Responses to Questions for the Record
Submitted by David A. Hoffman
Associate General Counsel and Global Privacy Officer
Intel Corporation

Senate Judiciary Committee

Hearing on “GDPR and CCPA: Opt-ins, Consumer Control, and the Impact of Competition and Innovation”

Questions for the Record from Senator Lindsey O. Graham
U.S. Senate Committee on the Judiciary
"GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"

1. **What was your estimated initial cost (both time and expense) to become GDPR compliant?**

   The General Data Protection Regulation repealed Directive 95/46, which constituted the previous privacy framework in Europe. Although the Directive was implemented in different ways in the 28 EU Member States, Intel had already a robust compliance program in place. Intel had also participated in the process for the development of GDPR, and during that time worked to evolve our program. Therefore, the entry into force of GDPR has been an opportunity for the company to review existing practices, streamline and update internal policies, and adapt the overall program to the new legal requirements. Intel's privacy program is shaped in a way that allows it to evolve with new legal provisions, without being tied to a specific piece of legislation.

   The GDPR readiness team worked for over two years following a plan divided in several work streams with checkpoints to make sure we could meet the timeline. The team worked closely with business units to identify gaps and challenges in order to establish a governance model that functions as a continuous cycle (implement-audit-assess-improve): in fact, demonstrating compliance is an ongoing effort that does not stop with the preparation for new legal requirements but one that requires an open-ended process that can flexibly adapt to business and regulatory changes.

2. **What are your estimated recurring annual GDPR compliance costs (both time and expense)?**

   Compliance to GDPR represents the everyday work for our EU/EMEA Privacy Team (ten employees), who are also monitoring enforcement by regulators at the national level. Other employees are consulted on an ad-hoc basis for specific issues (e.g. data management, marketing tools) and business unit lawyers are involved in tracking business roadmaps to anticipate privacy risks.

3. **What is your estimated initial costs (both time and expense) to become CCPA compliant?**

   For CCPA compliance, Intel leveraged the work done on GDPR and costs previously incurred on the global compliance program. However, given the differences between CCPA and GDPR, we will continue to invest a significant amount of time and resources to work toward compliance once CCPA goes into effect next year.

4. **What are your estimated recurring annual CCPA compliance costs (both time and expense)?**

   Compliance to CCPA represents an important daily task for our US Privacy team (which includes 17 employees, full or part-time). On specific requirements such as "do not sell" we foresee incremental work to maintain adequate compliance as Intel's business evolves.

5. **Are you differentiating your products based on consumers or businesses in the EU and California?**

   Intel offers appropriate privacy safeguards to employees and business customers worldwide. At this time, we do not differentiate our products based on GDPR or CCPA.

6. **What are the specific areas of the CCPA that could have a negative impact on competition and innovation? What areas of the CCPA need more clarity, improvement, or removal?**

   CCPA takes a "notice and consent" approach to privacy, which both burdens the innovative use of data, while also not sufficiently protecting privacy. CCPA puts too many burdens on individuals to understand when their personal data is processed. Instead, the obligations should be put on the companies that want to use the data. Intel's proposal at https://usprivacybill.intel.com does just that.

Questions for the Record from Senator Chuck Grassley
U.S. Senate Committee on the Judiciary
"GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"

Questions for the First Panel

1. **Please briefly explain the importance of transparency and ensuring that consumers can make informed decisions about the information they share.**

   Transparency is a fundamental concept for users to build and maintain trust and confidence in the technology and services they use. Our draft proposal codifies this notion in outlining policies around the principles of purpose specification, individual participation, openness, and accountability.[1]

2. **Transparency is critical in ensuring that consumers can make informed decisions. That can become more complicated, however, as our lives are increasingly connected to the technologies around us, like autonomous vehicles. According to one report, by 2025 each person will have at least one data interaction every 18 seconds – or nearly 5,000 times per day.[2]**

   a. **How do we balance the need for transparency and informed consent with the reality of our increasingly data-connected daily lives?**

      Technology companies need to make transparency convenient for the users they serve. Most people do not read privacy policies, and even if they did, they would not have time to read them for every situation in which their data is used. Further, even if they did have time, most people would not be able to clearly understand which organizations are using their data. This system no longer makes sense in today's data-connected world – too much burden is placed on the user to not only understand, but also agree to ways in which their data is being used.

