Responses to Written Questions Submitted by Honorable Jerry Moran to Bud Tribble

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. At Apple, we appreciate that information cannot be handled in a one-size-fits-all manner. The appropriate treatment of personal information depends on many factors, including the nature of the personal information (such as how sensitive the personal information is), the volume of personal information, the use to which the personal information will be put, and more.

That being said, companies and innovation thrive in stable environments, where new ideas can be explored within known frameworks. And, although technological developments have changed how people see and interact with the world around them, the categories of information that people hold close has been relatively stable over time. For example, people treat their financial information with great care, maintain the confidentiality of their government identifiers such as Social Security numbers, and believe their medical and health information should be private. Legislators can look to these long-held norms and expectations of consumers to enumerate a set of data categories identified as sensitive personal information in federal privacy legislation.

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. In today's interconnected world, any legislation or technological change that affects information necessarily has ripple effects throughout the global digital economy. As a leader in technology and innovation, the United States is well-positioned to impact not only how data is handled within its borders, but around the world. The US should seize this opportunity to create strong federal privacy legislation that sets a minimum floor for the responsible handling of personal information by companies doing business within its borders, or otherwise handling the personal information of individuals in the US. The legislation should include bolstered FTC authority with materially significant sanctions for the violation thereof. Because a person's interest in protecting their data does not stop at the national boundary, nor should the obligations to maintain reasonable privacy and data security standards to safeguard personal information. We would urge the Committee to consider developing and applying minimum standards to protect the privacy and security of personal information of individuals in the US regardless of the company's location or where the data is stored.

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 protection?

Response. At Apple, we believe that great products do not need to come at the expense of user privacy. Responsible innovation means carrying out research and development with privacy in mind. That is why we focus on techniques like on-device processing to avoid the need to collect user data, differential privacy to provide greater anonymity for users when we collect data, and intelligent tracking prevention. Legislation also plays an important role in incentivizing behavior and shifting norms. Well-crafted federal privacy legislation could help to encourage the research and development of products and services that improve privacy protections by requiring that companies put consumers in control of what personal information is collected and how it is used and shared. Legislation could also look to address the technical aspects of how companies process personal information that they have collected and encourage the use of privacy-protective techniques like anonymizing or de-identifying data. For example, we associate Apple Maps data with temporary random identifiers, not a user's Apple ID, meaning Apple can provide users with relevant information without building a history of their location.

We believe that comprehensive privacy legislation should also include accountability mechanisms, requiring that companies develop and maintain privacy and data security programs to protect the information entrusted to them by consumers. Such legislation should also allow for flexibility in such programs to encourage companies to create programs tailored to the nature and volume of personal data processed, and the risks posed by the company's activities. Depending on the legislation, it may be appropriate to introduce a safe harbor for companies that have appropriately implemented specified safeguards or employed other specified privacy techniques, such as certain encryption standards, to protect the personal information of consumers. Finally, the legislation should include strong sanctions to deter the violation thereof.

Question 4. As GDPR includes requirements like the "right to portability" and the "right to be forgotten," it is clear that these provisions aim to promote the consumer's ownership of their data by requiring companies to abide by their requests to permanently delete or transport their personal data to another company. However, how are these concepts enforced when the consumer's data is submitted as an input to one or multiple proprietary algorithms employed by the company?

Response. Apple believes that a user's data belongs to them. And Apple believes that consumers should be in control of the information that they provide about themselves. We support the GDPR's efforts to promote consumer control in the right to portability and the right to be forgotten as well as other mechanisms to make sure consumers are in control, such as the right to opt out of the use of their personal information, or the ability to correct their personal information.

We appreciate this Committee's identification of the practical challenges associated with implementing requests by consumers to exercise their rights under GDPR. It is important that tools designed to empower consumers are designed thoughtfully so as to avoid unintended

consequences and impractical results. For example, these rights should not require companies to delete data maintained about known fraudsters. And, once personal information about a consumer has been incorporated into the output of a proprietary algorithm, a company should not be required to destroy company property - in the form of a proprietary algorithm - to satisfy a consumer's request to delete their information. Instead, the rights granted to consumers and the technology industry's corresponding obligations should take into account technical feasibility, the encouragement of innovation, the welfare of consumers, and the interests of the general public, in their development and execution. By considering a well- rounded set of factors in developing consumer rights and business obligations, we believe that legislators could achieve the aim of putting consumers in control of their own information without unnecessarily or unintentionally harming innovation.

