On September 26, 2018, the U.S. Senate Committee on Commerce, Science, and Transportation ("Committee") convened a hearing entitled, "Examining Safeguards for Consumer Data Privacy." During the hearing, participants discussed a range of topics associated with federal data privacy legislative proposals, including: (1) provisions of the European Union ("EU") General Data Protection Regulation ("GDPR") and California Consumer Privacy Act of 2018 ("CCPA"); (2) state law preemption; (3) Federal Trade Commission ("FTC") authority; (4) personally identifiable information ("PII"); (5) default opt-in and opt-out consent; (6) third party data sharing and digital advertising; and (7) children's privacy protection. In his opening remarks, Chairman John Thune (R-SD) stated that the Committee would hold follow-up hearings on consumer privacy, one of which he said would take place in October and feature testimony from California privacy advocate, Alastair Mactaggart, and the European head of GDPR enforcement, Andrea Jelinek. In his concluding remarks, Chairman Thune entered into the record, with unanimous consent, letters submitted by: (1) the Association for National Advertisers; (2) the Interactive Advertising Bureau; (3) the Internet Association; (4) the National Association of Federally Insured Credit Unions; (5) Privacy for Cars; and (6) the U.S. Chamber of Commerce. The hearing featured the following invited witnesses: (1) Len Cali, Senior Vice President—Global Public Policy, AT&T Inc.; (2) Andrew DeVore, Vice President and Associate General Counsel, Amazon.com, Inc.; (3) Keith Enright, Chief Privacy Officer, Google LLC; (4) Damien Kieran, Global Data Protection Officer and Associate Legal Director, Twitter, Inc.; (5) Guy ("Bud") Tribble, Vice President for Software Technology, Apple Inc.; and (6) Rachel Welch, Senior Vice President, Policy & External Affairs, Charter Communications, Inc. A summary of the hearing follow below.

I. Member Opening Statements

Committee Chairman John Thune (R-SD) noted that: (1) in September 2017, news of the Equifax data breach broke and thereafter the Committee held a hearing that featured Equifax's former chief executive officer ("CEO"); (2) in April 2018 the Committee held a joint hearing with the Senate Committee on the Judiciary that featured Facebook CEO Mark Zuckerberg; (3) in May 2018, the EU's GDPR took effect; (4) in June 2018, the Committee's Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security held a hearing to discuss matters associated with Cambridge Analytica's reported improper access to Facebook users' data; and (5) on June 28, 2018, the CCPA, which Chairman Thune said will take effect in January 2020 and includes "privacy mandates and severe penalties for violators," was signed into law. With respect to federal data privacy legislation, he stated that the question is not whether legislation is necessary and rather, he said, what form it should take. He said the hearing's witnesses are industry leaders that have different approaches to data collection, use, and protection, and said the Committee seeks to examine how privacy laws, such as the GDPR and CCPA, affect the companies represented by the witnesses. He said Congress will not rush to action before hearing other stakeholders' views, and noted that the Committee will convene a second hearing on consumer data privacy, at which he said Alastair Mactaggart and Andrea Jelenik have agreed to testify.

Ranking Member Bill Nelson (D-FL) observed that this is not the first hearing held by the Committee to address privacy matters and noted that consumers have been impacted by breaches and misuse of personal data.

II. Witness Panel Opening Statements

Len Cali, Senior Vice President—Global Public Policy, AT&T Inc., said there is need for clear national rules regarding how data is used, shared, and protected and said such rules should empower consumers and not impede "consumer benefits that flow from responsible data use." Mr. Cali highlighted three points. (1) Information collection is widespread and takes place when consumers engage in a variety of activities (*e.g.*, shopping at brick and mortar stores, driving cars, using Internet services, etc.). He said Internet service providers ("ISPs") collect less information than consumers may expect because encryption between mobile devices and websites conceals a large quantity of information. (2) Different types of information can be collected (*i.e.* information provided by a consumer, information collected through observation, and information that is inferred). He said some information is private and individuals' perception of what is private varies. (3) The same information (*e.g.*, geolocation information) can be put to different uses and associated risks and benefits depend upon use. Mr. Cali said rules of the road should be understandable and apply to all firms, regardless of what technology is used, and expressed support for a "solution" that is straightforward, uniform, and employs a risk-based approach that accounts for data use and sensitivity. He said the FTC's existing privacy framework is good and can be improved, and highlighted the importance of establishing a single federal framework that codifies the FTC's role as the nation's privacy regulator.

