November 9, 2018

VIA EMAIL: privacyrfc2018@ntia.doc.gov

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

**Re: McAfee's comments in response to NTIA's Request for Comments on "*Developing the Administration's Approach to Consumer Privacy,*" Docket No. 180821780–8780–01**

McAfee LLC appreciates the opportunity to respond to the National Telecommunications and Information Administration's (NTIA) request for comments on *Developing the Administration's Approach to Consumer Privacy,* posted on September 26, 2018.

McAfee is one of the world's leading independent cybersecurity companies focused on accelerating ubiquitous protection against security risks for consumers, businesses and governments worldwide. Inspired by the power of working together, McAfee creates cybersecurity solutions that make the world a safer place. For consumers, we help secure their digital lifestyle at home and away. For businesses, our holistic, automated open security platform allows disparate products to co-exist, communicate and share threat intelligence with each other across the digital landscape. We enable the convergence of machine automation with human intelligence so our customers can streamline workflows more efficiently, be freed from operational burdens and be empowered to strategically combat threats from adversaries.

## *Our Comments*

### A Strong Advocate of Consumer Privacy and Data Security

Individuals and corporations must be able to trust technology for it to be effective. We believe that trust in the integrity of systems – whether a corporate firewall or a child's cell phone – is essential to getting the most value out of their technologies. McAfee is committed to enabling the protection of customer, consumer and employee data by providing robust security solutions.

The General Data Protection Regulation (GDPR), the E.U. Network and Information Security Directive, the California Consumer Protection Act and other new laws from countries around the world are making compliance with privacy and security regulations an important part of bringing

security products to market. Our customers are subject to many of these laws, making it imperative that we know what data our products collect, how they process and secure that data and what options are available for customers to delete or correct data.

McAfee's privacy notices are posted on our website and describe our approach to protecting data privacy and ensuring security. We work to remove artificial barriers, and promote innovation and continued success of businesses by fostering trust in the use of technology and in the responsible and protected collection and processing of data. We use a combination of policy, standards, procedures and guidelines to drive the effective management of personally identifiable information in the operational business processes and development of products and services, enabling customers, consumers and employees to trust digital devices.

**Why Privacy and Security Matter to McAfee**

At McAfee, we put the customer at the core of everything we do. Protecting our customers' data is an essential component of this value. Our products support the protection of personal data (including the data of our customers' customers and their employees) and our customers' intellectual property. The following principles inform our product portfolio and internal infrastructure:

- Robust privacy and security solutions are fundamental to McAfee's strategic vision, products, services and technology solutions.
- Privacy and security solutions enable our corporate and government customers to more efficiently and effectively comply with applicable regulatory requirements.

**Privacy and Security by Design and Default**

"Privacy and Security by Design and Default" requires companies to proactively consider privacy and security when developing products and services for the marketplace, as well as when implementing internal tools; it also means protecting data through proactive technology design. This proactive approach 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. McAfee believes Privacy and Security by Design and Default encourages accountability in the development of technologies, making certain that privacy and security are included as foundational components of the product and service development process.

**Internal Software Development**

Many corporate information technology, network and infrastructure staff develop specific applications, middleware or integration components for specific corporate needs. These

development efforts are often "quick and dirty," meant to solve a specific integration or a short term "gap." The software created is often meant for short-term use but ends up in production environments, making the organization's infrastructure much more vulnerable to attack, and potentially exposing customer, consumer and employee data. It is critical for organizations to consider privacy and security while internal tools are being developed. These types of tools are often not appropriately identified, documented and understood, and are often overlooked. Internally developed tools need to have just as many privacy and security reviews and focus as vendor-developed tools, and in many cases, more.

**Processing Threat Data**

Along with its colleagues in the cybersecurity industry, McAfee processes 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 protect customers from cybersecurity attacks and support them in meeting their privacy compliance obligations. The ability to gain operational insight into attack vectors, through the appropriate and responsible use of data, also enables the cybersecurity industry to continue to bring innovative solutions to market that increasingly drive the ability to detect and defeat "zero day" attacks (attacks that have zero days between the time a vulnerability is discovered and the initial attack).

