Cybersecurity Coalition

November 9, 2018

Submitted via email: privacyrfc2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue N.W., Room 4725
Attn: Privacy RFC
Washington, DC 20230

RE: Request for Comment on "Developing the Administration's Approach to Consumer Privacy"

The Cybersecurity Coalition ("Coalition") submits this comment in response to the Request for Comments ("RFC") issued by the National Telecommunications and Information Administration ("NTIA"), on behalf of the U.S. Department of Commerce, on September 26, 2018. The Coalition is comprised of leading companies with a specialty in cybersecurity products and services dedicated to finding and advancing consensus policy solutions that promote the security of digital systems and individual users. We seek to ensure that government agencies and companies of all sizes are able to take appropriate steps to improve their cybersecurity risk management.

The Coalition appreciates the opportunity to provide these comments and participate in this important discussion. The Coalition supports the advancement of a reasonable, risk-based federal privacy framework in which effective security principles are incorporated as a necessary component. We are encouraged by NTIA's inclusion of security as one of the seven desired privacy outcomes and note that robust security practices are critical to improved privacy protection. In these comments, the Coalition reiterates the importance of several key privacy outcomes and high-level goals set forth in the RFC, and provides additional recommendations for NTIA's consideration. In particular, the Coalition emphasizes: the importance of security as a key privacy principle; the need for an explicit recognition of security efforts as a legitimate interest based on recognized responsible practices; the role of privacy and security by design; a risk and outcomes-based approach; and incentives for the adoption of industry standards.

I. Privacy Outcomes

Security. Coalition members, as well as our peers in the cybersecurity industry, are charged with safeguarding the security of personal information on behalf of clients, as well as the personal information we ourselves collect, process, and store for routine business purposes. Security practices protect the confidentiality, availability and integrity of data and prevent waste, fraud, and abuse from external and internal actors. The Coalition supports NTIA's conclusion that security is a critical privacy outcome to protect personal information against risks of unauthorized access, misuse, and breach. The RFC's high-level description of the security principle is generally clear

and touches on the key concepts of reasonableness relative to risks and comprehensive protections at all stages of data collection, storage, processing, and transport.

As the RFC suggests, consensus best practices and widely accepted standards, where available, are important benchmarks in determining appropriate security protections, as well as providing clarity on compliance requirements. The Coalition believes that NTIA should consider incentivizing organizations to implement comprehensive, standards-based security programs with liability protections. This would encourage good corporate behavior and reward those companies that protect data in accordance with recognized industry standards and best practices.

Below we highlight the processing and sharing of threat information as regular components of a comprehensive security program, and in the federal action section we recommend NTIA ensure the privacy framework enables appropriate information processing and sharing activity to advance security.

Processing and Sharing Threat Information to Protect Privacy. To help organizations satisfy their privacy obligations and protect customers from privacy harms caused by security incidents, many organizations (including but not limited to companies in the cybersecurity industry) process and share large-scale information about cybersecurity threats. This is consistent with consensus best practices for comprehensive security programs, such as the NIST Cybersecurity Framework.[1]

Coalition members process threat data from hundreds of millions of Internet points of presence, the local access points that allow users to connect to the Internet with their Internet Service Provider ("ISP"), to ensure the security of customers' networks and personal information ("PI"). As discussed further below, collecting PI comes with the obligations of data stewardship including minimization, security, and other important privacy practices. Processing this data enables cybersecurity providers to detect cyberattacks that can lead to unauthorized access, misuse, and breach of personal information. Sharing threat data with other organizations – including other service providers, Information Sharing and Analysis Organizations, or computer emergency response teams – for security purposes can help those organizations mitigate vulnerabilities that compromise the confidentiality of personal information, avoid exposures that can lead to accidental breach of personal information, prepare for suspected or known malicious actors, and more.

By necessity, some of this data can be linked to individuals or specific devices, thereby potentially falling under common definitions of "personal information." For example, phishing, a highly prevalent and effective attack vector used to steal sensitive data, is based on spoofed emails and identities. To detect and avoid suspected phishing attempts, cybersecurity service providers may process such personal information including the email address, purported identity, and the IP address associated with the origination of the phishing email. This information may also be shared with other organizations for the purpose of helping them prevent the same attack.

[1] See, for example, ID.RA-2 and RS.CO-5 on information sharing in the NIST Cybersecurity Framwork.

Cybersecurity Coalition

Another example of processing "personal information" to protect privacy is the identification of devices for security purposes (see, *e.g.*, the Asset Management category of the NIST Cybersecurity Framework). As more digital devices become internet-accessible, there is a growing need for data and applications to be shared among devices and to be stored remotely (*e.g.* in the cloud). For there to be appropriate protections for this data, there must be increased focus on security of the networks, the connections between and among cloud services, and individual end devices. The presence of unauthorized or unsecure devices on a network can lead to compromise of the network, putting personal information accessible on that network at risk. Processing and sharing device information (*e.g.*, IP address, MAC address, or other device identifier) is a necessary activity for ensuring the devices connected to networks are authorized and secure. Identifying connected devices that are unauthorized, or devices associated with known attacks (such as devices flagged as participating in botnet activity), can help organizations prevent threats to the confidentiality and integrity of personal information, as well as comply with privacy and security requirements.

