Via Electronic Submission to privacyrfc2018@ntia.doc.gov

November 9, 2018

Mr. David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Attention: Privacy RFC
Washington, D.C. 20230

Re: Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780–8780–01

Dear Mr. Redl:

Attached please find the response of Zebra Technologies Corporation to the Request for Comments regarding "Developing the Administration's Approach to Consumer Privacy" (Docket No. 180821780–8780–01). For purposes of this response, the following information is provided:

- Filing Organization: Zebra Technologies Corporation
- Contact Person: Cristen L. Kogl, Senior Vice President & General Counsel
- Contact Person Email: ckogl@zebra.com
- Contact Person Telephone: (847) 793-5512

Thank you for your assistance in submitting these comments. Please contact me at (202) 256-4953 or at krichardson@heartlandsolutionsgroup.com should you have any questions.

Sincerely,

Kevin C. Richardson
Outside Counsel on Government Affairs

Attachment

Comments of Zebra Technologies Corporation
In Response To

National Telecommunications and Information Administration
Request for Comments on

"Developing the Administration's Approach to Consumer Privacy"

Docket No. Docket No. 180821780–8780–01
83 Fed Reg. 48600 (September 26, 2018)
RIN 0660–XC043
privacyrfc2018@ntia.doc.gov

Submitted By:
Cristen L. Kogl
Senior Vice President & General Counsel
ckogl@zebra.com
(847) 793-5512

November 9, 2018

Introduction

Zebra Technologies Corporation ("Zebra") is pleased to provide its views in response to the National Telecommunications and Information Administration (NTIA) Request for Comments (RFC) on the question of advancing consumer privacy while protecting prosperity and innovation.

These views reflect Zebra's position as a global leader in bringing enterprise Internet of Things (IoT) solutions to Business-to-Business (B2B) and Business-to-Government (B2G) markets. With annual revenues of more than $3.7 billion and 7,000 employees in more than 40 countries, Zebra is a trusted business partner that serves more than 95 percent of all Fortune 500 companies. Overall, Zebra's customers gain a performance edge through the use of its scanners, mobile computers, tablets, and printers. Zebra solutions move beyond the barcode and label to give customers actionable insights into the data that flows through their operations.

Of note relative to the purpose of the NTIA's RFC, Zebra leads the growing category known as Enterprise Asset Intelligence (EAI) which describes the ability of businesses, government agencies and other organizations to track critical assets within their operations and know exactly what they are, where they are and their condition so that smarter, faster decisions can be made to improve performance and bottom line operating results. EAI leverages and recognizes the fact that people,

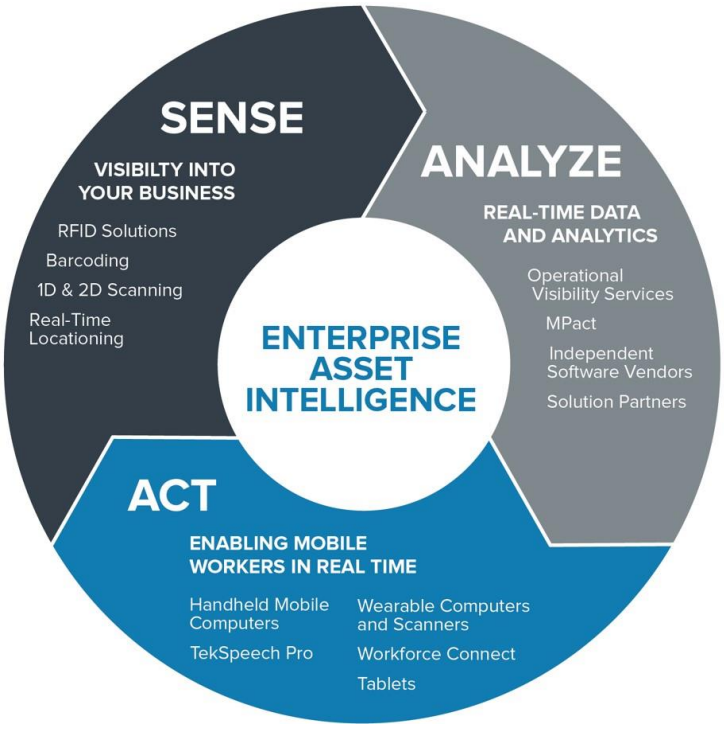
assets, and devices – especially mobile devices – are becoming increasingly connected and that this trend is advancing at an exponential rate.