      Intel's draft proposal lifts this burden from users and places it with companies to avoid the use of data that creates risk for individuals. To achieve both more transparency and more effective technologies and services, we need to place the responsibility for protecting privacy on

[1] https://usprivacybill.intel.com/wp-content/uploads/An-Ethical-and-Innovative-Privacy-Law-Summary.pdf

[2] David Reinsel et al., *The Digitization of the World—From Edge to Core*, IDC (Nov. 2018).

companies, not the users themselves. Intel's proposal focuses on providing appropriate transparency to both individuals and to regulators.

b. **Should consumers have to consent to every data interaction throughout their day?**

   As the report by the IDC suggests, we are already living in a data-saturated world. It is simply not possible for consumers to be expected to not only track but also understand and consent to every data interaction they may face throughout one day. A consent model puts too much of a burden on individuals. Intel's model focuses on encouraging organizations to find mechanisms to allow individuals to consent, while also providing other protections to make sure the use of data does not create risk.

   People use technology services because they make certain processes simpler and more convenient, and there are many instances in which it would be burdensome for users to consistently have to agree to data use for every single interaction.

3. **If Congress enacts federal data privacy legislation, how do we ensure that companies are still incentivized to innovate in their privacy and data protections, rather than just 'check the box' of regulatory compliance?**

   Strong privacy protections and innovation are not mutually exclusive. Protecting privacy while enabling ethical data innovation in areas like artificial intelligence will help users embrace new, data driven technologies, and our bill impels companies to think creatively about doing so.

   Additionally, our proposal includes provisions for organizations to consider the deployment of privacy enhancing technologies as part of their risk management processes, as well as funding, research, and guidance from the government about implementation.

Questions for the Record from Senator Mazie K. Hirono
U.S. Senate Committee on the Judiciary
"GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation"

1. **During the hearing, I mentioned that there is significant evidence that a consumer's privacy settings are "sticky," with consumer's rarely altering their default privacy settings.**

   Do you agree that the vast majority of consumers rarely change their default privacy settings?

   I agree. This behavior can be explained for two reasons: a) confidence in innovative products and b) lack of technical knowledge. Over the past five decades, Intel has built trust in technologies that improve people's lives. However, users are not abreast of the pace of technology today: unfortunately, some organizations like data brokers are monetizing and weaponing citizens' data. For this reason, we have always called for private companies to embrace risk-based accountability approaches.

   Accountability can be described as the ability of responsible organizations to demonstrate that appropriate measures have been put in place to minimize privacy and security risks. These technical or organizational measures should be tailored based on each business' needs as well as the specific risks associated to the data processing performed. Consequently, regulators could deem accountability measures as a proof of legal compliance or at least a mitigating factor in case of a data breach.

2. **In view of the "sticky" nature of privacy settings, my inclination is to have a system in which, by default, a consumer is considered to have opted out of data collection and a company can only collect that consumer's data if the consumer expressly opts in to data collection. I understand from the hearing that you do not support such an "opt-in" privacy regime.**

   Please explain why you do not think an "opt-in" privacy regime is the right approach and how you propose to ensure that each consumer is aware that his or her data is being collected and that the consumer consents to that collection.

   The "notice and consent" model has attempted to provide for individual participation for decades. It has been a valuable tool to empower citizens and give them control over data, but has always had a 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.