Question 5. Are the outputs of the company's algorithm decidedly the consumer's personal information and required to be deleted or transported at the request of the consumer? If so, do these requirements remain the same if the data outputs are anonymized?

Response. Apple believes that any information that relates to an identified or identifiable individual is personal information; and that no privacy legislation should require companies to re-identify or otherwise increase the identifiability of information they maintain. If the results of an algorithm relate to an identified or identifiable individual, then those results are personal information. Whether the results must be deleted or transported at the request of the consumer depends on the nature of the results and of the consumer. Is there a lawful reason for why the personal information should not be transported? For example, are the results from a proprietary security or fraud prevention algorithm, the disclosure of which would assist a bad actor in committing further fraudulent acts? At Apple, so long as the information relates to an identified or identifiable individual, any applicable consumer rights apply unless there is a countervailing lawful interest that applies; and the GDPR fully recognizes and is aligned with these concepts.

Question 6. Since companies often use aggregated data outputs to study and improve their existing algorithms, services, and products, what impacts do you expect these vague GDPR requirements to have on companies' abilities to innovate?

Response. We believe companies should challenge themselves to reduce the identifiability of information that they hold, and aggregating data is one way of doing so. We believe that meaningful privacy legislation should encourage companies to take these steps, and shouldn't require companies to re-identify data that is not held in an identifiable way. Encouraging responsible behavior, including reducing the amount of identifiable data collected and retained by companies for unnecessary or unlawful purposes, is a vital part of protecting user privacy while retaining pathways for innovation. We believe it is too early to tell how the GDPR's provisions will generally impact the technology sector's ability to innovate or the methods used, but would encourage this Committee to take the impacts into account as it undertakes the task of crafting federal privacy legislation.

Responses to Written Questions Submitted by Honorable Shelley Moore Capito to Bud Tribble

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. Apple believes that consumers own their personal information and therefore must be in control of their own information. The first step in putting the consumer in control is developing tools to help ensure that the consumer has all relevant information about how their personal information is being handled, at the time they need that information.

Apple has dedicated teams focused on how best to provide consumers with the information and tools they need to take control of their personal information. Throughout its history, Apple has developed and implemented a suite of innovative and privacy-protective tools. For example, we developed a privacy icon, which appears when a consumer launches or signs into an Apple service or feature that collects personal data, to make it as easy as possible for consumers to recognize when their data is being collected by Apple. We also provide users with meaningful information about their privacy choices immediately next to the mechanism they can use to exercise that choice, to make it as easy as possible for consumers to make informed decisions about their privacy.

Apple doesn't just hold itself to high standards, it also encourages App Developers to engage in the responsible collection and use of personal information through its app developer Program License Agreement (PLA} and our App Store Review Guidelines which have extensive privacy requirements. Apple also helps to ensure that the app developers comply with the terms of the PLA by creating technical controls to enforce requirements. For example, Apple provides technical controls via the operating systems we develop to require that an app developer that would like to access location information must explicitly ask and provide the consumer with an explanation as to why it would like to access the location information, before iPhone will allow access. These are just some of the ways that Apple works to help ensure that consumers are given the information they need to exercise informed choices about their information. And, because privacy is a core value at Apple, our job in protecting consumer privacy is never done - we are continuously challenging ourselves to improve our privacy protections and keep consumers in control of their data.

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

Response. Apple is deeply committed to the concepts of transparency, consent, and control so that users have the information and the tools available to make informed privacy choices. We believe in telling our users up front exactly what's going to happen to their personal information, and asking for their permission before they share it with us. And if users change their mind later,

we make it easy to stop sharing with us. Every Apple product is designed around those principles.

When Apple does ask for permission to use personal information, it's to provide our users with a better experience.

Apple's privacy policy is one of many places that users can go to learn about how Apple handles their personal information and how they can exercise their rights in their data. Apple has worked to help ensure that its privacy policy is useful to consumers, by using clear and plain language, altering font size to draw attention to key issues, and by layering the policy so that consumers can learn even more about practices that they are interested in by clicking on links to additional information.

Recently we introduced a new privacy icon to give our customers just in time privacy notices:

The icon is shown when a user launches or signs into a service or feature that collects personal data. Underneath the icon is an explanation of the key privacy practices for that product or service followed by "See how your data is managed" link with more fulsome details. Importantly, the icon is not shown when a user launches a privacy by default service such as Siri or Maps which doesn't collect personal data.