Andrew DeVore, Vice President and Associate General Counsel, Amazon.com, Inc., offered the following "policy perspectives" for consideration: (1) legislation addressing privacy should include all stakeholders; (2) legislation should ensure that additional overhead and administrative costs "produce commensurate privacy benefits"; (3) the CCPA gives consumers greater control over their data, includes some provisions that he said do not promote best privacy practices, and should be examined by Congress to identify its potential unintended consequences; and (4) focusing on consumers facilitates finding solutions. Mr. DeVore noted that Amazon is aligned to comply with the GDPR, and stated that to become compliant, significant resources that he said could have been put towards innovation were directed towards administrative tasks.

Keith Enright, Chief Privacy Officer, Google LLC, said that Google supports efforts to codify baseline privacy in law and has set forth "principles for a responsible data framework," that he said he hopes will contribute to the Committee's work: (1) transparency; (2) user control; (3) portability; and (4) security. Regarding transparency, he said that providing services free of charge is key to Google's mission and that free services are supported by advertising. He noted that Google does not sell personal information and aims to be upfront about how and why data is collected and used. He said Google has launched privacy and security tools that aim to help users control apps' access to Google account data, enable users to delete Google activity, disable personalized ads, and download copies of their information. Mr. Enright said data portability best serves users and characterized it as a means of driving innovation and competition.

Damien Kieran, Global Data Protection Officer and Associate Legal Director, Twitter, Inc., expressed support for efforts to build a privacy framework that supports innovation, protects privacy, and provides transparency and meaningful consumer control over how, when, and what data is collected, used, and shared. He said Twitter accounts are public by default and explained that Twitter collects information though individuals' use of the platform. He said Twitter's privacy policy is contained in a single document that includes graphics and makes use of technology to explain what data is collected and how it is used and shared. He expressed interest in improving how Twitter conveys this information. He explained that Twitter provides "granular" privacy controls, a "single master switch" that can disable all personalization, and said the Your Twitter Data tool enables users to view and download all information associated with their accounts, including username, phone number, inferred interests, and more.

Bud Tribble, Vice President for Software Technology, Apple Inc., noted Apple's support for comprehensive privacy legislation that enables innovation, said Apple believes that privacy is a fundamental human right that should be supported by social norms and laws, and said putting users in control of how their personal data is shared is central to privacy. Mr. Tribble stated that, to Apple, "privacy by design" entails limiting data collection, making data less identifiable, and to the extent possible, processing data on devices instead of transferring data to servers. He noted that Apple does not combine information into a single customer profile across services when data is sent to servers, strives to explain data processing in a manner that is specific and transparent, and takes measures to prevent exploitation by bad actors.

Rachel Welch, Senior Vice President, Policy & External Affairs, Charter Communications, Inc., described Charter Communications as a high-speed broadband, video, and voice services provider. She noted that sectoral rules legally protect certain types of data, including financial and health information, and said other types of data are being sold and tracked without specific protections. Ms. Welch called for uniform federal privacy protections that require meaningful consent regardless, she said, of where consumers go online. She said this framework should focus on: (1) consumer control, which she said is best effectuated by requiring opt-in user consent; (2) transparency; (3) parity, noting that a framework should apply to the entire Internet ecosystem without regard for whether a service is free or paid; (4) uniformity; and (5) security, which she said should protect against all unauthorized access. Ms. Welch expressed support for the adoption of legislation based on these principles and designated the FTC as the appropriate online privacy and data security oversight and enforcement agency.

