Responses to Written Questions Submitted by Honorable Jerry Moran to Leonard Cali

Question 1. Efforts to draft meaningful federal legislation on consumer data privacy will heavily rely upon determinations of what types of personally identifiable data are classified as "sensitive" and what are not. While some have suggested that expanded FTC rulemaking authority is necessary to flexibly account for new types of data sets coming from innovative technologies, I have concerns that excessive rulemaking authority could lead to frequent reclassifications of the types of data with ensuing liability adjustments. Do you have suggestions on how to best identify "sensitive" personally identifiable information?

Response. The potential for abuse of excessive rulemaking authority is a legitimate concern. Congress should identify the categories of sensitive personally identifying information that deserve heightened protections – e.g., Social Security numbers, financial, health, information about children, and precise geolocation information.[1] By providing clarity in the statute itself, Congress would provide consumers and industry needed certainty as to the statute's requirements, while also giving the FTC clear direction of its intent. Properly drafted, these statutorily-defined categories of sensitive information should be able to capture future technological and market developments without inadvertently providing undue discretion to alter the fundamental Congressional framework.

Question 2. NTIA issued a request for comment on ways to advance consumer privacy without harming prosperity and innovation. I commend the administration for their attention to this important issue. The "High Level Goals for Federal Action" that NTIA is seeking comments for includes inter-operability and the development of a regulatory landscape that is consistent with the international norms and frameworks in which the U.S. participates. How do you foresee federal legislation affecting cross-border data flows?

Response. Federal legislation should have a positive effect on cross-border data flows and avoidance of data localization laws that impede the free-flow of consumer data. By adopting a national privacy law, the U.S. can demonstrate privacy leadership and build global trust in its mechanisms to protect consumers' personal data. This should help the U.S. in the ongoing EU Privacy Shield negotiations to combat misperceptions concerning U.S. privacy law. We too commend NTIA and other U.S. Government efforts to ensure that the cross-border transfer mechanisms in which the U.S. participates, such as the APEC Cross-Border Privacy Rules system, are easily accessible to any U.S. company that seeks to benefit from them and are promoted more widely at the international level.

Question 3. Also included in NTIA's request for comments, how should the U.S. government encourage more research and development of products and services that improve privacy protections?

Response. The federal government can contribute to innovation in and the development of security solutions, which can also help protect privacy, in a several ways. For example, the

[1] U.S. Federal Trade Commission, *Protecting Privacy in an Era of Rapid Change*, 47 (2012).

government can: 1) Fund consumer education initiatives and grant programs that promote development of innovative security solutions; 2) promote government investment in technologies for federal systems; and 3) develop federal policies and approaches to security that are risk-based and voluntary (as opposed to prescriptive regulatory approaches). Such initiatives can help promote innovation in cybersecurity and data security technologies and avoid diverting resources away from innovation and security and towards checklist compliance. The government can also help by: 4) convening multi-stakeholder efforts to research and develop solutions designed to access, query, hold and secure data with privacy in mind; and 5) providing tax, student loan and tuition incentives for students to pursue careers in cybersecurity and for software engineers with cybersecurity expertise to participate in open source software forums.

Question 4. Your testimony included the suggestion of providing "safe harbor" protections in federal legislation to companies utilizing voluntary privacy programs and standards through public-private collaboration. Could you please explain how these types of mechanisms could be used to enable companies to adapt rapidly changing technology and market developments?

Response: The Administration, through NTIA, is actively working with stakeholders on a set of privacy principles that would provide an alternative to the GDPR's prescriptive approach. We commend the Administration for these efforts and support the high-level goals suggested in NTIA's September 25, 2018 Request for Comments. A number of private organizations, including the U.S. Chamber and the Business Round Table, are also working on privacy principles that could form the basis for federal legislation. In addition, there are numerous examples of successful voluntary industry privacy programs, such as the Digital Advertising Alliance's (DAA's) Advertising Choice program. Safe harbors based on voluntary industry standards are flexible and can adapt rapidly to changing technology and market developments.

These types of privacy programs could serve as the basis of a safe-harbor in legislation, which would create stronger incentives for companies to participate. Adherence to such guidelines could shield companies against potential enforcement actions, similar to the Children's Online Privacy Protection Act.[2]

[2] 16 C.F.R. § 312.11, Children's Online Privacy Protection Rule.

