November 9, 2018

Mr. David Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW
Room 4725
Attn: Privacy RFC
Washington, DC 20230

RE: Docket No. 180821780-8780-01

Dear Assistant Secretary Redl,

On behalf of Intel Corporation I write to share Intel's answers to questions raised by the National Telecommunications and Information Administration (NTIA) in its Notice regarding Developing the Administration's Approach to Consumer Privacy.

Intel's longstanding commitment to protecting privacy is at the core of the company's values. Our answers to the questions posed by NTIA are influenced directly by that commitment. Our company-wide privacy program is based on the Fair Information Practice Principles (FIPPs), as articulated by the Organization for Economic Cooperation and Development (OECD). While these principles remain as relevant as they were when established 40 years ago, we understand the need to constantly evaluate their application to new technologies and business models. It is a testament to the durability and flexibility of those principles that they continue to be the global common language of privacy. We encourage the Administration to embrace a policy approach that leads companies and not-for-profits to apply the FIPPs to their products, services, and processes that utilize individuals' personal data.

We support the core tenets of the Administration's Approach to Consumer Privacy as it largely tracks the OECD FIPPs, and we highlight in our comments the additional policies that Intel believes must be embraced. In short, individuals and businesses need all eight FIPPs in the digital age. Implementing notice and choice -- two of the FIPPs -- across the US economy alone is not sufficient. That approach has been aspirational for nearly 50 years and now, more is needed. In large part this is true because -- as many experts have noted -- the so-called notice-and-choice privacy regulatory model neither gives clarity to innovators nor provides adequate protection for individuals. Few people will read businesses' privacy policies designed to provide them notice, and even fewer will make effective choices about a

businesses' data practices in the emerging age of the Internet of Things, and widespread deployment of technologies such as artificial intelligence, machine learning, algorithmic processing and predictive analytics.

Intel believes the promise of these new technologies will be diminished, delayed or lost if America's data policies are not properly calibrated. Intel recently published a white paper outlining this approach, which is available at: https://blogs.intel.com/policy/2018/10/22/rethinking-privacy-in-the-age-of-ai/. Because many of these technologies are capable of making autonomous determinations in near real time, the U.S. government approach to data must also anticipate, embrace, facilitate and guide the implementation of these technologies. As our paper and this set of comments recommend, the use of individuals' data and automated decision making technologies should be fostered while being augmented with safeguards to protect individuals.

Individuals need to have trust in their use of technology. Privacy is a fundamental component of that trust. For the US to continue being a leader in data innovation, US policy must evolve beyond notice and choice to provide new leadership that fosters risk-based assessments, a culture of accountability, and policies that foresee and mitigate the risks of emerging harms to individuals and society. The country needs laws that promote business conduct that increases the public's willingness to share data with businesses. That is why Intel advocates for legislation that would direct companies and not-for profits -- including those that collect data directly from individuals and those that obtain it from other sources -- to implement a risk-based assessment of their data practices designed to advance personal privacy and security.

Strengthening and nationally harmonizing US policy regarding privacy and security is essential to our economy. US businesses and the public have benefited broadly from the utilization of personal data. The requirement for these processes must also be drafted in a way so as not to create an undue burden on small and medium size businesses, while also recognizing that some of those organizations may use sensitive information of a great number of people. If the Administration adopts these evolutionary approaches, it can achieve its stated goal of achieving harmonized privacy systems that benefit individuals and businesses.

Our comments and answers to those questions posed in this Notice highlight approaches that should be adopted to foster economic development. Doing so will lead to better protections for individuals, greater consistency at a state and federal level and greater clarity for innovators. Adoption of these broader policies in addition to those already articulated in this Notice, and the adoption of a

comprehensive privacy law that includes the provisions we discuss below will address longstanding limitations of the notice and choice approach.

Intel's recommendation for the Administration is that whatever policy is adopted it must achieve two goals in addition to directing businesses everywhere to create a process and culture embracing accountability. Accountability, while one of the eight FIPPs, has historically not been relied upon enough as a mechanism to provide privacy for individuals. The policies promulgated by the Administration must simultaneously: (i) provide regulatory clarity and certainty to businesses and organizations utilizing individuals' data; while (ii) increasing individuals' confidence that rules and protections exist to ensure people benefit from, and will not be harmed by, those data-driven innovations. Accountability makes these two goals achievable. Organizations cannot make sound investments without clarity concerning the rules of the road. People will not have confidence in the system unless they know that risk assessments have been undertaken, appropriate mitigation techniques for known and foreseeable risks are employed, and regulators are prepared to impose penalties for violations of the public's trust. Adopting this accountability structure through policies, and a comprehensive U.S. privacy law, will continue to ensure that the American economy is an innovators' economy that benefits the American people maximally and limits, or ideally, eliminates harmful misuses of data.

