November 09, 2018

Mr. Travis Hall
Telecommunications Policy Analyst
National Telecommunications and Information Administration
U.S. Department of Commerce
Washington, DC 20230

RE: NTIA Request for Public Comments on Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01

Dear Mr. Hall,

The Information Technology Industry Council (ITI) welcomes the opportunity to comment on the National Telecommunications and Information Administration's (NTIA) request for public comment (RFC) on Developing the Administration's Approach to Consumer Privacy.

ITI is the premier voice, advocate, and thought leader for the global information and communication technology (ICT) industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI member companies are leading internet services and e-commerce companies, wireless and fixed network equipment manufacturers and suppliers, computer hardware and software companies, and consumer technology and electronics providers.

ITI is encouraged by NTIA's RFC which aims to develop legislative and regulatory frameworks to protect and responsibly use personal information, encourage domestic innovation, attract foreign investment, promote the growth of trade, and facilitate the free flow of information.

Consumer trust is a key pillar of innovation, and our industry must do everything it can to deepen that trust and meet our customers' expectations when it comes to protecting their privacy and personal data. NTIA's RFC is a first step toward that goal by recognizing the importance of enhancing transparency, increasing individual control, establishing company accountability, promoting security, and fostering innovation. To that end, we offer the following comments in response to the various questions raised in the RFC.

A. Core Privacy Outcomes and B. High-Level Goals for Federal Action[1]

Through its RFC, NTIA seeks feedback on what it believes are the core privacy outcomes that consumers should expect from organizations and the high level goals for federal action. We support the key outcomes and end goals identified by NTIA and would like to additionally share our thinking on the outcomes and goals we believe form a key part of a meaningful privacy framework.

[1] Corresponding to questions under Part A and B of Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018

ITI and its member companies developed over the course of several months a document entitled "Framework to Advance Interoperable Rules (FAIR) on Privacy" (FAIR on Privacy), a roadmap toward the goal of protecting individuals. We anticipate this work will continue to take shape as we work alongside consumer advocates, lawmakers, industry partners, and other key stakeholders to advance meaningful federal privacy legislation in the Unites States.

In line with the goals identified in NTIA's RFC, FAIR on Privacy sets forth specific ideas that advance the privacy rights of individuals and makes explicit the responsibilities of companies in using personal data while continuing to deliver the innovative products and services consumers and businesses demand. Adoption of elements of the framework will give consumers more control and a clear understanding of their choices regarding the use of their personal data. It also clearly defines an entity's responsibilities, so they can be held accountable, thereby ensuring companies use personal data responsibly and transparently -- key outcomes and goals identified in the RFC.

The concepts built into the framework are intended to work the way people live their lives and use technology -- by providing both meaningful privacy protections and value for consumers regardless of the state in which they live. We summarize the framework below and then attach it for your reference, as it clearly expresses our thinking with regards to the various questions raised in the RFC.

Building on the strengths of other global approaches and principles, FAIR on Privacy aims to:

- **Enhance transparency**
- **Increase consumer control**
- **Establish accountability and responsibility**
- **Promote security and manage privacy risk**

Enhance Transparency

The framework recommends that individuals should be informed of the collection and use of their personal data in a way that is meaningful, clear, obvious, and useful so they have a better understanding of what they are (or are not) consenting to with respect to their personal data. This includes being informed of the categories of companies (including third parties) who collect their personal data and how they use it. We also offer the contours of definitions of "personal data" and "sensitive personal data." "Personal data" is any data that is reasonably linkable to or associated with, either directly or indirectly, a specific natural individual. "Sensitive personal data" is personal data consisting of ethnic origin, political affiliation, religious or philosophical belief, trade union membership, genetic data, biometric data, health data, sexual orientation, certain data of known minors, and precise geolocation data. We believe this builds on the position outlined by NTIA in the RFC but further elaborates the specific commitments that companies should be required to make to enhance transparency and create "informed consumers."

Increase Consumer Control

We agree with NTIA that one of the chief goals of a privacy framework should be to give users control of their personal information while also avoiding process-heavy approaches that challenge the equal and vibrant participation of small- and medium-sized enterprises. We believe the way to achieve this is

through a model that balances the various interests at play while being uncompromising in the protection afforded to individuals. FAIR on Privacy recognizes that individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, and to be able to access, correct, port, delete, and object to the use of their personal data where it is appropriate to the context of the use of such personal data. Privacy legislation should account for people's contextual expectations about how their information will be used in a given situation. Specifically, the law should recognize that people's expectations change based on the context in which information is provided and their relationship with the company that holds their data. We believe the context consideration is a critical one and provides alternatives to onerous process requirements that degrade user experience while retaining the flexibility to offer individuals robust protection where it is most required.