While an “opt-in” privacy regime is preferable to an “opt-out” one, Intel believes that these models still put excessive burden on individuals to understand the data lifecycle. The ever-changing technology environment shows that for instance, the use of notice and consent will increasingly be difficult in many data collection and creation contexts. For this reason, in our draft proposal we clearly define the fair information privacy principle of “use limitation” in permitted processing based on consent, or legal obligation, or consistent use and reasonable amount of privacy risk. This proposal is meant to empower organizations to process data without consent but does not represent a blank authorization, because it works in concert with the other substantive rights provided to individuals (access, correction, deletion, portability) and obligations on organizations, such as security safeguards and accountability approaches, described above.

3. **Intel’s proposed data privacy legislation recognizes the potential for machine learning, algorithms, and predictive analytics to discriminate on the basis of sex, race, or other protected class. It will be important that any data privacy legislation ensures that companies cannot hide behind technology to avoid responsibility for unlawful discrimination.**

   How can we ensure that a company’s algorithms are not illegally discriminating when those algorithms are often treated as trade secrets and protected from review?

   There have been many examples of unintended bias in datasets or algorithms resulting in unintended discrimination of individuals.[3] To prevent this, Intel’s bill calls for heightened protections related to automated processing that require covered entities to complete assessments that analyze both the potential for bias and the possibility for increased privacy risk. We believe that organizations implementing algorithmic or artificial intelligence (AI) solutions should be able to demonstrate that they have the right processes, policies, resources, and accountability measures into place to ensure that the data and algorithms they are using do not perpetuate bias or discrimination.

   Intel actively participates in and contributes to research in the fields of privacy preserving technologies, bias, and transparency. Additionally, we amended our draft proposal to include provisions to require covered entities to consider the deployment of privacy enhancing technologies as part of their risk management processes, for the Federal Trade Commission to recommend to Congress what funding is needed for research on privacy enhancing technologies, and for the

[3] See, for example, the notable work of Joy Buolamwini: https://www.media.mit.edu/people/joyab/overview/

Federal Trade Commission to provide guidance to covered entities on how to implement privacy enhancing technologies.

Intel also supports continued collaboration between government and the private sector to study and develop solutions to regulate discrimination caused by AI implementations.

Questions for the Record from Senator Cory Booker
U.S. Senate Committee on the Judiciary
"GDPR & CCPA: Opt-ins, Consumer Control, and
the Impact on Competition and Innovation"

1. **Marginalized communities, and specifically communities of color, face a disproportionate degree of surveillance and privacy abuses. This has been the case since the Lantern Laws in eighteenth-century New York City (requiring African Americans to carry candle lanterns with them if they walked unaccompanied in the city after sunset) up through the stop-and- frisk initiatives of more recent years.**

   There are echoes of this tradition today in the digital realm as marginalized communities suffer real harm from digital discrimination. For example, in recent years we have seen many instances of housing discrimination and digital redlining, employment discrimination through digital profiling and targeted advertising, exploitation of low tech literacy through misleading notice and choice practices, discriminatory government surveillance and policing practices, and voter suppression and misinformation targeting African Americans and other minorities.

   I am concerned that—rather than eliminating the bias from our society—data collection, machine learning, and data sharing may actually augment many of the kinds of abuses we fought so hard to eliminate in the Civil Rights Movement. We need privacy legislation that is centered around civil rights.

   a. **In your view, is a private right of action critical to protecting the civil rights of individuals affected by data collection and disclosure practices?**

      Intel's draft proposal focuses on granting the United States Federal Trade Commission (FTC), which has decades of experience protecting privacy, with enhanced rulemaking authority and more resources to develop guidance and regulations to communicate to organizations how they should implement robust privacy protections.