Intel has created a draft bill for a comprehensive U.S. privacy law based on a full implementation of the FIPPs. We want to promote full and transparent public dialogue about its provisions and have created a website at http://usprivacybill.com to invite people to join the dialogue.

Question A

It is long past time that US data policy moves beyond simply seeking for companies to provide people notice of a data collection or use of their data and asking them to provide their consent. First, personal data protection programs should be required for all businesses irrespective of the products or services they sell. Second, the complete set of FIPPs, core tenets of best privacy practices for the last 40 years of US and worldwide approaches to privacy, are essential. Individuals need to know what they can expect of organizations that process their personal data. The Administration should expand its proposals to embrace policy outcomes creating accountability for data practices by leading businesses and organizations to:

(1) POLICIES -. put in place written policies and procedures.
(2) INTERNAL LEADERSHIP, STAFFING, AND OVERSIGHT.— appoint a data privacy leader responsible for developing and implementing the organization's consumer privacy and data security program, and related policies and practices.

(3) STAFFING AND DELEGATION – dedicate resources to ensure that the privacy program is appropriately staffed by adequately trained personnel.
(4) EDUCATION AND AWARENESS.— implement an up-to-date education and awareness program to keep employees, contractors and third parties aware of data protection obligations.
(5) ONGOING RISK ASSESSMENT AND MITIGATION.— develop a process to identify, assess, and mitigate privacy risk, including privacy risk raised by new products, services, technologies, methods of processing, and business models.
(6) PROGRAM RISK ASSESSMENT OVERSIGHT AND VALIDATION.— conduct a periodic assessment of the accountability program and supporting processes to ensure compliance with this section.
(7) INCIDENT MANAGEMENT AND COMPLAINT HANDLING.— implement procedures for responding to data breaches and for addressing inquiries and complaints concerning personal data.
(8) INTERNAL ENFORCEMENT.— follow through on internal enforcement of the covered entity's policies and discipline for non-compliance.
(9) REDRESS.— adopt procedures to provide remedies for privacy risk.

In addition to recommending that the Administration promote practices that lead to risk assessments and systems promoting accountability, the US needs a privacy law that is unique for the country's ethos of freedom, innovation and entrepreneurship. A comprehensive privacy law needs to protect individuals and encourage the ethical use of data. We need a law that promotes ethical data use, not one that just attempts to minimize harm. Any law that prevents the beneficial uses of the data of an individual and groups of individuals will be too constraining and will ultimately diminish the promise of the digital age. Intel has seen that the use of data helps solve some of the most vexing global problems while spurring economic growth. Laws that permit novel data usage for innovations that benefit individuals and society must also require ethical uses of data.

Innovation cannot be an excuse for unfettered experimentation. Rather, a law that promotes innovation but consistently leads to benefits being produced for the individuals whose data is utilized and for society, writ large, creates a virtuous cycle that increases the benefits of the digital age. Therefore, the Administration should advocate for a privacy law that requires ethical usage of data. Prior to the enactment of such a law, the Administration can increasingly convene stakeholders and experts to establish greater understanding concerning the ethical treatment of data to further minimize risks of data misuse that could harm a specific individual or groups within society. Moreover, laws requiring the ethical use of data will be ever more critical as we use the data to train artificial intelligence algorithms to detect bias and protect cyber security, undertake machine learning, and apply predictive analytics to data.

A US privacy law should expressly create a framework both for the beneficial usage of artificial intelligence, and erect protections to ensure that individuals and society are not treated unfairly by the use of those technologies. These emerging technologies will create enormous benefits to American businesses and individuals. The Administration can and should foster policies and promote legal clarity that set forth when and under what circumstances these technologies can be employed. At the same time the Administration and Congress, when drafting any comprehensive privacy law, must anticipate new harms that may arise from the use of these technologies. Any new policy or law must include mechanisms for individuals and groups to be informed about the use of these technologies and obtain redress for unfair or unjust consequences arising from those technologies.