Responses to Written Questions Submitted by Honorable Shelley Moore Capito to Leonard Cali

Question 1. According to a study by Pew Research, only 38% of consumers know how to limit what information they give online. Consider me among those consumers who do not know what is being collected and how to keep my information to myself. Even with privacy settings and assurances that my data is not being collected and used without my consent, I still have concerns.

I believe the root of this issue is transparency and consumer confidence. What are your companies doing to increase the transparency when it comes to the type of data you collect?

Response. AT&T is committed to being transparent with our customers about our privacy and data collection practices. We do so in a number of ways. For example, AT&T Communications' Privacy Policy[3] describes in plain language the data we collect and how we use it. We also inform customers of their choices and controls with respect to how their personal information is used. Of course, we routinely review our policy with an eye toward making it simpler, clearer and reflective of planned changes in practice. AT&T was one of the first companies to adopt a simpler, plain-language privacy policy. The policy includes a short overview. Then, to better explain our policy, we also provide customers more detailed answers to frequently asked questions. In one of those answers we list the types of customer information we collect. The Privacy Policy web page also includes a short video highlighting AT&T's privacy practices. If a consumer has a question, the AskPrivacy mailbox is a one-click option to submit a question directly to AT&T's Chief Privacy Office, which monitors and responds promptly to requests.

AT&T also provides individuals with information about how to exercise their choices under the DAA's Advertising Choices program, which establishes a standardized icon for online ads delivered by many other ad networks. These types of industry privacy programs are an effective way to enhance transparency and consumer confidence. Finally, since 2014, AT&T has issued a Transparency Report (found at att.com/transparency) that identifies the number and types of U.S. government demands for customer information received in criminal, civil, and national security matters, as well as emergency situations and international demands related to global operations for customer information and web-site blocking.

Question 2. What difficulties have your companies faced when developing more transparent privacy policies?

Response. Consumers and policymakers want companies to provide short, easy-to-read explanations of their privacy policies. However, the goal of "simplicity" is often in tension with legal requirements that demand more detailed disclosures. We welcome input from policymakers on how best to inform customers of our privacy practices without overwhelming them with overly-detailed disclosures. Congress can help improve transparency by establishing uniform transparency requirements that eliminate a patchwork of state-specific or service- specific privacy policy disclosures (e.g., FCC disclosure requirements for CPNI). Differing disclosure requirements increase the complexity of company privacy policies and lead to consumer confusion.

[3] https://about.att.com/sites/privacy_policy. Referred to herein as "AT&T Privacy Policy."

Question 3. West Virginia has a high elderly population that is rapidly increasing as baby boomers retire. I am positive that a lot of my elderly constituents are among those individuals who do not know how to limit their online information.

What are some of the measures your companies are doing to teach consumers – and specifically older consumers – about what data they share on your platforms?

Response. AT&T values its senior customers and we work hard to ensure that our privacy policy meets their needs. We refer you to our response to your first question, which summarizes the multiple ways AT&T's Privacy Policy provides customers information about the data we collect and how we use it. We believe our simple, plain-English privacy policy provides all consumers, including seniors, straight-forward information on our data collection and use practices.

In addition, AT&T has a long history of working with local and national organizations to help consumers, including seniors, get the most out of technology. For example, Our Digital You® program provides tips, tools and information to help consumers get online safely and securely. The Digital You website, created in collaboration with Common Sense Media, LGBT Tech, National Consumers League, iKeepSafe, Family Online Safety Institute and other experts, is a resource that provides digital newcomers, parents, youth, people with disabilities, and community leaders with information on the devices they use and how to maintain privacy, safety and security in an increasingly connected world. The website addresses topics such as preventing cyberbullying, managing your online presence, protecting your computer and your data, and parenting in the digital age. In 2017, the Digital You campaign held more than 110 training events for people of all ages across the United States. We also participate in and host community summits, panels and educational events that help consumers of all ages learn how to safely and efficiently manage technology.

AT&T is also helping to narrow the technology-skills gap for older adults by supporting the Oasis Institute's Connections program. Our support enables Oasis to continue expanding and updating the Connections technology training program, which helps adults build skills and confidence using computers, the internet and portable devices. Oasis Connections programs are offered in 40 cities and have enrolled more than 120,000 people since 2000. In 2017, the curriculum expanded to include 3 additional cybercrime prevention classes.

