On October 10, 2018, the Senate Committee on Commerce, Science, and Transportation ("Committee") convened a hearing entitled, "Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act." During the hearing, participants discussed potential approaches to federal data privacy, focusing on: (1) provisions of the European Union's ("EU") General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act of 2018 ("CCPA"); (2) potential effects of the CCPA and GDPR on consumers and businesses; (3) roles of federal agencies and self-regulation; (4) enforcement; (5) consumer consent; and (6) how to define personal and sensitive information. Participants included Committee members and witnesses: (1) Andrea Jelinek, Chair, European Data Protection Board; (2) Alastair Mactaggart, Board Chair, Californians for Consumer Privacy; (3) Laura Moy, Executive Director and Adjunct Professor of Law, Georgetown Law Center on Privacy & Technology; and (4) Nuala O'Connor, President and CEO, Center for Democracy & Technology ("CDT"). The hearing followed a similarly focused hearing held by the Committee on September 26, 2018, during which Committee Chairman John Thune (R-SD) announced that follow-up hearings would be held to solicit stakeholder views on federal approaches to U.S. privacy legislation. A summary of the hearing follows below.

## I. Member Opening Statements

***Committee Chairman John Thune (R-SD)*** noted the Committee's previous hearing on consumer data privacy and stated that during that hearing, representatives from several companies discussed steps their organizations have taken to address privacy and comply with the GDPR and CCPA. He highlighted that a new federal privacy law "will not be written by industry" and said the Committee will continue to solicit input from stakeholders. He characterized the GDPR and CCPA as "useful examples" and noted that Congress has in the past passed laws protecting information associated with children, healthcare, and finance. He said the Federal Trade Commission ("FTC") and Department of Commerce ("DOC") have "long-standing roles" related to privacy and cited incidents involving Cambridge Analytica and Google+. He stated that industry self-regulation is not sufficient and rules establishing a national privacy standard are needed. He observed that the most visible impact of the GDPR to consumers has been an increase in cookie consent banners and pop-up notices, and said benefits and "potential unintended consequences" of the GDPR and CCPA should be examined.

***Sen. Ed Markey (D-MA)*** said data-driven services treat data as a commodity and stated that consumers lack "reasonable means" to prevent companies from "mining" and using personal information for "intrusive" purposes. He said companies that are advocating for federal privacy legislation are doing so because they will soon have to comply with the CCPA in addition to the GDPR and because, he said, these companies would like federal law to preempt the CCPA and other laws that may be more "burdensome." Sen. Markey said that before discussing preemption, consumers should have "true privacy protections" that give individuals control over their personal information. He expressed support for a "strong" federal privacy regulation that gives consumers: (1) knowledge of how data is used and shared; (2) notice in the event that data is compromised; and (3) the ability to say "no" to entities that wish to collect personal information. He said these principles constitute a "starting point" and are included in S. 2639,

the "CONSENT Act."[1] He expressed support for federal law that would additionally: (1) prohibit companies from offering financial incentives in exchange for personal information; (2) disallow "take it or leave it" terms of service; (3) set forth a "privacy bill of rights," enabling consumers to access, correct, and delete personal information and stop companies from collecting data not needed to deliver a service; (4) require that data be secured; and (5) provide "special protection" to children and teens, particularly, he said, those between the age of 13 and 15, who he said currently lack protection. Sen. Markey said that to keep pace with technology, robust rulemaking authority should be granted to the FTC or another authority. He expressed confidence that federal consumer privacy legislation can be written in a bipartisan way.

## II. Witness Panel Opening Statements

***Andrea Jelinek, Chair, European Data Protection Board,*** explained that it is her job to ensure consistent application of the GDPR. She said the GDPR evolved from rules that have been in place in the EU for 20 years and said the GDPR could serve as an example to the United States as Congress determines how to address privacy. She highlighted accountability as a core principle of the GDPR and said the GDPR "relies heavily on businesses' capacity to self-regulate." Chair Jelinek explained that compliance and the ability to demonstrate GDPR compliance is the responsibility of organizations, and said investment in privacy creates new opportunities. She said the GDPR provides a "one-stop-shop mechanism," explaining that it establishes a single "interlocutor" for companies involved in in cross-border cases and renders valid throughout the EU all action taken by the "lead supervisory authority." Chair Jelinek noted that EU data protection authorities have adopted 18 sets of guidelines detailing "novel aspects" of the GDPR. With respect to enforcement, she characterized fines as a last resort and one of several enforcement tools. She said fines must be "effective, proportionate, and dissuasive."