III. Questioning

State Law Preemption. In response to Sen. Deb Fischer (R-NE), Mr. Tribble stated that comprehensive federal legislation is needed to protect consumers. Sen. Mike Lee (R-TX) discussed the nature of the Internet, noted that Congress' regulatory authority covers matters of interstate commerce, and asked to what extent federal legislation should preempt state law. Mr. Cali replied that because the Internet is interstate, it should be regulated by Congress and, noting that there may be areas (*e.g.*, consumer protection) where Congress should not impede state law, said federal regulation should be exclusive. Sen. Jerry Moran (R-KS) noted that he, Sen. Roger Wicker (R-MS), Sen. Richard Blumenthal (D-CT), and Sen. Brian Schatz (D-HI) are collecting

feedback from a range of stakeholders and recently sent a letter to Commerce Secretary Wilbur Ross regarding how privacy should be addressed. In response to Sen. Moran and Sen. Wicker's questions, Mr. Cali, Mr. Enright, Ms. Welch, and Mr. Kieran expressed support for preemption. Mr. Kieran added that preemption constitutes part and not the whole of federal legislation and Ms. Welch highlighted the importance of opt-in consent. Mr. Tribble stated that Apple supports federal preemption so long as the standard set by such legislation adequately protects consumers, and Mr. DeVore expressed qualified support for including preemption in federal legislation, stating that a "patchwork of state laws" will not protect privacy. Sen. Schatz stated that Congress would not replace the CCPA, which he described as "progressive," with a federal law that is not progressive and Sen. Ed Markey (D-MA) stated that Congress does not want to override "strong" laws.

Privacy Approaches. Sen. Moran asked about the importance of an approach based on the sensitivity of data and the witnesses agreed that an approach based on sensitivity is important. Sen. Wicker asked whether edge providers should be subject to the same privacy requirements to which ISPs are subject, and all six witnesses answered in the affirmative. Mr. Enright added that the FTC's harms-based approach to enforcing privacy is best and highlighted the principles of user control, transparency, portability, and security. Mr. Cali noted that in many cases, a line cannot cleanly be drawn distinguishing services that are subscription based and services that are ad-supported and free to users, and said that these models and hybrid models collect consumer data, some of which he stated is sensitive and some of which he said is not. Sen. Tammy Baldwin (D-WI) asked if comprehensive privacy legislation should apply equally to all companies, regardless of a company's business model, and Mr. Tribble stated that it should. Mr. Enright explained to Sen. Gary Peters (D-MI), who asked about PII in the context of facial recognition, that Google defines PII as data elements that directly or specifically identify and individual user and noted that the definition of PII under the GDPR is overly broad in certain circumstances. In response to questions posed by Sen. Catherine Cortez Masto (D-NV), witnesses agreed that it would be helpful to establish a working definition for PII. Mr. Enright stated that a clear definition of PII would assist in compliance with regulations and Mr. Kieran stated that defining PII would help international interoperability. In response to Sen. Cortez Masto, Ms. Welch expressed support, and other witnesses expressed concern, regarding default opt-in privacy settings. Mr. Cali stated that requiring opt-in consent to all data collection would restrict the use of non-sensitive data and risk hurting innovation. Mr. Enright expressed support for an approach he characterized as "balanced" and Mr. Kieran noted that if an opt-in requirement were to apply to all data, it would restrict Twitter from using an individual's ISP address to infer the user's language and obtain permissions for use of the service.

GDPR and CCPA. Chairman Thune asked what provisions of the CCPA and GDPR should be emulated. Mr. Cali explained that the CCPA establishes opt-out consent by default, which he expressed support for and said underscores the value of data use. He added that the universal applicability of the CCPA and GDPR is helpful. He characterized the CCPA's nondiscrimination clause as ambiguous and said it may deny consumers benefits they receive for sharing information (*e.g.*, grocery story benefits cards). He said the CCPA's notice and consent process tends to be "serial" and may restrict data, and stated that AT&T will seek revisions to the CCPA's notice, consent, and nondiscrimination obligations and will seek changes to its

implementation period, which he described as "tight." Mr. Cali said limits the GDPR places on data sets may impede development of blockchain and artificial intelligence ("AI") technology. Sen. Lee expressed concerns associated with GDPR compliance costs and Mr. Enright and Mr. Cali explained that there are significant compliance burdens, which Mr. Cali said appear to have led some smaller-sized companies to exit the European market and appear to have strengthened incumbent platforms. Mr. Cali said GDPR provisions regarding consumers' right to access, deletion, and portability have caused fraud and security concerns, and stated that it has yet to be determined whether data portability will "enhance competition or embed incumbents." Sen. Blumenthal questioned whether "voluntary rules" and self-regulation protects consumers. He asked—without pausing for responses from witnesses—why Congress should not adopt the CCPA's framework, which he said is consistent with the EU's privacy standards, observing that the companies represented by the witness panel have not withdrawn from California or the EU and seem to be able to comply with rules in these jurisdictions.

