The US Innovation Economy Requires Strong National Privacy Protections

WRITTEN STATEMENT FOR THE RECORD

DAVID HOFFMAN

ASSOCIATE GENERAL COUNSEL AND GLOBAL PRIVACY OFFICER

INTEL CORPORATION

Before the UNITED STATES SENATE JUDICIARY COMMITTEE, Hearing on "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation."

March 12, 2019

Good morning Chairman Graham, Ranking Member Feinstein, and Members of the Committee. Thank you for the opportunity to testify today. I am David Hoffman, Associate General Counsel and Global Privacy Officer at Intel Corporation. I am pleased to address the Committee on the critical importance of protecting privacy while also spurring innovation and competition.

Intel's position is clear: we believe it is time for the United States Congress to enact strong federal privacy legislation. Some stakeholders may believe that a robust national privacy law is inconsistent with innovation, operating a profitable commercial enterprise, maintaining an open marketplace or driving economic growth. At Intel, a technology company that is an engine for global innovation, we know that is unequivocally false. In fact, the failure to implement a robust privacy framework in the United States presents the greater risk to the long-term economic wellbeing of our country. In addition, companies trafficking in personal data collected and used in ways outside individuals' reasonable expectations undermines the trust that is necessary for society to realize the full value of technology.

To ensure a thriving US economy that encourages the innovative use of data, Congress should prioritize enacting strong federal legislation that:

1) Enables Ethical And Innovative Data Use
2) Provides Meaningful Protections Instead Of The False Promise Of Control
3) Prohibits Unaccountable Data Sharing With Third Party Companies
4) Empowers And Fully Resources The Federal Trade Commission
5) Creates A Single National Standard

My more than two decades of experience in the US privacy debates inform these opinions. I joined Intel Corporation in 1998 and worked on legal and policy issues for many of the technologies that have created the internet infrastructure the world uses today.

I currently lead Intel's global privacy efforts, and serve on multiple private sector boards and advisory committees including for the Information Accountability Foundation, the Future of Privacy Forum and the Center for Cybersecurity Policy and Law. I participated on several government privacy advisory boards at agencies including the U.S. Federal Trade Commission, the U.S. Department of Homeland Security and the

European Commission. At the U.S. National Security Agency, I serve as the Chair of the Civil Liberties and Privacy Advisory Panel, supporting the NSA's mission to protect national security while preserving privacy and civil liberties. I lecture on the responsible and ethical use of data at schools around the world, and currently hold the appointment of Senior Lecturing Fellow at the Duke University School of Law, where I co-teach a class on Information Privacy and Surveillance Law.

Intel is an innovation success story. We are mindful that our success is predicated on the continuing trust placed in us by businesses and consumers that we will be ethical, thoughtful, protective and clear about how we use personal data and with whom we share it. We endeavor to earn that trust every day. Individuals who use our technologies rightly insist that we look out for their best interests. Trust is the foundation of innovation. Because Intel prioritizes earning that trust, we have succeeded and continue to innovate. This insight is the foundation of Intel's recommendations to the Committee this morning.

Intel's commitments to innovation and trust forms the foundation of our draft legislation, which is appended to this testimony and which we released publicly in November. To help us create a thoughtful recommendation for Congress, we invited many of the world's top privacy experts from industry, civil society and academia to comment on our legislative proposal and invited the public to do the same. Those experts examined the draft and submitted comments to Intel both publicly and in private meetings. Based upon the extensive feedback we received, Intel released a second version on International Data Privacy Data this past January. The resulting legislative language reflects thousands of hours of work over many months. Our proposed bill has been well received by industry privacy practitioners, leading privacy lawyers who represent a cross section of American industry, privacy advocates, and widely respected academics. We understand the daunting challenge policymakers face to put in place a national standard and it is our hope that our extensive work can support your efforts.

INTEL'S COMMITMENT TO INNOVATION AND PRIVACY

There appears to be confusion on what it means to be a technology company and what is required to innovate and drive economic progress.

Intel is the world's largest semiconductor manufacturer. We have powered computing and communications for over fifty years. Intel is the world leader in the design and manufacture of essential technologies and platforms that power the cloud and an increasingly smart, connected world. We employ over 100,000 people, with approximately 87% of our employees in technical roles. More than 200,000,000 of our latest-generation transistors can fit on the head of a pin. Our semiconductor fabrication facilities are some of the most complicated manufacturing operations on the planet, and our materials scientists produce inspiring new discoveries that propel Moore's Law forward.