***Alastair Mactaggart, Board Chair, Californians for Consumer Privacy,*** explained that Californians for Consumer Privacy sponsored a ballot measure that brought about the passage of the CCPA in June 2018. He stated that during the Committee's hearing on September 26, 2018, witnesses suggested the CCPA was rushed, poorly drafted, and should be preempted. Mr. Mactaggart said the CCPA was informed by conversations with tech experts and privacy advocates, only applies to data brokers and "large business with over $25 million in annual revenue," and is not antibusiness. He said the CCPA's key provisions include: (1) consumers' right to know what information companies have collected; (2) consumers' right to say "no" to businesses' sale of information, adding that the CCPA enables organizations to use a person's information to advertise to that person so long as the organization does not "resell" data to other entities if a person had rescinded permission; and (3) a requirement that businesses safeguard consumer data. Mr. Mactaggart stated that companies use people's "digital footprint[s]" to track them across the Internet and curate a "detailed profile" that enables companies to "take advantage of [a person's] life's circumstances." He stated that the CCPA: (1) was passed unanimously by both chambers of the California legislature; (2) would cover one in eight

[1] *See text of* S. 2639, the "Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act," *available at* https://www.congress.gov/115/bills/s2639/BILLS-115s2639is.pdf.

Americans; (3) consistently polled at 80% and above; and (4) evolved from a ballot measure supported by a petition signed by 629,000 California voters.

***Laura Moy, Executive Director and Adjunct Professor of Law, Georgetown Law Center on Privacy & Technology,*** said now is not the time for light touch regulation and highlighted four points. First, she said there are uses of information that are never permissible. She said data should never be used to amplify hate speech, target disinformation, or discriminate in housing, education, finance, employment, and healthcare. Second, she expressed support for notice and choice and called for "robust enforcement" by an expert agency with the authority to levy fines. Ms. Moy said state attorneys general should be empowered to enforce privacy. She added that FTC officials and staff have requested original fining authority and said Congress should consider including a private right of action in federal privacy regulation. Third, she said, any new privacy law must include a mechanism for shifting standards to keep pace with technology. Ms. Moy expressed support for "a floor, not a ceiling," which she said would enable states to pass privacy laws. She called for "robust rulemaking authority" to be granted to a designated regulatory agency. Forth, she stated, Congress should not use a "one-size-fits all" approach to address privacy on the Internet. Noting that there are many actors on the Internet, Ms. Moy stated that industry has asked for "regulatory uniformity" and said that if a uniform approach to Internet governance is taken, the "lowest common denominator" of consumer privacy will be achieved.

***Nuala O'Connor, President and CEO, CDT,*** said that baseline privacy protection should: (1) apply broadly to all personal data and all commercial entities that collect personal data; (2) recognize data subjects' rights, including the right to access, correct, and remove personal information—she said these provisions are included in the GDPR and CCPA—and such rights should be set forth such that businesses can comply; (3) prohibit the collection, use, and sharing of data that is not necessary to the performance of a service or delivery of a product; (4) expressly empower the FTC to investigate potentially discriminatory uses of data; and (5) be "clear on its face," provide information to the market, give the FTC resources and original fining authority, and permit state attorneys general to enforce the law and any implementing rules. In describing the importance of limiting the collection, use, and sharing of data to strictly specified purposes, Ms. O'Connor stated that under Section 5 of the FTC Act, it is generally considered "presumptively unfair" to use sensitive data—including geolocation, microphone, camera, children's, health, and biometric information—for "secondary purposes."

