**An Ethical and Innovative Privacy Law**

**Why Pass a US Federal Privacy Law?**
Effective privacy regulation is critical to allow technologies like artificial intelligence to help solve the world’s greatest challenges. The combination of advances in computing power, memory and analytics create a possibility for technology to make tremendous strides in precision medicine, disease detection, driving assistance, increased productivity, workplace safety, education and more. At Intel we are developing many of these technologies and are focused on integrating artificial intelligence capabilities across the global digital infrastructure. At the same time, we recognize the need for a legal structure to prevent harmful uses of the technology and to preserve personal privacy so that all individuals embrace new, data-driven technologies. At Intel we know that privacy is a fundamental human right and robust privacy protection is critical to allow individuals to trust technology and participate in society.

What the US needs is a privacy law that parallels the country’s ethos of freedom, innovation and entrepreneurship. That law needs to protect individuals and enable for the ethical use of data. As noted above, the use of data by new technologies such as artificial intelligence will help us solve some of the most vexing global problems while spurring economic growth. Ethical use of data will be critical as we use data to train artificial intelligence algorithms to detect bias and enhance cyber security. In short, it takes data to protect data. The US needs a law that promotes ethical data stewardship, not one that just attempts to minimize harm. 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. Intel has drafted proposed legislation to realize that potential. It promotes innovative data use, while requiring organizations that process personal data to implement measures to demonstrate responsibility.

**How is the proposal structured?**
The law uses the Fair Information Practice Principles (FIPPs) from the Organization for Economic Cooperation and Development’s (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. The OECD FIPPs are “the Global Common Language of Privacy” and many of the privacy laws around the world are based on them. For the past few years, Intel has worked on a “Rethinking Privacy” initiative to take the OECD FIPPs and show how they can be implemented in law differently to promote the innovative and ethical use of data given the changes in technology we have seen since the OECD FIPPs were first adopted.

In our new proposal, these eight FIPPs work in concert with each other to allow for data use while protecting individuals. We do this by “rethinking” how they relate to each other.

**Collection Limitation**
The law encourages organizations to create new mechanisms for individuals to provide meaningful consent for data use. Most uses of data will require a risk/benefit analysis that will restrict an organization from using data in a way that creates undue risk for individuals. However, in many situations, individuals may be ok with these risks, and will want to have the benefits of the use of the data. This bill encourages organizations to create mechanisms where those individuals can make informed choices.
An Ethical and Innovative Privacy Law

Data Quality
As artificial intelligence tools are deployed across more industry sectors, it will be critical that the data used to train those algorithms has adequate diversity and volume. For example, for precision medicine, it is critical that the algorithms are trained with sufficient data from ethnic and racial minorities. This is one reason that international data flows are so important. This bill allows for the access to the data that creates better quality in the algorithms, while also requiring organizations to measure that data quality and adjust for any deficiencies.

Purpose Specification
It is critical that organizations state their purposes for collecting and processing data. The law makes clear those purposes must be described narrowly and specifically.

Use Limitation
Our proposal requires organizations to analyze the risks and benefits from the use of data. It also requires organizations to control the uses of data from the entities to which it transfers data.

Security Safeguards
The bill requires organizations to adopt reasonable measures to protect personal data.

Openness
Research shows that for the most part people do not read privacy policies. However, privacy policies can play a useful role to describe how an organization uses personal data. Our proposal requires three types of policies to foster that understanding: 1. An explicit notice when particularly sensitive data is being collected, which will enable better informed consent, 2. A thorough report of the organization’s use of personal data, to enable regulators and advocates to better understand the entity’s practices, and 3. Publication of the traditional privacy policy, but with more detailed information on the purposes of data collection.

Individual Participation
It is critical to understand when organizations have data, and for the individuals to whom that data relates to have an ability to object when that data is either incorrect or when its use will disproportionately cause harm.

Accountability
The law encourages organizations to implement robust privacy programs that will decrease the risk of data misuse and security breaches.

How will the law be enforced?
Robust, harmonized and predictable enforcement is necessary. The US Federal Trade Commission (Commission) has decades of experience protecting privacy. What the Commission needs are: 1. More resources, 2. Authority to oversee all industry sectors, 3. A clear mandate to develop guidance and regulations to communicate to organizations how they should implement the FIPPs, and 4. The ability to enforce meaningful but fair sanctions. Our proposal provides all four of those elements, while also preserving a role for State Attorneys General to apply sanctions in situations where the Commission
An Ethical and Innovative Privacy Law

delays to start an enforcement action. The law uses those sanctions as a way to further encourage organizations to demonstrate their accountability, by allowing those entities that adopt robust privacy programs to have a safe harbor from civil penalties.