      In addition to strong, harmonized FTC enforcement, our proposal also preserves a role for State Attorneys General to bring enforcement actions.

   b. **How easy is it for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information? How can that information be used to discriminate?**

Over the past few years, we have seen many examples of how information like zip codes – despite being non-sensitive – can reveal an individual's identity or other information about them that can be used in discriminatory ways through the potential to link it with other personal data. Regardless if there is real intent to discriminate, harm can be caused to consumers that can be economic, legal, social, and psychological, reputational, and physical. The use of non-sensitive information linked with personal, sensitive information is one of the many ways in which data brokers have been able to condense and sell information about consumers without any interaction and entirely without the consumer's knowledge. This is a reason why any effective privacy law must define personal data broadly and include publicly available data and government records.

c. **Significant amounts of data about us are gathered by companies most people have never heard of. Do we need a registry of data brokers, similar to what Vermont established last year?**

Data brokers represent some of the most harmful types of data companies, legally allowed to monetize and weaponize the data of others without their knowledge or consent. Any federal privacy law needs to include strong protections against data brokers and the harm they cause to individuals. Creating a registry is one such way in which data brokers could be put in the spotlight, and we support a strong federal privacy law that equips the FTC and State Attorneys General to prosecute and hold data brokers accountable.

2. **The tech journalist Kashmir Hill recently wrote a widely circulated article on her efforts to leave behind the "big five" tech companies—Facebook, Google, Apple, Microsoft, and Amazon. Using a VPN, she blocked all of the IP addresses associated with each company and then chronicled how her life changed. She experimented first by blocking individual companies, and then, at the end of the series, she blocked all five at once. Ms. Hill found that—to varying degrees—she could not get away. Repeatedly, her efforts to intentionally block one company created unpredictable ripple effects for engaging with other, seemingly unrelated, companies and services. Ms. Hill's article spoke to how pervasive these companies are and how much data they capture about us when we're not even (knowingly) using their services. [4]**

a. **How would you respond to the following argument? "If people are**

[4] Kashmir Hill, *I Cut the 'Big Five' Tech Giants from My Life. It Was Hell*, GIZMODO (Feb. 7, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

uncomfortable with the data practices of certain tech companies, they simply shouldn't use their services."

The above argument simply does not hold in the current technology environment, in which people have to navigate not only which digital platforms, payment services, or online shopping websites to use, but also are expected to digest the privacy policies and other terms of each of those digital options. We cannot expect people to have the time or expertise to reasonably evaluate these services.

Instead of being encumbered by having to make decisions about which services to use or worrying about a company's privacy practices, consumers should be able to embrace new, data driven technologies, but this is only possible if people are able to trust the technologies with which they interact.

Intel's federal privacy law proposal encourages this trust by removing the onus from consumers and placing it with companies to make their data practices more safe and not burdensome for consumers. We believe that it is the responsibility of technology companies to make their services and policies more straightforward, and believe that our bill provides the right balance for allowing companies to innovate while upholding strong privacy protections.

b. **What does providing consent mean in a world where it's extremely difficult to avoid certain companies?**

Consistent with the answer to part "a" above, any model that relies upon consumers to give consent to participate in certain services is not applicable in today's data-driven world. It is simply too burdensome to consumers to expect them to consent to all of the digital companies and the services they may provide.

3. **It would take each of us an estimated 76 working days to read all the digital privacy policies we agree to in a single year.[5] Most people do not have that much time. They might prefer something simple, easy, and clear—something much like the Do-Not-Track option that has been featured in most web browsers for years. However, there is a consensus that Do-Not-Track has not worked, because despite the involvement and engagement of stakeholders across the industry, only a handful of sites actually respect the request. A 2018 study showed that a**

[5] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar.1,2012),https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you- encounter-in-a-year-would-take-76-work-days/253851.

quarter of all adult Americans were using Do-Not-Track to protect their own privacy—and yet 77 percent of Americans were unaware that Google, Facebook, and Twitter don't respect Do-Not-Track requests.[6] Just last month, Apple removed the feature from its Safari browser because, ironically, Do-Not-Track was being used for browser fingerprinting, i.e., having the feature turned on was used to distinguish individual users and track them across the web.[7]

a. **What purpose does a notice-and-consent regime serve if the most prominent consent mechanism is only regarded as a suggestion at best?**

   Notice-and-consent is not a sufficient model to protect consumers or allow for the convenient interaction with the services they wish to use in today's technology environment. Technology has moved past the point where "notice and consent" or "notice and choice" privacy models actually provided effective privacy protections.