As a result, Zebra is working with companies, government and other organizations to provide solutions that yield real-time visibility into processes, assets, and people. The key elements which enable this work include:

- **Sense**. The employment of unrivaled expertise in sensor and device connectivity enables businesses, government, and other enterprises to inter-connect devices to software and to mobile workers so that decision makers and workers alike have substantially more real-time visibility into operations.

- **Analyze.** Equally important, the access to the unprecedented amount of data that EAI enables allows companies, government, and organizations to plan more effective short and long-term strategies by delivering real-time insights into the critical data captured by the sensors in connected devices.

- **Act.** The explosive growth of mobile devices across the private, public and non-profit sectors enables management and workers at all levels to act on these visibility-driven insights in real-time.



Zebra recognizes that data is the lifeblood of private and public-sector enterprise effectiveness and that it is essential to success in the 21st century. Zebra devices and solutions empower those on the front line in retail, healthcare, transportation and logistics, manufacturing, government, hospitality, and variety of other sectors to achieve a performance edge that translates into delighted customers and taxpayers as well into superior operating performance.

Overview

As the global leader in enterprise asset intelligent solutions, Zebra understands that while each business and government market segment is unique, they share a similar need for real-time data exchange to drive enhanced performance and operating outcomes. Zebra printers, handhelds, labels, scanners, and other products and solutions enable retail, transportation and logistics, manufacturing, healthcare, government, and other enterprises to better serve their customers, and constituents.

For example, manufacturers are adopting Industry 4.0 in which cyber-physical systems create "smart factories" where workers use a combination of RFID, wearables, automated systems, and other emerging technologies to monitor the physical processes of the plant and enable companies to make faster and more decentralized decisions.[1] With this comes instant access to operations data and the ability to ensure that production processes operates ever more efficiently. Importantly, real-time access to data gives manufacturers the ability to anticipate the emerging needs of their customers. It also enables manufacturers to keep less inventory on hand and eliminate points-of-failure. To this point, fifty percent (50%) of the respondents to Zebra's 2017 Manufacturing Vision Study stated that improving their ability to adjust to fluctuating market demands is a top business growth strategy.[2]

In Zebra's view, both manufacturers and the overall U.S. economy are already realizing the very real benefits of data connectivity through such things as:

- Increased visibility into the entire manufacturing process.
- Implementing state of the art safety practices.
- Faster identification of points-of-failure.
- Improving the ability to adjust to fluctuating market demand.
- Increasing the number of product variants.
- Decreasing the cost of production.
- An accelerated pace in shipping and receiving.

Beyond manufacturing, a variety of other private and public sector enterprises benefit from access to real-time employee and business data, including retail, transportation and logistics, manufacturing, healthcare, and government. In all of them, the reality is the same – data that is specific to a worker acting within both the scope of his or her job function and within his or her defined work environment must be differentiated from consumer data in order to preserve and enhance both the workplace safety and overall innovation and global competitiveness benefits that result from an enterprise properly using employee data. Allowing public and private sector enterprises to leverage the employee-generated data that is captured, stored, and transmitted in enterprise settings is essential to achieving the insights that makes data actionable.

---

1 Source: Bernard Marr, *What Everyone Must Know About Industry 4.0*, Forbes Magazine, June 20, 2016, https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#1f25bf89795f.

2 Source: Zebra Technologies Corporation, *2017 Manufacturing Vision Study*, July 31, 2017, https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/vertical-solutions/manufacturing/white-papers/2017-manufacturing-vision-study-en-emea.pdf.