As the digital economy becomes increasingly complex, it is likely that consumers will be presented with even more information about how their data will be collected and used. One of the key challenges facing industry and legislators today is how to ensure that consumers are provided with the information they need at the time that they need it - in other words, by focusing on not just transparency, but pertinence. We believe that a privacy policy is a useful tool - but not the only tool - that companies should offer consumers to help them learn more about how their data is handled. At Apple, we work to meet that challenge by providing consumers with privacy policies, just-in-time notices, and meaningful controls. As this Committee takes up the difficult task of federal privacy legislation, we would encourage it to challenge companies to come up with creative ways to provide consumers with relevant information about their privacy practices at the time that consumers need that information to make a decision, to help consumers them stay in meaningful control of their personal information.

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. As a company dedicated to creating great products for peopleof all ages and backgrounds, we understand that people experience technology differently. That is why we provide information about our products and services - including our privacy practices - in a variety of ways, to help ensure that, no matter what consumers are looking for, there is a solution that works for them.

On our website, at www.apple.com/privacy, consumers can learn more about how our products work. Apple's privacy policy provides an overview of Apple's approach to privacy and how we handle personal information. And we provide just-in-time privacy notices with detailed information about Apple's handling of personal information, together with our Apple privacy icon, to help alert users to particular privacy practices when they become relevant. Interested consumers can review detailed information on the technical safeguards we have built in our iOS Security Guide and macOS Security Overview.

Consumers can also contact Apple by phone, email, or text, or visit us in a retail store to learn more about the tools that they can use to control their personal information and to have trained personnel help walk them through how to take certain actions, such as how to enable location Services or change other settings.

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. Apple's online store does not create user profiles based on personal information collected from third parties to recommend purchases. We do use the information you expect us to know about your Apple online store activity to personalize your experience; for example, if you purchase an iPad, you may be shown an iPad case or cover. To help consumers navigate the thousands of apps made available on the Apple App Store, we offer the ability to personalize the App Store experience. Consumers can turn off App Store personalization at any time by disabling the "Personalized Recommendations" switch. When personalization is enabled, we use information about a consumer's use of the App Store, such as the content searched for, downloaded and purchased, to suggest relevant apps. We accompany this with a transparency page which makes clear to the user what data was used to personalize their Store experience.

Apple also helps its developers promote their apps by advertising on the App Store. Even so, because privacy is a fundamental value at Apple, we have taken additional steps to help ensure that consumers' identity and other personal information remains protected: Apple does not allow developers to target specific individuals or even groups of a handful of individuals. Instead, consumers are grouped in buckets of at least 5,000 consumers to help ensure that no one consumer's identity or characteristics is known or knowable. Finally, consumers can opt out of targeted advertising by Apple entirely, at any time, by enabling "limit Ad Tracking."

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

Response. The digital economy runs on information. For the economy to continue to succeed, it must be built on a solid foundation of trust between consumers and companies, grounded in a

common understanding of how information will be collected and used. In enacting comprehensive federal privacy legislation, Congress can help establish that common understanding by setting minimum standards for the collection and treatment of personal information by companies operating in or otherwise handling the personal information of individuals in the US. Doing so will help set the groundwork on which a vibrant digital economy can flourish.

To help ensure that technological innovation can and does continue, any legislation should acknowledge and leave room for responsible innovation - including with respect to privacy - protective technologies. In all industries, but particularly in the digital economy, the technology of tomorrow is light years beyond the technology of today. Therefore, to help enable privacy innovations and help ensure the protection of the personal information of consumers, we encourage this Committee to consider establishing a framework for data protection that ensures consumers have robust and enforceable protections and incentivizes companies to innovate, develop, and deploy new and meaningful privacy-enhancing technologies.

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 extensive 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. As the GDPR has only recently come into force, it is too soon to assess the administrative impact of the legislation on businesses and how potential penalties may affect the market. GDPR acknowledges that special considerations in relation to record-keepingmay be present for small- and medium-sized enterprises (generally understood to be companies with under 250 employees). More generally, some GDPR requirements may serve to help smaller businesses by spurring competition, such as the right to data portability. In large part, the impact of GDPR on small businesses will be left to the discretion of the enforcement bodies, the data protection authorities.

We believe that well-crafted comprehensive privacy legislation should impose obligations on businesses that are appropriate given the potential risks to consumers and the public. We appreciate the challenge that this poses and would encourage the Committee to look to the provisions and impact of all existing privacy and data security legislation as it looks to craft a federal law.

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.

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?

The United States has taken a reasoned and measured approach to legislating the flow of information, which provides it with benefit of learning from the successes and challenges of various data protection regimes around the world, as well as sectoral laws in the United States. We would encourage this Committee to take into account all available information regarding the language and effect of laws governing the handling of personal information as it considers comprehensive federal privacy legislation.