**Device to Cloud Concerns**

As more digital devices are connected to the internet, there is an increased need for data and applications to be shared among devices and stored remotely, including in the cloud, with augmented focus on the balance of performance, power management and security. The move from device to cloud adds additional complexity to the data landscape and subsequent complexity to the threat landscape, multiplying the number of possible threat vectors. For there to be appropriate protections for this data, there will need to be an increased focus on the security of networks, the gaps between and among cloud providers, and individual endpoint devices. As more devices are connected to the internet, carefully selected device information (e.g., IP addresses) will need to be processed to provide device security. It is important that this processing of device information is recognized as a necessary mechanism for protecting privacy by better securing the data.

**Privacy and Security Policy Recommendations**

McAfee believes clear privacy and security expectations and regulations are necessary prerequisites for companies to comply with laws, grow businesses and improve efficiencies, and also for consumers to trust technology. Effective privacy laws should include capable data security and enable technology neutral security solutions. Additional tenants of ours include:

- McAfee is a strong believer in and advocates for proactive Privacy and Security by Design and Default to provide the most effective end-to-end privacy and security technology solutions.
- Effective cybersecurity solutions require an integrated approach to privacy and data security, recognizing that there is a balance between the need to collect data to secure infrastructure but also to provide for the privacy of the individual.
- Regulatory policies must promote interoperability and data sharing to enable effective threat analysis.
- Privacy and security regulatory requirements must promote technology-neutral, risk-based solutions that encourage accountability, innovation and efficiency.
- Processing of device information (e.g., IP addresses) is necessary to connect to the internet and provide reasonable security for personal data.

McAfee 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. Organizations should be incentivized to implement end-to-end security programs and solutions with liability protections where reasonable standards are met.

We believe that a U.S. federal privacy law should provide:

- A technology-neutral approach for effective, risk-based and flexible privacy and data security strategies to protect personal information.
- Minimum procedural standards for breach notification (e.g., definition of a breach, clear standards for who must be notified and how, etc.).
- A flexible framework similar to the NIST Cybersecurity Framework, which provides guidance on how to develop and implement realistic operational models to meet its objectives. McAfee supports and is participating in the development of the NIST Privacy Framework based on the broad success of the NIST Cybersecurity Framework. We believe that a privacy framework should address best practices in privacy while being compatible with and supporting an organization's ability to operate under the various domestic and international legal or regulatory regimes. The privacy framework should not be focused on the specific legal aspects of privacy, but rather on what organizations need to consider in developing and continually improving their own privacy programs in support of regulations and customer promises.
- A safe harbor for encrypted data and other well-defined cybersecurity protections. The ideal law would encourage good corporate behavior and reward those companies that protect data in accordance with recognized industry standards such as the NIST Cybersecurity Framework and the emerging NIST Privacy Framework.

- Clarity and uniformity on the penalties, and the administration of those penalties, for not implementing reasonable security and privacy measures as outlined within the applicable laws.
- A legal structure that recognizes that compliance burdens can be disproportionately difficult for small companies and startups and supports the growth of new businesses and technologies by focusing on risk-based, accessible solutions to reasonably protect data.

Requirements for federal preemption of state law must be carefully considered so that they do not stifle innovation or arbitrarily provide weaker protections to those in states with strong breach and data protection laws. While eliminating the patchwork of existing laws will provide the benefit of uniformity, this goal should not be accomplished by lessening existing strong and effective state laws that have achieved broad-based support from policy makers, privacy advocates and industry.

## Summary

Effective consumer privacy policies and regulations are critical to the continued growth of the U.S. economy, the internet and the many innovative and life-improving technologies that rely on consumer personal data. The development of a comprehensive federal privacy regulatory framework is an important step toward increasing consumer privacy and trust.
However, federal privacy regulations must also include robust and clear data protection and cybersecurity frameworks to truly enable effective consumer privacy protection. The creation of a federal privacy regulatory framework should not weaken robust privacy protection currently provided by strong and effective state privacy laws that have achieved broad-based consensus among a wide array of stakeholders.

NTIA has an important role to play in the administration's efforts to improve consumer privacy. McAfee would like to sincerely thank NTIA for the opportunity to comment on this issue and looks forward to continued engagement on this and other topics.