Question 4. I know advertising through data collection has a monetary value, and appreciate the business model, however, I find it hard to know what is being collected and how I can keep my information to myself. Even with privacy settings and assurances my data is not being used without my consent, I still have concerns.

Please explain how your business model allows both data to be used to make suggested recommended purchases on your site? As well as how you use that data to target ads to consumers? And how do you do that while protecting personal data?

Response. AT&T is committed to ensuring that we describe the personal information we collect and explain how we use it. AT&T's Privacy Policy, for example, explains that we use customer information to deliver customized content, or advertising, such as personalized offers for

products and services that may be of interest to a customer. AT&T's offer of customized advertising prioritizes the protection of customer personal data.

For example, we and our business partners may match information using double-blind procedures to ensure that no personally identifiable information is exchanged between companies, but that things like interest categories can be identified for purposes of ad delivery. We also combine information into aggregate "audience segments." These segments are based on particular interests and/or factual characteristics that everyone in the audience segment is likely to share. We might use that information to send customers advertisements that are relevant to those interests or characteristics.

In terms of security safeguards, as a communications provider, we've established electronic and administrative safeguards designed to make the information we collect secure. Some examples of these safeguards, which are highlighted in the AT&T Privacy Policy, include the following:

We've implemented various technology and security features and strict policy guidelines to safeguard the privacy of customers' personal information. Some examples are:

Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;

Applying encryption or other appropriate security controls to protect customer personal information when stored or transmitted by us;

Limiting access to customer personal information to only those with jobs requiring such access; and

Requiring caller/online authentication before providing account information.

Our privacy principles are reflected in our values. For example, the AT&T Code of Business Conduct (COBC) requires covered employees to follow the laws, rules, regulations, court and/or administrative orders that apply to our business - including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of customer records. We take this seriously and employees who fail to meet our standards are subject to disciplinary action. That includes dismissal.

Question 5. How can Congress ensure that data collected is used responsibly without shutting down the collection of data completely?

Response. We suggest that policy makers look to the FTC's existing privacy framework, which applies a risk-based approach to protecting customer data.[4] The FTC recognizes that not all data is the same. On the one hand, the FTC identifies categories of "sensitive" data that deserve additional protections: Social Security numbers, financial information, health information, information about children, and precise geolocation information. Subject to limited exceptions, the FTC requires opt-in consent prior to collecting this data and using or sharing it for marketing purposes. On the other hand, additional consent generally is not required to use non-sensitive

[4] U.S. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (2012).

data, provided that companies are transparent with consumers about their data collection and use practices and offer consumers the opportunity to opt-out of certain uses. This balanced approach has provided customers strong protections without stifling innovative and responsible uses of data. While the FTC framework has served us well, it can be improved upon. We look forward to working with the Committee on legislation that builds upon the FTC's successful framework.

Question 6. In April, the European Union (EU) passed the General Data Protection Regulation (GDPR) in order to protect personal data and uphold individual privacy rights. These new regulations have created uncertainty for U.S. firms, despite several already coming into compliance.

Innovation is important to small businesses, especially in rural America. The new European standards have created massive hurdles for these businesses to be in compliance. Many small companies in Europe are already expressing an inability to afford the legal consequences. For example, if a rural grocery store advertises online and provides a link to coupons. Under the GDPR compliance rules, this simple practice can result in expensive legal consequences.

For those who do business in Europe, do you think GDPR has the potential to have negative impacts on rural small businesses in Europe?

Response. Yes. The GDPR took effect on May 25, 2018, and its impact is still being assessed. Thus far, reporters have documented cases of smaller U.S. based companies that chose to pull out of the European market, to pull advertising from the EU, or to block European customers from accessing their Web sites and services.[5] GDPR has reportedly prompted hundreds of websites to go dark in Europe, and U.S. startups Payver, Steel Root, Unroll.me, and Drawbridge are among those to exit the EU completely. Owners of small businesses, such as food distributors and beauty salons, have expressed concerns that they lack the resources needed to understand the impact of the new rules on ordinary practices such as emailing customers and operating Web sites.[6] Dozens of American media and news outlets have also gone dark in Europe.[7] Time will tell, but GDPR could inadvertently reduce competition by reinforcing the power of existing platforms that have the resources to comply.