Question B

Intel encourages the Administration to expand its list of goals to: (i) study and resolve problems arising from onward transfer of personal data to third parties; and (ii) set expectations that leadership is required in the digital age and by US policy.

First, as stated above, Intel suggests that the Administration should embrace a policy approach that requires organizations - both companies and not-for-profits, of all sizes to analyze the risks and benefits from the use of data. This is especially true for the risks arising from the sharing of personal data with a third party and any additional, onward transfer of that data. In addition to the approach already outlined, the Administration also should require organizations to require responsible approaches to the subsequent uses of that data by the entities to which it transfers data. Current privacy laws provide mechanisms for enforcing violations of public trust by a company that an individual interacts with directly and intentionally. Current laws do not yet, however, fully address misuse of data by companies that subsequently and legitimately obtain that data, for example through a processing agreement with the data holder, nor do they provide a means for individuals to exercise the FIPP of individual participation with third parties acting as data brokers who obtain and resell their data. The Administration should build on work the Federal Trade Commission has done to understand the data industry and convene experts to study how best to minimize risk from the onward transfer and subsequent use of data by companies with which individuals have no relationship.

Second, NTIA and the Administration should expand the stated goals to set an expectation of leadership within each organization that touches individuals' data. The Administration should foster programs that educate corporate leaders concerning their responsibilities involving personal data. Organizational leadership can lead to practices and requirements that transform organizational culture and

instill greater trust in the public concerning the collection, storage, use and sharing of individuals' data.

Question C
Intel recommends that the Administration convene a broad range of experts and stakeholders to examine several questions not presented by this notice, such as:

- How should individuals exercise the FIPP of individual participation with respect to third parties with whom they do not have an existing relationship?
- What policies can be adopted to mitigate or eliminate foreseeable, emerging harms to individuals, such as price discrimination, redlining based on data, misuse of genetic data, etc.?
- What policies can be adopted to mitigate or eliminate foreseeable, emerging harms to society?
- How can the government ensure that the use of artificial intelligence, algorithms and predictive analytics result in accurate and fair outcomes for the individual whose personal data is processed and for groups within society?
- How can government encourage the sharing and availability of data needed to train artificial intelligence algorithms to solve the world's large problems, including those that protect privacy such as improving cybersecurity or reducing discrimination and bias?
- How can the government ensure that individuals have appropriate information and visibility into the collection and use of their information in a way that will not stifle innovation?

Answering these questions could lead to additional policies and recommendations from the Administration that will increase the public's confidence in the widespread use of personal data to power our economy.

Finally, the Administration should work hard to counteract the misperception that deletion of data (i.e., minimization) is per se beneficial for privacy. While companies should not collect data they do not and will not need, policies requiring that companies purge data after its use or prohibiting repurposing that data are often counter productive. Intel has learned that, in fact, often reusing data, with appropriate application of the FIPPs can be beneficial for fostering innovation, gleaning unexpected insights from data sets and to advance data security purposes. In fact, it often takes data to protect data. For example, algorithms can help detect unintended discrimination and bias, and identify theft risks or cyber threats.

Question E
Robust, harmonized and predictable enforcement is necessary for any future federal privacy law. The US Federal Trade Commission has decades of experience protecting privacy. What the Commission needs are:

(i) More resources;
(ii) Authority to oversee all industry sectors';
(iii) A clear mandate to develop guidance and regulations to communicate to organizations how they should implement the FIPPs'; and
(iv) The ability to enforce meaningful but fair sanctions.

We propose that the Administration adopt policies that preserve a role for State Attorneys General to further enforce harmonized policies and law.

Question F
A comprehensive US privacy law must facilitate data usage by innovators and provide equal protections to US persons no matter where they live and work. This will require harmonization of any federal law with any state laws. A non-harmonized patchwork of state legislation will cause companies to default to restrictive requirements and the result will decrease the likelihood of realizing technology's great potential to improve lives.

In addition to policies and a law that harmonizes data practices across the US, the Administration should seek policies and law that harmonize rules for all technologies and all sectors of the economy. All companies are now data companies, irrespective of their size, scope or goods or services sold. It stands to reason, therefore, that rules should apply universally and consistently throughout the economy and be written intentionally to be tech neutral so that they stand the test of time.

Conclusion
In conclusion, Intel stands ready to assist the Administration and NTIA in this inquiry.

Respectfully submitted,

David A. Hoffman
Associate General Counsel and Global Privacy Officer
Intel Corporation