Consumer Privacy Principles

As a global leader in enterprise asset intelligence, Zebra is committed to ensuring that private and public sector customers succeed in protecting consumer data integrity through a combination of strong privacy policies and innovative enterprise technologies which respect and work to protect an individual consumer's personal, family or household information. By way of example, Zebra barcodes and other technologies are integral to maintaining privacy as they provide for the obfuscation of personal data that may be associated with a consumer, patient, or specimen.

Zebra commends the NTIA for its effort to work with stakeholders in establishing outcomes-based principles that protect consumer privacy while enabling enterprise users in business and government to access and utilize their own data for legitimate operational purposes. Among the issues of importance that Zebra urges NTIA to consider are:

- Employ A Risk-Based, Outcome-Oriented Approach. The nature and essence of data varies. Personal information, sensitive information, aggregated information, de-identified information, and pseudonymized information each carry different levels of risk if breached or used for improper and unauthorized purposes. Applying a cybersecurity risk-based approach to privacy policy is reasonable, warranted, and can help clarify requirements for varying data sets.

  For example, B2B solutions utilize data from devices operated by employees that capture nuanced data elements for enabling Industry 4.0, asset management, and enhanced customer experiences. In Zebra's view, such data elements must be considered in context. The application of overly restrictive privacy requirements on data that, if exposed, would not lead to a particular harm lacks fundamental fairness and dilutes the full allocation of resources to protecting the kinds of data sets that the public rightly demands protection and safeguard for while needlessly jeopardizing the tremendous benefits to both the overall economy and to worker safety that arise from the proper and prudent use of employee data. Any regulation that gives individuals an unrestricted "right to be forgotten" from business records not only imposes an unfair and impractical burden on enterprises of all types but also eliminates data that is vital to making workplaces safer and operations more competitive.

- Harmonize With The International Regulatory Landscape. Consistency across world-wide regulatory jurisdictions is critical to providing clarity and certainty, especially for U.S. companies which operate globally. Harmonization with the European Union's (EU) General Data Protection Regulations (GDPR) is important in helping assure that compliance is made more effective on a global basis. However, the harmonization process must recognize that many global companies have open questions and policy concerns with GDPR and that GDPR should not necessarily serve as a model for the United States in developing its own privacy policies.

  For example, a challenge with GDPR and the proposed EU e-Privacy Regulation is whether work email addresses and/or other information that can identify an individual employee and which relates to the individual's employment should be considered within scope relative to a

policy intended to protect *consumers*.[3] Information concerning employees (and which relates to their work and is conducted within their role as employees) is properly deemed as separate from and out of scope relative to *consumer* privacy policies regardless of whether such data is "capable" of identifying an individual.

- Enhance Domestic U.S. Privacy Via Federal Preemption. Similarly, the Administration and Congress should collaborate in passing legislation which creates a single federal standard for consumer privacy so as to avoid an unwarranted burden upon legitimate interstate commerce. Preemption will allow compliance efforts to be more fully devoted to providing a robust set of privacy protections, choices, and controls while avoiding a needless misdirection of resources into the far less valuable work of navigating a patchwork of divergent state laws and regulatory regimes. California, Colorado, Illinois, and other states have already advanced potentially conflicting privacy laws and others may soon follow and create significant operational uncertainties that will stifle innovation and growth. This is especially true in an era where data moves seamlessly and instantly across domestic and international borders.

- Increase Resources for Federal Trade Commission Enforcement. Similarly, any new policy should assure that the Federal Trade Commission (FTC) has needed enforcement authority except in instances where sector-specific laws – such as the Health Insurance Portability and Accountability Act (HIPPA) and Gramm Leach Bliley (GLB) – already exist and apply.

- Safe Harbor. In Zebra's view, one of the most effective ways government can foster compliance with any new privacy policy or standard is through the creation of clear safe harbors. The FTC should establish a self-regulatory privacy safe harbor program similar to that used to certify compliance under the Children's Online Privacy Protection Act (COPPA). The FTC should also establish appropriate guidelines so that enterprises can self-certify adherence. Further, the FTC could also outsource this responsibility in a manner similar to the COPPA Safe Harbor program. Additionally, regulations should encourage the development of best practices through a process of public and private collaboration.