   The United States needs a comprehensive federal privacy law that forces companies to move beyond reliance upon outdated concepts such as notice and consent and instead leverages traditional privacy principles to promote innovative data use while requiring organizations to safeguard personal data. Intel's proposed draft legislation does just that.

b. **How much faith should the failure of Do-Not-Track give us in the ability of the industry stakeholders to regulate themselves?**

   Self-regulatory measures like Do-Not-Track provide just one of many examples as to why a robust law with strong enforcement from the FTC and State Attorneys General is needed to create and uphold privacy protections.

c. **In your view, should this approach be abandoned, or would federal legislation requiring companies to respect the Do-Not-Track signal breathe new life into the mechanism?**

   Rather than focusing on specific mechanisms like Do-Not-Track, Intel believes in a federal law that creates strong rules and guidelines and requires companies to demonstrate responsible data practices that avoid uses of data

[6] *The "Do Not Track" Setting Doesn't Stop You from Being Tracked*, DUCKDUCKGO BLOG (Feb. 5, 2018), https://spreadprivacy.com/do-not-track.

[7] Ahiza Garcia, *What Apple Killing Its Do Not Track Feature Means for Online Privacy*, CNN (Feb. 13, 2019), https://www.cnn.com/2019/02/13/tech/apple-do-not-track-feature/index.html.

that creates risk for individuals. We believe our draft proposal accomplishes this.

4. **Given that California has enacted its own privacy legislation that will take effect next year, much of the discussion at the hearing centered on how a federal data privacy law will affect state-level efforts to regulate in the same space. However, most of our existing privacy statutes do not include provisions to overrule stricter protections under state law.[8] These preemption provisions are the exception rather than the rule, and became more prevalent starting in the 1990s in statutes like the Children's Online Privacy Protection Act of 1998, the CAN-SPAM Act of 2003, and the 1996 and 2003 updates to the Fair Credit Reporting Act.**

   a. **In your view, should a federal data privacy law preempt state data privacy laws? Why?**

   The United States needs a robust, harmonized, and enforceable framework that provides protections for individuals from state to state and encourages innovation to thrive. A non-harmonized patchwork of different state laws could cause companies to default to restrictive requirements, resulting in a decrease in likelihood of realizing the potential of new technology like artificial intelligence to improve lives. Put plainly: Intel believes in a strong, comprehensive law that promotes ethical data stewardship, not a set of laws that differ in their attempts to minimize harm.

   b. **In your view, should a federal data privacy law implement the requirements of the California Consumer Privacy Act as a floor? If not, please explain the most significant change you would suggest.**

   While CCPA has been a tremendous effort to drive the conversation around the need for strong privacy protections forward, we need a federal law that is stronger and better than CCPA and creates harmonized protections for all users.

   CCPA relies too heavily on models consistent with "notice and choice" and provides consumers the illusion that it's model of protection will give them more control over their data.

[8] The following statutes do not preempt stricter protections under state law: the Electronic Communications Privacy Act, the Right to Financial Privacy Act, the Cable Communications Privacy Act, the Video Privacy Protection Act, the Employee Polygraph Protection Act, the Telephone Consumer Protection Act, the Drivers' License Privacy Protection Act, and the Telemarketing Consumer Protection and Fraud Prevention Act.

While "notice and consent" or "notice and choice" model has attempted to promote individual participation for decades and has been a valuable tool to empower citizens and give them control over their data, it 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.