## III. Questioning

***Approaches to Federal Privacy Regulation.*** Chairman Thune asked what aspects of the GDPR and CCPA should and should not be incorporated in a federal privacy law. With respect to data collection, Ms. Moy expressed support for minimization and purpose limitation, and for EU data protection authorities' ability to assess fines under the GDPR. She said that consumers should not be penalized for not consenting to data collection. Ms. O'Connor characterized consent, notice, choice, access, portability, and deletion as "core values" of the CCPA and GDPR and said these values are "largely consonant." She stated that there is a lack of bright line rules and guidelines outlining what practices are permissible. Regarding the CCPA, Ms. O'Connor called for small entities to be covered to the same extent that large entities are covered and said second and third-party data use should be more clearly delineated. Sen. Tammy Duckworth (D-IL) stated that a DOC official recently said that it is too soon to evaluate the impact of the GDPR and CCPA. Ms. O'Connor said in reply that the GDPR and CCPA's provisions may be clear regarding notice and not regarding what data is and is not covered, and said it is too soon to judge the laws' "eventual outcome" and impact on business. Sen. Roger Wicker (R-MS) asked if there should be a single federal privacy standard and Ms. O'Connor said a federal law should do no less than the CCPA and echoed Sen. Markey, stating that it is too early to talk about preemption. Sen. Jerry Moran (R-KS) asked whether privacy rules should be based on the sensitivity of data and apply across the entire Internet ecosystem. In response to Sen. Moran and Sen. Catherine Cortez Masto (D-NV), Mr. Mactaggart stated that all information should be treated equally, and explained that information that was not considered sensitive in the past can be used in new ways now. He said the CCPA "draw[s] a line" on first-party information and Sen. Cortez Masto said it seems that under the CCPA it is up to individuals to determine what information is considered sensitive.

***Preventing Breaches and Misuse of Data.*** In response to Sen. Markey, Ms. Moy called for a federal privacy law to establish limits on the use of consumer information, stating that only data needed for business should be collected. Sen. Maria Cantwell (D-WA) said cyber hygiene is important and expressed concern about the use of data for purposes that differ from those for which data was collected. Ms. O'Connor stated that unexpected data use and transfers to third-parties are a matter of concern that extends beyond tech and telecommunications companies and encompasses information moving on and offline. In response to Sen. Maggie Hassan (D-NH), Ms. Moy said financial incentives exist that encourage companies to retain information for as long as possible. She explained that as technology evolves, new and yet unknown applications for stored information may be revealed. She stated that unless there are repercussions for retaining excess data, current storage practices will persist.

***Role of the FTC and Self-Regulation.*** In response to Sen. Brian Schatz (D-HI), Mr. Mactaggart expressed support for the FTC to be given privacy-related rulemaking authority. Ms. O'Connor stated that Section 5 of the FTC Act does not give enough "direct authority" to the agency, explaining that before the FTC can impose a fine, it must (1) identify a malicious or untrue statement in an organization's privacy policy; (2) take action and investigate; (3) issue a consent order; and (4) find the organization has violated a consent order. Ms. Moy noted that under the GDPR, a company can be fined up to 4% of its annual revenue and stated that a fine

recently imposed on Google by the FTC was not substantial. Sen. Cortez Masto noted that there are some data privacy cases that the FTC may not take up, which could be taken up by state attorneys general and expressed a belief in the possibility of role for self-regulation.

***CCPA.*** Chairman Thune and Sen. Schatz asked about industry-proposed revisions to the CCPA. Mr. Mactaggart explained that the language of the CCPA was taken from a ballot initiative that was carefully drafted, and said passage of the CCPA was rushed. Mr. Mactaggart noted that the CCPA grants rulemaking authority to the attorney general, and explained that granting rulemaking authority to the enforcement authority renders the measure flexible over time. He said that a measure that was recently passed to amend the CCPA removed a whistleblower provision. He said that the tech and telecom industry has tried to insert into recent amendment bills language that he said would have "gutted" the CCPA. Sen. Moran asked whether too much information is included in the CCPA's definition of personal information. Mr. Mactaggart said the language was derived from previous California legislation, explained that the objective was to ensure that information pertaining to individuals' devices was captured by the CCPA, and stated that if the definition turns out to be problematic, the state attorney general has the authority to provide clarification. In response to Chairman Thune, Mr. Mactaggart stated that he cannot see how the CCPA would prohibit customer loyalty programs and that the CCPA does not take issue with "first-party" data use. He said under the CCPA, companies cannot be coercive, unfair, or unreasonable in offering "different pricing mechanisms." Ms. Moy stated to Sen. Markey that financial incentives or penalties associate with individuals' consent to data collection and use are often not commensurate with the value of the information in question.