The processing and sharing of cyber threat information is a necessary component of a comprehensive security program, which in turn is an integral part of a privacy framework. The Coalition recommends below, in the federal action section, that any federal privacy framework ensure this beneficial activity can continue to effectively protect security and privacy. It is important to avoid overly broad limitations on information sharing or a narrow "exception" for security practices in order to ensure companies have the necessary flexibility and incentives to undertake critical cybersecurity activities.

Privacy and Security by Design. The RFC preamble states that the desired end goal includes products and services that are inherently designed with appropriate privacy protections. The RFC also states that external accountability should encourage privacy by design. The Coalition supports these outcomes and notes that privacy by design must also include security by design, because security is a critical principle in an effective privacy framework.

A combination of policy, standards, procedures and guidelines are used to drive the effective management and protection of personal information in operational business processes and the development of products and services. Privacy and Security by Design requires companies to proactively consider privacy and security when developing products and services for the marketplace, as well as when implementing internal tools. This proactive approach to designing technology is the most effective and efficient way to enable data protection because the data protection strategies are integrated into the technology when it is created. The Coalition believes Privacy and Security by Design encourages accountability in the development of technologies, making certain that privacy and security are included as a foundational component of the product and service development process. The Coalition advocates proactive Privacy and Security by Design to provide the most effective end-to-end privacy and security technology solutions.

II. High-Level Goals for Federal Action

Enabling cybersecurity activity. Effective cybersecurity solutions require regulatory policies that enable effective and responsible data processing, data sharing and threat analysis. As

described above, processing and sharing data for defensive cybersecurity purposes is a critical activity for safeguarding personal information, complying with privacy and security requirements, and avoiding privacy harms. This must be performed in a responsible and transparent manner, taking into account the nature of the data, the risk of its loss or misuse, and the tools available to minimize these risks, all established components of responsible data protection programs. The Coalition urges NTIA to ensure that the privacy framework does not restrict responsible processing and sharing of information for defensive cybersecurity purposes, both by first party collectors of information and third parties processing information on behalf of others.

Numerous privacy regulations and best practices explicitly recognize the need for processing data for cybersecurity purposes and permit the use, retention and sharing of information for cybersecurity on legitimate interest and other bases beyond user consent. For example, the European Union's General Data Protection Regulation (GDPR) frames network and information security as a generally applicable legitimate interest for processing personal data and does not limit the processing of this data to circumstances in which an end-user has expressly consented to the collection and use of data. The GDPR's legitimate interest analysis accounts for context and reasonable controls, including minimizing data where appropriate and transparency concerning data handling practices.[2] Similarly mindful of the critical importance of cybersecurity, the California Consumer Privacy Act notes that service providers are not required to comply with individual requests to delete personal information if maintaining that information is necessary to detect security incidents or protect against malicious, fraudulent, or illegal activity.[3] To achieve NTIA's privacy and security goals and provide consumers and organizations with appropriate protection, we believe similar provisions allowing the processing of data based upon risk-based decision-making and responsible data handling practice will be necessary in a federal privacy framework.

Employ a Risk and Outcome-Based Approach. Privacy and security regulatory requirements must promote technology neutral risk-based solutions that encourage accountability, innovation, and efficiency. The Coalition supports the development of reasonable, risk-based, fairly applied federal privacy regulations where robust security principles are included as a necessary and integrated part of the solution. The Coalition recommends NTIA promote adoption of flexible, consensus-based frameworks like those developed by NIST to accomplish this goal.

---

[2] Recital 47 of GDPR states: "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."

Recital 49 of GDPR states: "The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. "This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopped 'denial of service' attacks and damage to computer and electronic communication systems."

[3] See Cal. Civ. Code 1798.105(d)(2).

The Coalition urges NTIA to consider how organizations using such frameworks can satisfy reasonable privacy and security obligations, and thereby be afforded liability protection.

The GDPR provides a recent example of incorporating security frameworks and guidelines into privacy requirements.[4] Applied in the context of a U.S. approach to privacy, promoting adoption of codes of conduct and certification mechanisms (such as adherence to the NIST Cybersecurity Framework or other consensus- and standards-based best practices) can incentivize a flexible and risk-based approach, rather than prescribing rigid security requirements that can be ill-suited to some technologies and unduly burdensome to smaller organizations.

Standards development. Privacy outcomes are achievable in part through practices and technologies aimed at securing personal information and other sensitive data at each stage. However, awareness, adoption, and proper implementation for organizations' unique needs and environments are fundamental to the effective prevention of theft, loss, or misuse of personal information. The federal government has valuable roles to play in raising awareness and facilitating standards development, and the Coalition recommends incorporating this role into the federal action plan.

* * *

The Coalition appreciates the opportunity to submit these comments, and looks forward to continued collaboration with NTIA as it continues its efforts to advance consumer privacy.

Respectfully Submitted,

The Cybersecurity Coalition

November 9, 2018

CC: Ari Schwartz, Venable LLP

[4] Article 32 of GDPR Article 32 requires controllers and processors to implement "…appropriate technical and organizational measures to ensure a level of security appropriate to the risk."

Article 40 of GDPR provides that adherence to an approved code of conduct or an approved certification mechanism may be used to demonstrate compliance with the GDPR's security requirements.