- Risk of Overreach. Zebra urges NTIA to consider a light regulatory touch when making policy in this area and make a critical distinction between:

    - Employee and enterprise-related business data, and
    - Consumer data.

  In an employment setting, it is reasonable to expect that the employer will both control the selection of the type of device used by an employee in the discharge of his or her duties and that any business data collected by the employee with that device in the course of his or her job is not fairly considered "personal" information. Data sets that are employment-focused must remain accessible as part of business operations. Like the work-for-hire doctrine under copyright law, the data generated by employees needs to be acknowledged as being owned by

[3] Source: European Commission: *Proposal for a Regulation on Privacy and Electronic Communications*, January, 2017, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

the enterprise employing an individual worker and excluded from obligations delete or "forget" such business records. Certainly, an employee's sensitive personal data disclosed to

Human Resources can still be protected without creating the unintended consequence of imposing restrictive retention and destruction obligations on operations-related business data that is associated with an individual employee.

- Strong, Secure Identities and Identity Credentials Enhance Privacy. NTIA should encourage further use of innovative technologies and systems to further enhance and strengthen consumer privacy. Technology solutions that are privacy-enhancing for consumers include biometrics, blockchain, mobile device authentication and smart cards. Encouraging deployment of privacy enhancing technologies strengthens the entire privacy eco-system and enhances consumer consent.

- Device Selection. Similar to using strong, secure identities and identity credentials to enhance privacy, the importance of device selection in protecting both personal/consumer and employee/business data is a critical issue and one with which Zebra has significant familiarity. Indeed, experience shows that a growing part of addressing cybersecurity and data privacy protection begins with the selection of a mobile computing device. The three options in mobile device selections that are available today include:

    - Enterprise Devices – both private and public-sector enterprises can choose enterprise handheld mobile computers that are purpose-built for specific environments and use cases.

    - Consumer Devices – both private and public-sector enterprises can choose consumer devices, such as smartphones or consumer tablets.

    - "Bring Your Own Device (BYOD)" – both private and public-sector enterprises can permit their employees to use their own individual consumer smartphones or other mobile devices.

  Enterprise-class devices, such as the enterprise mobile computing devices manufactured by companies like Zebra, are designed to provide required levels of security while typical consumer-class devices can typically fall short. An enterprise's choice to encourage a Bring Your Own Device (BYOD) program or to use consumer-grade technology may well require an enterprise to develop a plan to commit additional resources for security. For example, an enterprise may develop in-house security solutions as consumer-grade mobile operating systems (OS) do not provide required levels of security. Enterprise-grade devices such as those manufactured by Zebra are designed to operate within secure network architectures and are typically deployed by knowledgeable system administrators.

  Overall, studies show that the total cost of ownership (TCO) of using consumer-grade devices for enterprise applications can be between 40% and 78% higher than purpose-built enterprise

devices.[4] Security is an important element in this differential as consumer devices used in enterprise applications often lead to a security breach. In one BYOD study by *Decisive Analytics*[5], nearly half (46.5%) of the companies surveyed reported a data or security breach as a result of an employee-owned device accessing the corporate network. While significant investments are being made to counter this threat, there are no guarantees that these security workarounds will continue to be effective against emerging threats.

In contrast, purpose-built enterprise devices are designed and augmented to satisfy and simplify compliance with key regulatory mandates on security. The scope of security compliance can range from the very broad (e.g., user training) to the very detailed (e.g., validation of the integrity of cryptographic algorithms).

Similarly, multipurpose operating systems and applications can create multiple pathways for cyber criminals to exploit. The lifecycles of consumer operating systems typically do not last longer than 36 months – often well short of the 5+ years of service many enterprises require. A gap between OS and hardware lifecycles can create exposure to a growing number of security risks.

In addition, most enterprises do not have visibility into when vendors will release OS security patches and that can create uncertainty as well as potential – and significant - security issues. If no formal patch policies are in place, a multitude of possible problems can arise.