Establish Company Responsibility and Accountability

Our framework fleshes out in detail the responsibilities organizations should have when using personal data, a key question NTIA has identified in the RFC. As articulated in FAIR on Privacy, companies should be required to identify, monitor, and document uses of known personal data, and ensure all uses are responsible and permissible under the law. Companies transferring personal data to a third party that acts as service provider are further required to perform due diligence to ensure the data is protected by the third party. This includes ensuring that the third party employs appropriate controls, contractually binding the third party to assist in upholding the companies' legal responsibilities and requiring the third party to notify the company if it can no longer meet such obligations. We are aligned with NTIA that accountability and responsible use are the foundations of a meaningful privacy framework and have fleshed these concepts out accordingly in FAIR on Privacy.

We believe critical to any privacy framework are clear mechanisms for regulators to hold companies responsible for their data practices. We support the adoption of federal privacy legislation in the United States that is aligned with FAIR on Privacy and that provides regulators with first time penalty authority. We also support additional technical capacity and resources for the responsible oversight body, such as the Federal Trade Commission, as necessary to regulate and carry out enforcement actions against bad actors effectively.

Promote Security and Manage Risk

There can be no privacy without security. We appreciate NTIA highlighting the importance of security measures to ensure a privacy framework is effective. FAIR on Privacy explicitly recommends that companies be required to implement comprehensive security programs that can support and protect a company's operations, activities, and information. Similar to what NTIA has alluded to in the RFC, our framework recommends that companies comprehensively identify, assess, and monitor the privacy risk to individuals relating to the use of personal data, and take reasonable steps to mitigate these risks. In doing so, companies should balance the possible benefits of the personal data use to individuals, other stakeholders, and society at large.

Please see attached, ITI's FAIR on Privacy for additional details.

C. Next Steps[2]

We believe consumers are better off when there is a uniform and consistent set of privacy protections; we therefore support legislation offering federal preemption. Consumers use technology seamlessly across borders every day and our laws should work the same way. NTIA and the administration should proceed with this aim in mind.

FAIR on Privacy outlines clear responsibilities that, if adopted and enacted into federal law, regulators can hold our member companies accountable for, including through the imposition of financial penalties. The enactment of a federal law would mean companies would be subject to hefty civil penalties for first time violations of the law. Acknowledging that, it is important that any future privacy law strikes a balance between the various relevant public interests at play. Our industry has an important role to play as discussions regarding US federal privacy legislation move forward and can provide expertise in developing an actionable and workable set of solutions. We appreciate NTIA's approach so far and hope to continue to engage in this process going forth.

We thank NTIA for seeking comments from stakeholders on next steps and measures the administration should take to effectuate the previously discussed user-centric privacy outcomes, and to achieve an end-state in line with the high-level goals.

We support NTIA convening stakeholders to further explore additional commercial-data privacy-related issues, particularly with the aim of building out and defining the concepts of context and privacy risk as referred to in our comments and FAIR on Privacy. We also hope to see NTIA coordinate its efforts with NIST as it embarks on a process to create best practices for privacy risk assessment, management, and response.

D. Definitions[3]

The foundational elements of any privacy policy framework are the definitions of "personal data" and "sensitive personal data." We define these, and other terms in FAIR on Privacy and would like to put forth the same definitions here for NTIA's consideration. We define "personal data" as any data that is reasonably linkable to or associated with, either directly or indirectly, a specific natural individual. "Sensitive personal data" is personal data consisting of ethnic origin, political affiliation, religious or philosophical belief, trade union membership, genetic data, biometric data, health data, sexual orientation, certain data of known minors, and precise geolocation data. Data that is anonymized, pseudonymized and protected, or otherwise publicly available is not personal data. Publicly available data means information that is lawfully made available in federal, state, or local government records, or that is lawfully made available to the general public.

