to provide adequate security.

International Cooperation

Insecurity abroad can foster insecurity at home. According to an article in the *Harvard Business Review*, cybersecurity "is a global problem requiring a global solution" and "[i]nternational cooperation is critical."[22] The IPTF must utilize the multistakeholder process to encourage international cooperation guided by principles such as due process, oversight, and transparency.[23] Increasing cooperation would reduce the justification for government surveillance tactics that harm digital security.[24]

When a non-negligible amount of cybercrime originates abroad, inward-focused policies are inadequate. Access has teamed with companies and civil society organizations to promote the

[19] Symantec, *Internet Security Threat Report Volume 20*, 17, 41 (Apr. 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf.
[20] Rahul Kashyap, *Why Malvertising is Cybercriminals' Latest Sweet Spot,* Wired (Nov. 2014), http://www.wired.com/2014/11/malvertising-is-cybercriminals-latest-sweet-spot/
[21] Existing IPTF efforts to counter botnets include the Federal Communication Commission (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) developed U.S. Anti-Bot Code of Conduct for Internet Service Providers. The Code of Conduct only encourages "respect" for privacy and fails to address whether blocking user access or directly monitor user activity is appropriate. It does little to incentivize adherence; Communications Security, Reliability and Interoperability Council (CSRIC), *Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)*, (Mar. 2012), https://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf
[22] David M. Upton, *The Flaws in Obama's Cybersecurity Initiative*, Harvard Business Review (Jan. 20, 2015), https://hbr.org/2015/01/the-flaws-in-obamas-cybersecurity-initiative.
[23] *See* International Principles on the Application of Human Rights to Communications Surveillance, Principle on Safeguards for International Cooperation (May 2014) https://en.necessaryandproportionate.org/text#principle_12.
[24] *See e.g. Jeremy Scahill and Josh Begley, The Great SIM Heist*, The Intercept (Feb. 19, 2015), https://firstlook.org/theintercept/2015/02/19/great-sim-heist/.

mutual legal assistance treaty (MLAT) system as a way of encouraging the sharing of information between governments in a rights-respectful manner.[25] However, MLATs do not cover the transfer of all types of information.

International cooperation should promote collaboration and exchange of methods of addressing security risks. According to the Organization for Economic Co-operation and Development (OECD), cross-border cooperation on botnet mitigation is limited due to "legal, organisational, and technical barriers".[26] The IPTF should develop the standards for companies engaging internationally with the objective of protecting the interests and rights of users.

Conclusion

Incentives should encourage companies to adopt identified practices that protect human rights of users. However enforced, "openness, transparency, and consensus-building" are critical to developing user-friendly cybersecurity rules.[27] As the IPTF moves forward, it must ensure it develops rules that protect user security and the rights they exercise online.

Respectfully Submitted,

Amie Stepanovich
Access U.S. Policy Manager

Drew Mitnick
Access Policy Counsel

[25] Access et al., Letter to Congressional Leaders in support of improvements to MLAT process (Apr. 23, 2015), http://www.siia.net/Portals/0/pdf/Policy/International/MLATfunding_CongressionalLeadership_23April2015.pdf.
[26] Organisation for Economic Co-operation and Development, *Proactive Policy Measures by Internet Service Providers Against Botnets*, 14 (May 7, 2012), http://www.oecd-ilibrary.org/docserver/download/5k98tq42t18w.pdf?expires=1432792446&id=id&accname=guest&checksum=7B3CE7603CDD999E735EFE69DB11E21E.
[27] Request for Public Comment at 14363.