April 5, 2019

The Honorable Jerry Moran
Chairman
Committee on Commerce, Science, and Transportation
Subcommittee on Manufacturing, Trade, and Consumer Protection
U.S. Senate
Washington, District of Columbia 20510

The Honorable Richard Blumenthal
Ranking Member
Committee on Commerce, Science, and Transportation
Subcommittee on Manufacturing, Trade, and Consumer Protection
U.S. Senate
Washington, District of Columbia 20510

Dear Chairman Moran and Ranking Member Blumenthal,

I applaud the Senate Commerce, Science, and Transportation Committee's Subcommittee on Manufacturing, Trade, and Consumer Protection for examining important consumer privacy concepts and practices in this hearing, *Small Business Perspectives on a Federal Data Privacy Framework*. In previous privacy hearings before this Subcommittee and others across Capitol Hill, Members of Congress heard from a broad swath of large company and consumer group interests. Even in those hearings, the discussion turned to how small companies would deal with compliance burdens imposed by existing and proposed commercial privacy regimes. The time is right to consider the views of small companies like ACT | The App Association's members, and we commend the Subcommittee for giving small companies a voice on the critical issue of a federal privacy framework.

The App Association is a trade group representing about 5,000 small to mid-sized software and connected device companies across the globe. In the United States, our member companies are part of a $987 billion industry, supporting about 4.7 million jobs. We regularly work to keep our member companies up to speed on the latest policy and legal developments and to translate those into practical and useable guidance to ease the burden of compliance.[1] Further, we are committed to promoting proactive approaches to ensuring end-user privacy and participate frequently in the privacy debate at the federal level.[2]

We recognize that many commenters in this debate are asking you to reject even the aspirational goals of Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)—and certainly, both are flawed manifestations of the protections they seek to provide.[3] Nonetheless, we are in a CCPA-GDPR world, and our recommendations reflect this reality, with an

[1] *See, e.g.,* ACT | The App Association, General Data Protection Regulation Guide (May 2018), *available at* https://actonline.org/wp-content/uploads/ACT_GDPR-Guide_interactive.pdf.
[2] *See, e.g.,* https://www.ntia.doc.gov/files/ntia/publications/2018-11-09_-_ntia_-_privacy_filing_-_final.pdf; http://actonline.org/wp-content/uploads/2018-04-10-FTR-ACT-the-App-Association-Facebook-Privacy-FINAL.pdf.
[3] *See, e.g.,* https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2886&context=historical.

1401 K Street NW Suite 501
Washington, DC 20005
202.331.2130 @ACTonline
ACTonline.org /actonline.org

eye toward assisting you in producing legislation that creates the optimal conditions for companies to provide innovative and meaningful privacy protections, while avoiding several-hundred-human-year compliance requirements.[4] Steep compliance requirements like these would do doing little to improve privacy outcomes, while causing our member companies to raise prices or go out of business to pay legal fees. With CCPA going into effect January 1, 2020, time is running short. But the time crunch should not prevent us from spotting the real issues. Although many of the congressional hearings and public debate on privacy have centered on advertising, a broad privacy bill will regulate a lot more than just online ads. The online ad-driven issues that have been observed should not define the laws that bind the entire app economy, most of which is not driven by advertising revenue. A federal privacy framework is necessary, and our goal is to help bring us to one that preserves innovative market activity and competition while drawing on established rules from existing laws.

Commercial privacy is not a static concept and yet products and services should be designed to respect user privacy. Often this can only be accomplished through an ongoing dialogue with users that accounts for changing contexts and expectations. Our member companies compete with each other and larger companies to create better, more efficient privacy protection measures. They work hard to comply with privacy laws, best practices, and regulations, but they know that their clients, customers, and users usually have a choice and the kinds of privacy practices they employ inform that choice. This is a foundational concept that this Subcommittee must consider as it proceeds with negotiations over a federal privacy framework. It forms the core of our privacy philosophy and guides our policy recommendations, laid out in more detail in this statement.

I. Transparency

The right to transparency is crucial to a federal privacy framework. Consumers have no basis on which to evaluate their privacy options without understanding the kinds of data that are being collected about them, who is collecting that data, and what that data is being used for. The CCPA requires transparency along a few dimensions, including the "categories" of personal information that are collected and processed.[5] Similarly, the commercial privacy legislation introduced in the Washington state Senate (SB 5376, as it passed the Washington state Senate) requires companies to disclose, in a "clear, meaningful privacy notice," information including "categories of personal data collected by the controller," the purposes for collection, etc.[6] The App Association supports a general requirement for companies to disclose the categories of personal information it collects, the purposes for which it is collected, and the categories of third parties to which companies make such data available. Such a requirement is perhaps not a "right" in a legal sense, but it is likely the most legally sound means of expressing a "right to transparency."