We appreciate that defining some aspects of any privacy framework will necessitate regulatory rulemaking. Context is an area that is ripe for such rulemaking to ensure consideration of the factors

[2] Corresponding to questions from Part C of Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018

[3] Corresponding to questions under Part D of Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018

identified in FAIR on Privacy as well as others that may be relevant (e.g., factors related to public safety). Identification and classification of privacy risk factors would also benefit from further collaborative development and guidance by all relevant stakeholders. We are supportive of NIST in its initiation of such a collaborative process to develop a privacy risk management framework to provide a catalog of privacy outcomes and approaches for all categories of entities to: better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services.

E. Role of the Federal Trade Commission (FTC)[4]

One of the high-level end-state goals identified in the RFC is for the FTC to continue as the Federal consumer privacy enforcement agency, outside of sectoral exceptions beyond the FTC's jurisdiction. In order to achieve the goals laid out in this RFC, and as suggested in FAIR on Privacy, companies should maintain records pertaining to risk assessments and security programs so that they are auditable by the designated authority in the event of an incident. We believe the FTC is well suited to fill this role, and we support the allocation of sufficient resources and rulemaking authority to the FTC so it has the technical capacity and ability to ensure robust enforcement of these principles. Given its long-standing experience in this area the FTC would also be the ideal body to provide individuals with redress mechanisms, such as complaint handling and resolution procedures, to ensure their rights are adequately protected.

F. Global Interoperability and G. U.S. Leadership[5]

We are pleased NTIA recognizes the importance of global collaboration on mechanisms to promote compatibility between regional mechanisms for international transfer, such as the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) and the EU's Binding Corporate Rules. With the EU's General Data Protection Regulation (GDPR) now in effect, the time is ripe to resume this dialogue to identify commonalities between the approaches of the EU and other regions of the world, particularly the Asia-Pacific, by exploring potential interoperability through certifications pursuant to GDPR Article 42 and APEC CBPR. We urge NTIA and the administration to continue to prioritize these efforts and encourage the America's global partners to commit to ongoing dialogue in appropriate official forums related to international transfer mechanisms. We stand ready to support the administration's efforts towards promoting greater interoperability and data flows globally.

We hope our comments will serve as a useful resource and we look forward to working with NTIA and other stakeholders in the administration and beyond to help develop a best-in-class interoperable privacy regime in the US that offers both a model for governments worldwide and a workable alternative to a looming patchwork of laws that will create confusion and uncertainty surrounding individuals' privacy protections, rather than deepening their trust.

---

[4] Corresponding to questions under Part E of Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018

[5] Corresponding to questions under Part G and F of Federal Register / Vol. 83, No. 187 / Wednesday, September 26, 2018

Best Regards,

John Miller
Vice President, Policy and Law
Information Technology Industry Council

Framework to Advance Interoperable Rules (FAIR) on Privacy

1. Purpose

This framework is a robust, technology and business model-neutral approach for the protection of privacy and personal data that advances the interests of all stakeholders, including consumers, businesses, individuals, and governments.[6] The purpose of this framework is to inform the development of legislation or the promulgation of rules that enhance personal data protection, further the trust relationship between companies and their customers, and enable innovation while also avoiding regulatory fragmentation that undermines all three goals. Inspired by the Fair Information Practice Principles (FIPPs), Europe's General Data Protection Regulation (GDPR), and the Asia-Pacific Economic Cooperation's (APEC) Principles and Cross Border Privacy Rules (CBPR), this framework provides recommendations to both protect individuals' privacy and allow society to harness the potential of the digital age.[7]

While building on the strengths of existing global approaches, this framework is grounded in the principles of accountability, context, and mitigation of privacy risk to the individual and offers several key advantages including:

- creating alignment with the privacy protections of other privacy regimes across the globe and enabling interoperability with these global approaches;
- avoiding onerous process requirements that degrade the user experience, inject unnecessary costs into the ecosystem, or otherwise deter continued innovation and the participation of small- and medium-sized enterprises in the digital economy;
- encouraging innovation in and the adoption of security and privacy best practices by recognizing the benefits of techniques and controls that obstruct reidentification; and
- better enabling valuable research and innovation in areas such as machine learning and artificial intelligence that rely on the use of personal and non-personal data.

These elements advance both the rights of individuals and the responsibilities of entities in using personal data while sustaining the innovation necessary to deliver the products and services that consumers and businesses demand.