In the United States, for example, the federal Privacy Act of 1974, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act all serve as useful data points to consider regarding the appropriate governance of personal information. States have also served their role as laboratories in enacting similar but differing laws in areas such as data breach notification and financial privacy. Globally, the European Union's GDPR and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules System should provide further source material.

In addition to existing legislation, we also believe that consumer concerns and the characteristics and limitations of technologies (as well as the need for flexibility to accommodate future technologies) should be taken into account. Importantly, to help ensure that legislation does not unnecessarily stifle innovation and economic development, we would encourage this Committee to consider the impact on consumers, businesses, and the public and find the appropriate balance when considering legislation.

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

Response. Any regulator tasked with overseeing federal privacy legislation should be armed with resources and knowledge, including technical experts, to appropriately enforce meaningful federal privacy legislation. As the current leading federal privacy enforcement agency is the Federal Trade Commission, we believe the FTC should play an important role in interpreting and enforcing comprehensive privacy legislation.

Question 9. According to recent research by Magid, a media research firm, 35% of millennials share their password to access streaming services. I certainly understand that the terms and conditions of these services already note that access is for personal use and not to be shared with others. And that the account holder remains responsible for the actions of that third party. However, as the number [of those in the] younger generations sharing their password grows so has the potential for abuse. This "overly sharing of passwords" and the younger generation operate differently than many my age.

Are your policies flexible to cover a third party that may use a friend's or spouse's password? Is this something we should consider as we create federal guidelines?

Response. Meaningful privacy controls are built upon great security and need security to function properly. Whenever data security controls are compromised, the safety and confidentiality of data is put at risk. This is true even where passwords are shared with friends or loved ones, as such sharing creates another avenue through which a bad actor could attempt to gain access to a consumer's account.

As part of Apple's commitment to privacy, we challenge ourselves not to take steps that would decrease the security of consumers' information - we believe there is a better way. When Apple was confronted with the problem of sharing of passwords among family and friends, instead of encouraging such security-weakening behavior, Apple worked to develop a means for consumers to share information and activity with their friends and loved ones through Family Accounts, which allow users to share media they have purchased, including movies, songs, apps, and books, among accounts that share one payment method. We challenge ourselves to incentivize everyone in the ecosystem to allow for great experiences while leaving passwords - and personal data - under the control of individual people.

Responses to Written Questions Submitted by Honorable Todd Young to Bud Tribble

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.

What questions should policymakers be asking in developing data portability rights?

Response. Data portability and data access are used somewhat inter-changeably. Data access is the right to access all personal information stored about you, with very limited exceptions by a company or organization. It is a cornerstone of privacy as it allows for an individual to know what an organization holds on them and then act appropriately. Data portability is a new concept introduced by the GDPR that could also help drive innovation and competition in the global digital economy. As with other rights, such as the right to deletion, it is important that the right is properly scoped, so that bad actors cannot perversely use the rights to harm others. For example, a person should not be able to port all information that a company has about them, regardless of source. Doing so would sweep up information provided about them to the business by other persons, to which they would otherwise have no right. Doing so would also sweep up internal proprietary information about a company's fraud and security efforts that, if ported, could divulge trade secrets and/or confidential security information to potential bad actors. It is a right that is very much in its nascent stage and while we have enthusiastically sought to give effect to it under GDPR, it does need more time to fully develop. We would encourage the Committee to adopt a data portability mandate, bounded by firm guardrails, to help ensure that this right serves to further empower consumers and not create new or unforeseen consumer risks.

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

Response. As you know, Art. 20 of the GDPR requires that companies maintain the information to be ported in a standard format or to have the ability to move the data into that format. As technology continues to evolve, moving data to a standard format may not be feasible, especially given the speed at which innovation occurs. And, doing so may be cost-prohibitive for small businesses who lack the resources to move data into a "standard" format.

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

Response. As the GDPR is still young, it is difficult to tell what aspects of the right to data portability will operate as intended to create new competition and what might result in the entrenchment of incumbent companies. We look forward to learning more as enforcement begins and matures. However, we do believe that, in order to help ensure that competition is created, new entrants and small businesses should not be driven out of business as a result of the requirement itself. For example, a new entrant or small business should not be required to transfer personal information to a "standard" format if doing so would be cost-prohibitive. We look forward to continuing to work with the Committee on this and other issue as it considers comprehensive federal privacy legislation.