Question 7. California has already passed a sweeping consumer protection law that threatens established business models throughout the digital sector. I appreciate the industry taking the initiative in creating a framework, in addition to the privacy principles released by the US Chamber of Commerce.

---

[5] Hannah Kuchler, "US small businesses drop EU customers over new data rule," Financial Times, 5/24/18 (reporting that small U.S. companies Payver, Steel Root, Unroll.me, and Drawbridge are among those to exit the EU following GDPR's entry into force).

[6] See, e.g., BBC, "GDPR: Data protection overhaul hits small businesses," May 22, 2018; MinuteHack, "Small Businesses 'Wasting Time and Money' on GDPR," May 22, 2018.

[7] Alex Hern and Martin Belam, "L.A. Times among U.S.-based news sites blocking EU users due to GDPR," The Guardian, May 25, 2018, available at: https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news- websites-eu-internet-users-la-times.

As we begin discussing the appropriate position of the federal government, can you describe what actions we should investigate more closely for any potential national framework?

Response. AT&T welcomes the Administration's efforts, through NTIA, to work with stakeholders on a set of privacy principles and goals that would provide an alternative to California's approach and be used as a starting point for federal legislation. The California Consumer Privacy Act was pushed through the legislature in 7 days, without meaningful input from the public, privacy advocacy groups, or industry, and its full impact remains unclear. In addition to the U.S. Chamber of Commerce initiative, we are active in the Business Round Table's efforts to outline the fundamentals of a privacy law. The principles put forth by these and other organizations are generally based on international standards, such as the APEC Cross-Border Privacy Rules (CBPR) and the OECD Privacy Framework, which are accountability-based frameworks that facilitate the cross-border flow of data. The FTC's existing privacy framework also is consistent with these international standards and provides a good starting point for federal privacy legislation, as discussed above.

Question 8. Who, in your opinion, is the appropriate regulator to oversee any framework and why?

Response. We believe the FTC is the proper regulator for privacy. The FTC has decades of experience regulating consumer privacy. And it has been an aggressive "cop on the beat," having brought more than 500 enforcement actions for privacy and data security violations, including cases involving major internet and telecommunications companies. The FTC has the added benefit of broad oversight across industry sectors.

Responses to Written Questions Submitted by Honorable Todd Young to Leonard Cali

Question 1. GDPR establishes a right of data portability, which some believe is key to driving new innovation and competition within the emerging data ecosystem. Others are concerned that data portability rights, depending on how crafted, could further entrench incumbent companies.

Response. There are serious questions and considerations associated with any proposal that would allow customers to "port" their data from one company to another. First, there are serious data security and fraud concerns. As Peter Swire has noted, giving customers a single file with all of their data means that "one moment of identity fraud can turn into a lifetime breach of personal data."[8] As important, portability and other similar requirements run the risk of further embedding the market power of the large platform companies that already dominate consumer data collection and processing. Customers will likely be more willing to "port" their data to a large, established platform company than an unknown startup. For these reasons, Congress should carefully consider whether a portability requirement will truly benefit consumers.

Question 2. What improvements would you make, if any, to Art. 20 of GDPR, which addresses the right to data portability?

Response. For the reasons discussed above, we are skeptical of a portability requirement. That said, any data portability requirement should be limited to data, such as account information, that an individual provides directly to a company. It should also only apply to digital records. The requirement should be crafted in a way that allows individuals to port photographs or files stored in the Cloud, but does not require companies to retain a broad range of data about a user's activity in personally identifiable form in order to comply with such requests. Finally, any requirement must take into account its potential fraudulent use, allowing companies to implement methods and procedures to minimize fraud and security risks and providing reasonable liability protections for companies that have made good faith and reasonable efforts to comply with any portability requirement in a secure and responsible way. Legislation should also provide business sufficient time to develop and implement the potentially costly and complex operational changes that may be required to comply with any portability requirement.

Question 3. How best can data portability rights be crafted to create new competition, but not further entrench incumbent companies?

Response. For the reasons noted above, we are skeptical that a portability requirement would create new competition. Such a requirement could unduly burden competitors, especially small business, and serve to benefit larger platforms with whom customers may be more comfortable sharing data.

[8] Peter Swire and Yianni Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, 72 Md. L. Rev. 335, 339 (2013), available at: http://digitalcommons.law.umaryland.edu/mlr/vol72/iss2/1.