---

[1] Given existing laws governing the rights of individuals as employees, this framework does not apply in the employment context

[2] In recognition of the need for government agencies and law enforcement or their third-party data processors to use personal data for the prevention, investigation, detection, or prosecution of criminal offenses; the execution of criminal penalties; or for preventing threats to public safety, data protection requirements and derogations for these purposes will need to be considered separately from this framework

2. Defining Personal Data and Sensitive Personal Data

The foundational elements of any privacy policy framework are the definitions of "personal data" and "sensitive personal data." In this framework, "personal data" is any data that is reasonably linkable to or associated with, either directly or indirectly, a specific natural individual. "Sensitive personal data" is personal data consisting of ethnic origin, political affiliation, religious or philosophical belief, trade union membership, genetic data, biometric data, health data, sexual orientation, certain data of known minors, and precise geolocation data. Data that is anonymized, pseudonymized and protected, or otherwise publicly available is not personal data. Publicly available data means information that is lawfully made available in federal, state, or local government records, or that is lawfully made available to the general public.

3. Transparency

Individuals should be informed about the collection and use of their personal data in a fashion that is meaningful, clear, conspicuous, and useful to the individual. Such notices should be informed by state- of-the-art practices on effective disclosure, and include information regarding:

- the types of personal data collected;
- the entity that is collecting their personal data;
- how the personal data will be used;
- how long the personal data will be retained;
- whether and for what purposes personal data may be accessed by or transferred to third parties and the types or categories of third parties to whom such data may be transferred; and
- an explanation of control, choice, and redress mechanisms available to individuals.

4. Individual Control Rights and Context

Individuals should have the right to exercise control over the use of their personal data where reasonable to the context surrounding the use of personal data. These individual control rights, consistent with the rights and legal obligations of other stakeholders, include the right to access, correct, port, delete, consent, and object to the use of personal data about themselves.

Sensitive Data

Individuals should have the right to expressly and affirmatively consent to the use of their sensitive personal data, unless such use is necessary based on the context or otherwise permitted under applicable law.

Access, Objection, Correction, Deletion, and Portability Controls

Subject to the context considerations of the following subsection, where reasonable, individuals should have the right to the following:

- be informed about the categories of companies who are collecting their personal data and how they are using it;
- access in a timely manner personal data collected from them;
- object to the use of their personal data;
- rectify, complete, or delete inaccurate or incomplete personal data;
- have an entity delete their personal data; and
- obtain and port personal data that they provided to the entity across different services.

Enabling Context-Based Individual Control

While individual control mechanisms may differ in design features and deployment, and may also evolve over time, they should always provide individuals with reasonable transparency and the means to exercise the rights laid out above to the extent they are appropriate to the context surrounding the use of that personal data.

Key considerations in determining the appropriate level and means of enabling individuals to exercise control over the use of their personal data in a particular context should include, but are not limited to the:[3]

- extent, frequency, nature, and history of interactions between individuals and an entity, if any, and whether the personal data being used is inferred;
- expectations of reasonable users about how an entity uses their personal data, including through any notice it provided;
- extent to which personal data is exposed to public view;
- extent to which personal data is pseudonymized and the probability and ease of reversing that pseudonymization for any given entity that has access to such data;
- practical difficulty or infeasibility of accessing or deleting data from backup

systems or archives, or segregating the individual's personal data from others in order to enable access;

- benefits to individuals and society of a certain use of personal data;
- types of personal data that need to be used for an entity's customary internal operations;
- age and sophistication of individuals to whom an entity targets or markets its goods or services, including whether it is directed toward minors or the elderly;
- sensitivity of the personal data being used;
- reasonably discernible potential privacy risks of an entity's planned use of personal data;[4]or
- extent to which personal data is processed to protect the vital interest of the individual or necessary for the performance of a task carried out in the interest of public safety, for law enforcement purposes, or in the exercise of the official authority vested in the controller entity.

5. Responsible Uses

For purposes of this framework, the term "use" is defined as all processing, collecting, handling, storing, retaining, disclosing, and transferring of personal data. This use concept is further refined by the entity's relationship to the data. For instance, liability and accountability obligations vary based on the extent to which the entity determines the purposes for and manner of use of the personal data. Where a company does not determine the purposes and manner of use of the personal data but has been contracted to use that data on behalf of another entity, that company acts as a service provider.

Using Data Responsibly

Companies should identify, monitor, and document uses of data they know to be personal and ensure that all identified uses of that personal data are legitimate. When acting as a service provider, companies should only use the personal data provided to them in accordance with the instructions of the entity that provided the data, and to assist that entity in meeting its privacy and security obligations.