Privacy begins with communication, but it does not end with disclosures like privacy policies. It is not enough to simply disclose to consumers a company's practices with respect to data collection, processing, and sharing. Experience shows that a simulated meeting of the minds via click-wrap agreements is insufficient to apprise consumers of the complexities of modern data practices. Nonetheless, we agree with many of the advocates and experts this Subcommittee heard from

---

[4] *See, e.g., Examining Safeguards for Consumer Data Privacy Before the Senate Comm. On Commerce, Science, and Transportation*, 115th Cong. (2018) (comments of Keith Enright, Chief Privacy Officer, Google LLC).

[5] CCPA Sec. 1798.110.

[6] SB 5376, 2019 Leg., Reg. Sess. (Wash. 2019) (SB 5376).

that the underlying purpose of federal privacy legislation must be to address observed harms that result from privacy failures. Those harms are notoriously difficult to define in part because they are so driven by individual expectations and contexts. As such, a touchstone of addressing them flexibly is to create conditions where consumers are empowered to make choices—and where companies are empowered to develop meaningful lines of communication with consumers with whom they have a relationship. Addressing the harms, therefore, starts with a baseline transparency requirement.

II. Right to Control, Including Rights to Access, Edit, and Delete

Federal legislation should require companies to respond to verifiable requests by a consumer to access, correct, or delete their own data, with some exceptions. Various combinations of these requirements appear in GDPR, CCPA, and SB 5376. Of these three frameworks, the Washington legislation comes closest to striking the right balance. First, the Washington bill gives covered entities some leeway to verify the request, defining a "verified request" as the process by which a covered entity can "reasonably authenticate" the consumer making the request using "commercially reasonable means."[7] Second, the Washington legislation only requires correction of personal data held in "identifiable form concerning the consumer."[8] This is an important caveat. The use of machine learning algorithms or creation of synthetic datasets—separately generated data designed to mimic actual datasets, but without any connection to real people or situations—would be difficult if the company were required to unwind and edit a single person's data upon request, without reasonable exception.

Third, the Washington state legislation only requires a covered entity to honor a verified request to delete data concerning a consumer in limited circumstances. Moreover, if the reason for the deletion request is objection to processing, deletion is only required if "there are no business purposes for processing the personal data for the controller."[9] Strong countervailing factors—more than just consideration of a "public interest" in preserving the data—must be present to ensure that consumer rights are not appropriated by bad actors and to avoid other process abuses. Policymakers must be sensitive to the prospect of competitors inundating market rivals with "verified requests." Strong data control mechanisms for consumers are important, but naively assuming they will be used only for their intended purposes risks unintentionally creating opportunities for mischief. Moreover, a failure to allow companies to use the means necessary to verify the consumer—and the corresponding ability to deny the request if it cannot verify—could have the ironic effect of assisting with the violation of consumer privacy by requiring the covered entity to share personal data with a bad actor posing as a verified consumer.

III. Right to Prohibit Disclosure or Sale to Third Parties

From a small business standpoint, this is an area where policymakers should be especially careful. One of the main purposes of CCPA is to restrict the sharing or sale of data with third parties. It turns out that the app economy is built on close relationships between big platform companies and third parties. Our member companies are, in GDPR parlance, usually both controllers and processors (that is, they have both direct and indirect consumer relationships). Provisions that too severely limit how entities with direct consumer relationships (controllers) deal with their service

[7] SB 5376 Sec. 3(26)
[8] SB 5376 6(2)
[9] SB 5376 6(3)(a)(iii).

providers/third parties/processors will likely result in deterring those controllers from outsourcing activities—usually to smaller businesses. As a result, innovative activity in the highly competitive app economy is eventually subsumed into larger businesses that currently serve as platforms that also facilitate direct relationships between developers and consumers.

Our member company's experience is instructive in this regard. This company makes an app that blocks unwanted robocalls. Not long after CCPA was enacted and GDPR went into effect, the company received notice that it would be temporarily removed on a specific date from an app platform for privacy reasons. Certainly, the core function of the app requires it to collect and analyze the phone numbers of incoming phone calls, so it was unusual in the app's nine-year history to suddenly be called into question over this term of service. Throughout this process, the company never made changes to the core functionality of the app to gain reapproval but was finally cleared to remain on the platform the day before its scheduled removal.