Our technologies unlock the power of data so we can: ride in self driving cars, connect with each other over lightning fast mobile networks, facilitate advances in artificial intelligence to improve many aspects of our lives, and experience virtual worlds. We are creating technologies that are transforming the entire economy, including the manufacturing, agriculture and health care sectors.

We produce these technologies as platforms that others can innovate on top of to develop businesses across all industry sectors that drive the global economy. In short, Intel is a real technology company.

In contrast, many companies are now called "technology companies" merely because they monetize and weaponize the data of others. Many of these companies do not manufacture anything and they do not create platforms on which others can innovate. Thousands more create a wholly unregulated, secondary market buying and selling individuals' data without any consequence for their misuses of personal data or the misuses they empower. At Intel we do not consider these organizations to be technology companies. Too many of them lurk in shadows profiting off of data in ways that are unexpected and harmful to those individuals to whom that data relates. These data brokers use technology to fuel malicious business models, but do not further the state of technology in any way that helps society. Instead, these companies poison the well of trust out of which real technology companies like Intel and our customers must drink. Calling a data broker a technology company is like calling a paparazzi an investigative journalist.

Intel depends upon two things for our technology to drive economic and social progress:

- INNOVATION – we need a legal and policy environment that properly encourages companies to invest in technology innovations on top of our platforms.
- TRUST – we need individuals to have trust and confidence in their use of these innovative new products and services.

The current environment of surreptitious, dangerous and harmful uses of personal data weakens the trust that individuals have and thereby decreases the likelihood of innovation in a variety of uses of technology (new methods of online banking, digital education products, electronic healthcare delivery). Net – privacy invasive companies are holding back society from realizing the full value of technology. As we move into an environment where we will have even more potential for progress from innovations such as autonomous driving, artificial intelligence and 5G, it is critical we address this issue of malicious actors unjustly profiting from the manipulation and sale of personal data. It is critical we do not allow data brokers' short term gains to put at risk individuals' and society's long term needs.

Policymakers have explored issues related to commercial privacy for decades. It is a complex issue that has far reaching implications and requires thoughtful deliberation. But after years of debate, we now need this Congress to create a law to properly protect individuals, while also encouraging the innovative use of technology. Do not believe those who tell you that the innovative use of data and protecting privacy are a zero sum game. We can accomplish both of these goals, and Intel has provided this Committee with a draft legislative proposal, which we believe achieves both outcomes.

I. Enable Ethical and Innovative Use of Data

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 the possibility that technology can make tremendous strides in precision medicine, disease detection, driving assistance, increased productivity, workplace safety, education and more. Intel recognizes 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.

As we approach the third decade of the 21st century, the US needs a privacy law that supports the development of 21st century technology consistent with our country's long standing commitment to respect for the individual, the protection of privacy and freedom from unreasonable surveillance, as well as our uniquely American ethos of freedom, innovation and entrepreneurship. The US needs a privacy law that promotes innovative data use, not one that just attempts to minimize harm.

Many of the laws currently being proposed at the state level unduly restrict the use of data, even in situations where the use does not increase privacy risk or harm to the individual. A patchwork of these laws will decrease the likelihood of realizing technology's great potential to improve lives.

In contrast, the legislation drafted by Intel proposes a system that preserves the opportunity for ethical businesses to innovate using individuals' data provided that companies analyze risks to individuals, their families and society and then take actions to mitigate those risks. We urge Congress to legislate a similar approach.

II. Provide meaningful protections instead of the false promise of control

GDPR and CCPA both rely significantly on the concepts of "notice and consent". The "notice and consent" model has attempted to provide for the Organization for Economic Cooperation and Development's (OECD) Fair Information Practice Principle (FIPP) of Individual Participation for decades. It has been a valuable tool to empower citizens and give them control over data, but has always had limited effect due to the tremendous burden it places on individuals to fully understand how information that relates to them is collected, processed and used. In many situations the control of personal data is not only helpful, but also it is necessary. Organizations should be encouraged to provide the ability for individuals to consent to the use of their data in situations where that consent will be practicable and meaningful.

However, virtually all existing privacy laws around the world and many of the proposals pending in Congress and the states suffer from the same flaw: they put an undue burden on individuals to protect themselves from misuse of personal data. The notice-and-consent model is fatally flawed; it must be replaced. People do not have time to read privacy policies for every interaction where their personal data will be collected and used. Even if they did read these policies, it is unlikely they would be able to understand how this data will be used. Further, we know that as technology advances increasing amounts of data that relates to individuals will not come directly from them. Instead, it will come from government records, what other people post on the internet or from inferences derived from peoples' social connections and activities.