In sum, policy decisions relative to what data should be protected *by law* and to what degree must also consider the equally important question of how *data of all types* can and should be best protected. U.S. privacy law should support the development of best practices and such best practices should include device selection as a critical element in protecting data.

- Additional Data Security Considerations. Protecting and securing data – whether consumer data or completely separate employee data – from unauthorized access, destruction, disclosure, use, and modification is reasonably expected by the public and those entities which collect, store, transport, and use data must assure the public that appropriate security measures are in place in a manner commensurate with the level of risk associated with the data. Providing this assurance raises two questions: (1) What data requires what level of protection, and (2) How can any data of any type be securely captured, stored, and transmitted from a device that is being used by a worker operating at the edge of any enterprise's operations?

---

[4] Source: Zebra Technologies Corporation: *Establishing A Robust Mobile Security Policy: The Key Risks And How Enterprises Can Avoid Them*, October 18, 2017, https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/product/Software/Mobility%20Software/lifeguard-for-android/white-paper/lifeguard-for-android-security-white-paper.pdf, citing "Total Cost of Ownership Models – Enterprise and Government Mobility Applications" (Slide 13), VDC Research, Josh Martin, David Krebs (2009); "A 3 Year Cost Comparison of Consumer-grade vs. Durable Smart Devices", Jack Gold, Gold Associates.

[5] Source: Zebra Technologies Corporation: *Establishing A Robust Mobile Security Policy: The Key Risks And How Enterprises Can Avoid Them*, October 18, 2017, https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/product/Software/Mobility%20Software/lifeguard-for-android/white-paper/lifeguard-for-android-security-white-paper.pdf, citing "Mobile Consumerization Trends & Perceptions, IT Executive and CEO Survey Final Report", Prepared for Trend Micro, Inc. by Decisive Analytics, LLC (2012).

In Zebra's experience, data security is a key consideration when selecting a device for employees in any private or public-sector enterprise as any such employees often transmit sensitive, personal, medical, and otherwise confidential data and images over a Wi-Fi or a cellular network. Key considerations here include:

- Over-the-air transmissions are referred to as Data-In-Motion (DIM). The best solution must consider the possibility that a device that may fall into the wrong hands, or be lost or stolen.

- Data on the device is referred to as Data at Rest (DAR) and it, too, must remain secure and encrypted, ideally through means of a cryptographic module on the device itself.

Enterprise-class mobile devices can be remotely tracked, locked, and "wiped" clean in case device is lost, stolen or when a user is terminated abruptly. Moreover, consumer privacy can be further enhanced when private and public-sector enterprises opts for the use of enterprise-class mobile computing devices for data capture, storage, and transmission as such enterprise devices can be purpose-built to comply with FIPS (Federal Information Processing Standard) level security. Often referred to as FIPS 140-2 level security, this is the data encryption standard mandated by a number of federal agencies, including:

- The Federal Bureau of Investigation (FBI) relative to the protection of confidential law enforcement data.

- The U.S. Department of Health and Human Services (HHS) relative to the protection of personal and medical records information (as required by the Health Insurance Portability and Accountability Act (HIPPA), which addresses the security and privacy of personal, health, and medical records data).

- The Department of Defense (DoD).

Care must be taken to make sure that appropriate security includes *device level* security such as FIPS 140-2. Indeed, as cybersecurity vulnerabilities become a more urgent concern for agencies at all levels of government, FIPS 140-2 validation is increasingly important. FIPS 140-2 is required when selling to federal agencies and encryption requirements at the device level are seen as key tools in addressing and assuring device cybersecurity concerns.

Conclusion

Zebra appreciate the opportunity to present its views on this important topic and looks forward to working with NTIA as it develops the Administration's approach to consumer privacy. Inconsistency with respect to consumer privacy laws across jurisdictions can create a needlessly complicated regulatory environment that undermines the significant economic benefits that result from reasonable and proper access to employee and business data. Data associated with employees and work done in an employment setting should be treated as separate from that which is designated as consumer data. Protection of consumer data is best achieved through a combination of a strong federal privacy standard and innovative enterprise device technologies.