We need a law that does not rely on notice and consent or opt out mechanisms, but instead creates rules and guidelines around data use and puts the onus on companies – not consumers – to demonstrate responsible data practices and avoid the use of data that creates risk for individuals.

c. **The specific wording of a proposed preemption provision will invite considerable debate in Congress and, ultimately, will still require courts to interpret and clarify the provision's scope. Should the Federal Trade Commission have notice-and-comment rulemaking authority to aid in the statute's interpretation and to clarify which types of state laws are preempted? Or, alternatively, is case-by-case adjudication of multiple state privacy laws preferable? Would rulemaking authority obviate the need for Congress to solve each and every preemption issue in drafting the text?**

Intel's proposal grants rulemaking authority to the FTC, as well as calls for frequent reports from the FTC to Congress regarding the effectiveness of the law, including compliance, proposed modifications, and particularly, inconsistencies or overlaps in the overall US legal framework.

Rulemaking authority, in conjunction with frequent reporting, could not only suspend the need for Congress to solve each and every preemption issue, but also create opportunities to make other modifications as needed, as well as clarify where there may be gaps or rules in place that may no longer be necessary or provide a benefit to consumers. With frequent reporting, Congress can rely on the FTC to supervise inconsistencies and advise on how to avoid these gaps to properly and effectively carry out provisions of the law.

d. **The preemption language in, for example, the amendments to the Fair Credit Reporting Act was included as part of a heavily negotiated process in which consumers received a package of new rights in exchange for**

certain preemption provisions.[9] Rather than centering the federal privacy bill debate on the existence of a preemption provision, shouldn't our starting point be: "Preemption in exchange for what?" In other words, what basic consumer protections should industry stakeholders be willing to provide in exchange for preemption? Do the requirements of the California Consumer Privacy Act represent a good floor for negotiating preemption?

Companies need to be willing to provide privacy protections that allow for the innovative and ethical use of data and demonstrate that they have responsible practices that avoid data uses that create risk to individuals.

Intel's bill promotes just this: Removing burden from consumer and placing it on companies to provide clear, robust privacy protections. We need a law that is stronger and better than CCPA, which still places too much burden on the user.

5. **At the hearing, several witnesses indicated that opt-out requirements that permit users to tell companies not to process and sell their data are more protective of data privacy and more conducive to the user experience, since they do not impose the "take it or leave it" dynamic that opt-ins tend to create. In your view, are opt-outs preferable to opt-ins in terms of both data privacy and user experience? Why?**

   While an "opt-in" privacy regime is preferable to an "opt-out" one, Intel believes that these models still put excessive burden on individuals to understand the data lifecycle. The ever-changing technology environment shows that for instance, the use of notice and consent will be increasingly difficult in many data collection and creation contexts. For this reason, in our draft proposal we clearly define the fair information privacy principle of "use limitation" in permitted processing based on consent, or legal obligation, or consistent use and reasonable amount of privacy risk. This proposal is meant to empower organizations to process data without consent but does not represent a blank authorization, because it works in concert with the other substantive rights provided to individuals (access, correction, deletion, portability) and obligations on organizations, such as security safeguards and accountability approaches.

6. **At the hearing, several witnesses also indicated that the Federal Trade Commission, and perhaps state attorneys general, should have primary enforcement authority for data privacy violations. In your view, what additional authority and/or resources would the FTC need to perform this**

[9] The 1996 and 2003 amendments included, for example: new obligations on businesses to ensure the accuracy of reports, increased civil and criminal penalties, remedial rights for identity theft victims, and the right to free annual credit reports.

function effectively?

Intel’s draft proposal calls for increased but specific rulemaking authority for the FTC. The specific sections under which the FTC should create rules and explanatory language on the parameters of the rules can be found in our draft proposal at usprivacybill.intel.com.

Intel’s draft proposal recommends both increased legal and technical personnel within the FTC.

Intel’s draft proposal calls for at least an additional 250 personnel in attorney positions, and at least 250 additional personnel in project management, technical and administrative support positions in the Division of Privacy and Identity Protection within the Bureau of Consumer Protection.