For these reasons, telling people they will have the ability to control data is a false promise. While giving consumers "rights" to control their data sounds sufficient, it asks too much of them and thereby perpetuates the erroneous notion that consumers can have control. Also, a focus solely on telling individuals to manage privacy by controlling how their data is used will create potentially anticompetitive consequences by providing the benefits of the use of the data to those companies that have the most direct relationship with the individual and can thereby encourage the provision of consent.

Instead, Congress should acknowledge this mistaken premise of existing laws and place affirmative obligations on companies that would like to use personal data. A better regulatory model requires companies to adopt measures to demonstrate their accountability and restricts companies' use of data that creates undue risk for the individual or society.

III. Prohibit Unaccountable Data Sharing with Third Party Companies

Intel fears that the promise of artificial intelligence could be left unrealized by both improper transfers and sales of data to third party companies and by clear misuses of that data by those recipient companies. Congress should act now to prohibit both of these abuses. Congress can and should prohibit subsequent transfer or sale of personal data to third party companies and organizations that is contrary to individuals' expectations and where the transfers will likely harm the individual or society. Additionally, Congress should anticipate obvious misuses of consumer data and take those off the table.

Just as the notice-and-consent model is fatally flawed, individuals cannot know or understand when any of the myriad of companies that collect their data each day are sharing that data with third parties. Congress should prohibit the uncontrolled, unaccountable data sharing by companies that collect consumer data with third party companies and organizations.

Once data is loose, it can be and is transferred or resold countless times without consequence for the companies that collected it and without any punishments for misuse of that data by the companies that subsequently obtain the data. Congress can and should require companies that wish to transfer data to third parties to: (i) analyze the risks of that sharing prior to doing so; (ii) impose contractual limitations on subsequent sharing and the usage of that data; (iii) demand commensurate or better protections from the recipient companies for that data; and (iv) be held accountable when they, or the recipient companies, fail to safeguard the personal data they transfer.

IV. Empower and Fully Resource the Federal Trade Commission

Robust, harmonized and predictable enforcement is necessary. Without enforcement, organizations that use data irresponsibly will decrease the ability for companies who invest in accountability to compete in the marketplace and invest in innovation. The US Federal Trade Commission (Commission) has decades of experience protecting privacy. What the Commission needs are: (i) more resources; (ii) authority to oversee the data practices of 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 and 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 declines 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.

V. Create a Single National Standard

The lack of a US federal law requires individual states to legislate, and thereby creates an unworkable patchwork. This confusing approach is bad both for individuals and companies. The only entities that will benefit from conflicting and confusing state laws will be large law firms, as even the smallest of companies will need to pay exorbitant legal fees to understand their obligations. Similarly, privacy protection through widely varying state laws hopelessly confuses individuals as they try to understand which rights they have with respect to their data. Our analysis of current state proposals convinced us these laws will create limitations on appropriate uses of data without preventing the misuses of personal data that cause significant harms to individuals and animate the public's fears. Without a strong federal law, we will have an environment that impedes innovation while inadequately protecting individuals.

As an alternative approach, the legislative proposal we submit for your consideration provides a strong national standard. The model uses the OECD FIPPs. The FIPPs are an American creation, first introduced in July 1973, when an advisory committee of the U.S. Department of Health, Education and Welfare proposed a set of information practices to address a lack of protection under the law at that time, 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. What follows is a short description of how our proposal implements the FIPPs.

Collection Limitation
The proposal 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.

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 bill 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.

Enforcement

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

Conclusion

Competition and innovation require clear standards for data use, obligations to implement measures to demonstrate accountability and robust harmonized and predictable enforcement. The current environment allows data brokers and other malicious actors to destroy the trust that individuals should have in their use of technology. State legislatures are attempting to repair that trust, but their efforts will decrease competition, harm innovation and provide false promises of protection to individuals. If Congress does not act, the resulting patchwork of state laws will impede the use of technology to improve society, while allowing data brokers to continue to profit off of the pain of the American people.

In contrast, Intel's proposal pushes companies to analyze the risks to individuals from the use of their data. The framework requires companies to anticipate those risks and act before there is harm, not only after the bad actors are caught. Our proposal provides strong protections and robust enforcement, while still allowing for the innovative use of data to allow artificial intelligence and other technologies to fulfil their promise. I encourage you to use our framework to put in place a law that will optimize for the ethical and innovative use of data. The full text of our draft can be found at http://usprivacybill.intel.com.

Thank you again for the opportunity to testify this morning and share Intel's experience and perspective. We stand ready to support this Committee's efforts to advance legislation.