Introduced Legislation. Sen. Markey noted his introduction of S. 2639, the "Customer Online Notification for Stopping Edge-provider Network Transgressions ("CONSENT") Act," said the bill would support consumers' right to know what information is gathered about them, and asked witnesses if they would support a provision that would require explanation of how consumer information is used, shared, retained and sold.[1] All witnesses answered "yes." Sen. Amy Klobuchar (D-MN) asked whether witnesses would support a provision in S. 2728, the "Social Media Privacy and Consumer Rights Act of 2018," that she said would require companies in the event of a data breach to notify impacted consumers within 72 hours.[2] None of the witnesses expressed support for this provision. Sen. Klobuchar stated that S. 2728 would enable consumers to easily withdraw consent, which Mr. Kieran stated is enabled by Twitter. She said S. 2728 would require online platforms to provide "plain language" disclosure of data practices, which Mr. Enright and Mr. Kieran stated their platforms currently strive to provide.

FTC Authority. Ranking Member Nelson asked whether witnesses would support giving the FTC additional resources to protect consumers. Mr. Enright stated that in Google's experience, the FTC has been a "rigorous and effective" enforcement agency with respect to privacy. Other witnesses expressed qualified support, stating that the FTC should have the resources it needs and that requisite resources should be included as part of a comprehensive privacy measure. Ranking Member Nelson asked if the FTC should be granted additional legal authority to protect privacy. Mr. Tribble stated that a potential legal mechanism should be informed by what is currently working, Mr. DeVore emphasized that details matter, and Mr. Cali noted that it is the responsibly of Congress to establish "guardrails" and designate authority to the FTC. In response to Sen. Wicker and Sen. Moran, all witnesses agreed that the FTC is the appropriate agency to enforce federal privacy standards, Mr. Tribble qualifying his "yes," noting that there may be additional federal privacy standard enforcement "mechanisms." Sen. Schatz stated that laws that stand the test of time "empower the expert agency" to promulgate rules, and

[1] *See text of* S. 2639, "Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act," *available at* https://www.congress.gov/115/bills/s2639/BILLS-115s2639is.pdf.
[2] *See text of* S. 2728, "Social Media Privacy and Consumer Rights Act of 2018," *available at* https://www.congress.gov/115/bills/s2728/BILLS-115s2728is.pdf.

expressed support for granting the FTC rulemaking authority under the Administrative Procedure Act. Mr. Cali, Mr. Enright, and Mr. Tribble expressed qualified agreement, and Mr. DeVore stated that details are critical. Sen. Schatz asked if the FTC should have the authority to issue a fine in the first instance of violation and witnesses gave a range of qualified answers.

Digital Advertising and Third Party Data Access. Sen. John Tester (D-MT) expressed concern associated with the sale of individuals' personal information for the purpose of targeted advertising. Mr. DeVore explained that Amazon runs several services he described as "information dependent" and said Amazon is not in the business of selling personal information. Mr. Enright said that Google offers an advertising platform that enables publishers to advertise to users without passing personal information to third parties and said Google does not sell personal information. Mr. Enright explained to Chairman Thune that Google enables users to grant Gmail account access to third parties and that Google does not give third party app developers access to Gmail accounts. Mr. Enright noted to Rep. Peters that through My Google, users can view their Internet activity, including ads they have interacted with, and can opt out of targeted advertising.

Children's Privacy. Sen. Markey expressed concerns associated with Amazon's facial recognition technology and compliance with the Children's Online Privacy Protection Act ("COPPA"). Sen. Tom Udall (D-NM) cited reports that he said allege that thousands of apps collect children's information in violation of COPPA and called on the Committee to hold a hearing on a future framework to protect children's privacy.

Political Ads. Sen. Klobuchar noted her introduction of S. 1989, the "Honest Ads Act," and stated that she views Russian meddling, which she said included use of individuals photos without consent, as a matter of both privacy and security.[3] Mr. Enright said that Google supports the goals of the measure and will work with staff.

* * *

Please contact us with any questions.

[3] *See text of* S. 1989, "Honest Ads Act," *available at* https://www.congress.gov/115/bills/s1989/BILLS-115s1989is.pdf.