Legitimate uses of personal data include those:

- that are appropriate to the context and where the associated privacy risk to individuals is negligible or has been minimized to a reasonable level;
- where the benefits to individuals and other stakeholders outweigh any potentially negative impacts on individuals and other stakeholders and where the associated privacy risk to individuals is negligible or has been minimized to a reasonable level;

- for which individuals have provided informed, freely given, and unambiguous consent;
- that are necessary to provide a requested good or service;
- that are for research and measurement purposes and where the data is protected through appropriate security measures;
- that ensure the efficient operation of devices, networks, and facilities, and where the associated privacy risk to individuals is negligible or has been minimized to a reasonable level; or
- that are for specified public interest uses such as:
    - preventing or detecting fraud;
    - protecting the security of people, devices, networks, and facilities;
    - facilitating the efficient distribution of website and other internet content;
    - protecting the health, safety, rights, or property of the organization or another person;
    - mitigating institutional risk, including using, processing, or sharing of data for the purpose of protecting information systems and the data they store, process, and transport;
    - fulfilling contractual or other legal obligations; or
    - responding in good faith to valid legal process or providing information as otherwise required or authorized by law.

In addition to prohibitions of data use laid out in sectoral privacy laws, the use of data that is not captured by the above list of legitimate uses and where privacy risks cannot be mitigated to a reasonable level based on the context and where individuals have not provided informed consent should be prohibited. Regulatory authorities should be permitted to create specific public interest exemptions to this prohibition.

6. Risk Assessment and Mitigation

Companies should institute technical, contractual, and organizational measures and processes that comprehensively identify, assess, and monitor the privacy risk to individuals relating to the use of personal data, and should take reasonable steps to mitigate these risks. In doing so, companies should take into consideration the possible benefits of the personal data use to individuals, other stakeholders, and society at large. Privacy risk assessments may include reviews of data sources, systems, information flows, partnering entities, and data and analyses to examine the potential for privacy risk.

Companies should mitigate privacy risk to individuals by anonymizing, pseudonymizing where anonymization is not possible, or encrypting personal data whenever possible and appropriate to the context.

7. Security and Minimization

Companies should implement comprehensive security programs that are reasonable and proportionate to the size and complexity of their operations, the nature and scope of their activities, and the sensitivity of the personal information they knowingly use or that is under their control.

Security programs should be designed based upon an organization's risk profile and should include specific protections for an organization's most valuable data, which may include personal data, customer data, or business proprietary data. Security programs should be designed to prevent unauthorized access, use, or disclosure, as well as misuse, alteration, destruction, or other compromise of this data. Companies should regularly assess the sufficiency of any safeguards in place to prepare for reasonably foreseeable internal and external risks.

Companies should ensure that personal data under their control is adequate (sufficient to properly fulfill the stated purpose), relevant (has a rational link to that purpose), limited to what is appropriate in relation to the purposes for which the data is used, and used only for purposes compatible with the context.

8. Disclosure of Personal Data to Service Providers

Companies providing access to or transferring personal data to a service provider should perform due diligence over such entities to ensure they have the appropriate procedures and controls in place to protect personal data. Companies should also require service providers to help them uphold these responsibilities via contractual commitments or other means, such as a recognized and enforceable self- certification program, and require service providers to notify them if they can no longer meet their obligations.

Liability among entities in the event of a breach of privacy or security should be allocated according to contractual agreements or, barring such agreements, according to the demonstrated fault giving rise to the breach event. When a service provider follows the instructions of the entity that provided the personal data, including the use of appropriate technical and organizational measures to ensure privacy and security, the service provider’s responsibility under this framework is limited to meeting the obligations identified in the instructions provided by such entities.

In contrast, when personal data is transferred to another entity for that entity’s own use, where it determines the purposes for and manner of use of such data, that entity is accountable for upholding the responsibilities articulated within this framework.

9. Accountability and Oversight

Companies should maintain records pertaining to risk assessments and security programs so that they are auditable by the designated authority in the event of an incident. The development of technical capacity within the oversight body to ensure robust enforcement of these principles is an important consideration in any privacy regime.

Individuals should have the right to redress mechanisms, such as complaint handling and resolution procedures, that ensure their rights are adequately protected and to be notified in a timely manner if a breach of their personal data triggers a risk of concrete and measurable harm to them or their rights.