***GDPR.*** Sen. Hassan asked why the GDPR uses an "occurrence standard" and not a "harm standard" for consumer notification. Chair Jelinek replied that big tech companies are capable of providing notice to consumers and expressed support for the GDPR's 72-hour notification requirement. Chair Jelinek explained to Sen. Wicker that EU authorities sought to enact a single law that would apply to the entire EU, noting that from 1995 onward, the EU had a directive on privacy and the GDPR is an "evolution" of that measure. Chair Jelinek stated to Sen. Cortez Masto that before EU data protection authorities take enforcement action, the GDPR relies on self-regulation. In response to Chairman Thune, Chair Jelinek explained the process by which the EU data protection authorities address cross-border cases. She said the first step involves determining the member state that should have lead supervisory authority and whether and what other member states' data protection authorities care to contribute. Chair Jelinek said that the lead supervisory authority is responsible for investigating, serving as the interlocutor between the company and the data protection authorities, and drafting a decision on the case. She explained what may trigger involvement of the European Data Protection Board and how the draft decision is reviewed. Chairman Thune asked about GDPR compliance costs and Chair Jelinek said that during the Committee's previous hearing on privacy, the witness representing Google stated that Google spent thousands of hours of manpower on GDPR compliance. Chair Jelinek said that if this figure were divided by the number of employees working for Google, the cost of compliance would equate to a matter of roughly three hours per employee. She said that in response to GDPR, most tech companies have developed "robust" systems for consumers to exert more control over their personal data.

***Privacy Regulations' Effects on Business.*** Sen. Moran stated that consumers may be less likely to consent to a lesser-known company's request to collect data and said Mr. Mactaggart has previously criticized the GDPR for requiring opt-in consent. He and Sen. Todd Young (R-IN) expressed concern that the GDPR and CCPA may advantage incumbents and negatively affect small businesses. Chair Jelinek said a startup can implement privacy by design and default from day one and said that complying with a single framework that applies regardless of the EU member state within which a company operates makes certain aspects of business easier for new and small companies. Mr. Mactaggart stated that to prevent the CCPA from stifling small companies, it imposes a threshold of $25 million in annual revenue. He said the CCPA gives consumers choice regarding whether to permit the sale of data and is "silent on the collection side" so, he said, startups can compete. Ms. Moy said data portability can help new market entrants. Ms. O'Connor said that small businesses should be included in privacy laws' provisions, noting that Cambridge Analytica was a small business and stating that loss of data by a small business can do as much damage as loss of data by a large business. Sen. Moran asked about the impact of GDPR enforcement action on small businesses and Chair Jelinek stated that EU data protection authorities issue warnings and that fines are assessed in proportion to "the nature of the business" and the nature of infringements, and are not dependent on size.

***Children's Privacy.*** Sen. Markey noted himself as the author of the Children's Online Privacy Protection Act ("COPPA") and said the CCPA requires affirmative consent to collect information from 13-16 year olds. He asked whether federal privacy law should include "special protections" for children ages 13, 14, and 15, and Mr. Mactaggart and Ms. Moy answered "yes." Sen. Markey asked whether witnesses would support an "eraser button" for children. Ms. Moy and Mr. Mactaggart noted that this feature may have implications with respect to the First Amendment, said they believe these implications can be reconciled, and expressed support for an "eraser button." In response to Sen. Tom Udall (D-NM), Ms. O'Connor and Ms. Moy said COPPA has been effective over time and said additional protections for children may be needed. Regarding the role of platform owners and apps' compliance with COPPA, Ms. Moy noted that there are incentives for platforms not to have knowledge of whether apps are directed towards children and said this is a "gap" that should be fixed.

***Proposed Legislation.*** Sen. Klobuchar asked about several provisions of S. 2728, the "Social Media Privacy Protection and Consumer Rights Act of 2018," which she and cosponsor Sen. John Kennedy (R-LA) introduced.[2] Chair Jelinek expressed support for the principle of consent and a 72-hour notification window in case of a breach. Ms. Moy expressed support for state attorneys general's authority, stating that they can take action in cases that are not expansive enough to trigger FTC involvement. She said state attorneys general do an effective job consulting and helping companies understand what their obligations are. Sen. Richard Blumenthal (D-CT) stated that he is working on a bill that would establish a floor and not a ceiling for data privacy and protection, and expressed support for privacy by design and a "privacy bill of rights" incorporating GDPR and CCPA principles.

[2] *See text of* S. 2728, "Social Media Privacy Protection and Consumer Rights Act of 2018," *available at* https://www.congress.gov/115/bills/s2728/BILLS-115s2728is.pdf.

*  *  *

Please contact us with any questions.