If the platform had removed the app—even temporarily—it would have been catastrophic for a small company that depends on access to platforms to reach its customers. Moreover, removal would have taken away a tool for consumers to use to block unwanted robocalls, of which there were 26.3 *billion* to US mobile phones in 2018.[10] The proposed removal of the app is an illustrative example of how companies are responding to the prospect of serious liability for unclear restrictions on how they can share data (or facilitate the sharing of data) with third parties like App Association members. We hope it serves as a cautionary tale for the Subcommittee of what strict third-party sharing regulations mean for small to mid-size software development companies: when we regulate the big guys, we also regulate the little guy, albeit in less predictable ways. Policymakers ought to keep in mind the symbiotic nature of platforms and apps. We are already beginning to observe that the default responses to these kinds of requirements threaten to push innovative activity out of the app economy, leaving larger companies with compliance teams as the only viable competitors.

IV. Lawful Bases for Processing or a Prohibition on Harmful Processing

Two main features of GDPR are a set of consumer rights and the illegalization of all data processing *except* where lawful bases are stated. We strongly urge the Subcommittee to outright reject the idea of putting the burden on covered entities to explain why their data practices are legal, with a backdrop presumption of illegality. We believe there are better ways of achieving the goal of outlawing undesirable data processing activities. And experts tend to agree that European laws like GDPR are aspirational—that is, they are not usually enforced strictly but are meant to set a high bar for market behavior that gives regulators leverage to call private sector entities into their offices to discuss how they do business. Moreover, the First Amendment makes a presumption of unlawfulness difficult and perhaps even unconstitutional.

The Subcommittee should instead consider outlawing certain data processing practices known or likely to be more harmful than beneficial. For example, Congress should outlaw—and in many respects already has outlawed—discrimination that denies classes of people financial benefits or legal rights based on race, sexual orientation, gender, etc. In some cases, Congress will not *need* to include antidiscrimination provisions in a broad privacy bill, especially where current laws are

[10] Sarah Krouse, "The FCC Has Fined Robocallers $208 million. It's Collected $6,790," The Wall St. J. (Mar. 28, 2019), available at https://www.wsj.com/articles/the-fcc-has-fined-robocallers-208-million-its-collected-6-790-11553770803.

being interpreted to prohibit discriminatory activities in new contexts. The federal government is testing the applicability of the Fair Housing Act to online targeted advertising as the Department of Housing and Urban Development (HUD) is suing to enjoin ad targeting HUD says limits housing options for people.[11] Similarly, federal agencies have scrutinized the applicability of the Equal Credit Opportunity Act (ECOA), which prohibits discrimination in access to credit, to newer online lenders (especially "marketplace lenders" that specialize in non-banking lending).[12] It is clear, however, that there is an appetite in Congress to address harms arising from discrimination in the context of privacy legislation. We are happy to work with the Subcommittee as it seeks to draft provisions that restate the illegality of discrimination or otherwise update relevant laws in the context of a privacy bill.[13]

Aside from addressing certain kinds of discrimination, which U.S. law has generally determined to be *per se* harmful, the Subcommittee should consider flexible options for curtailing net harmful data processing activities. The Subcommittee could start to develop a taxonomy of informational injuries that includes harmful discrimination by looking first to the framework proposed by previous Acting FTC Chairman Maureen Ohlhausen.[14] This framework breaks down difficult-to-define informational injuries to provide a foundation on which to operationalize the prevention of evolving privacy threats. Similarly, SB 5376 requires controllers to conduct risk assessments to evaluate the risk certain data processing activities present to consumers. Under this provision, if the risk assessment "determines that the potential risks of privacy harm to consumers are *substantial* and *outweigh the interests* of the controller, consumer, other stakeholders, and the public in processing the personal data of the consumer, the controller may only engage in such processing with the consent of the consumer or if another exemption under this chapter applies" (emphasis added).[15] Not only does this flexible prohibition avoid the problems of categorically declaring processing of personal data illegal with specific, enumerated exceptions, it is also familiar. The Federal Trade Commission (FTC) Act currently prohibits acts or practices in or affecting commerce that "cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[16] Thus, a risk assessment could be rooted in existing law and require companies to

---

[11] *See* Andrew Liptak, "The US government alleges Facebook enabled housing ad discrimination," THE VERGE (Aug. 18, 2018), *available at* https://www.theverge.com/2018/8/19/17757108/us-department-of-housing-and-urban-development-facebook-complaint-race-gender-discrimination; Russell Brandom, "Facebook has been charged with housing discrimination by the US government," THE VERGE (Mar. 28, 2019), *available at* https://www.theverge.com/2019/3/28/18285178/facebook-hud-lawsuit-fair-housing-discrimination.

[12] *See* U.S. Department of the Treasury, Opportunities and Challenges in Online Marketplace Lending (May 10, 2016), *available at* https://www.treasury.gov/connect/blog/Documents/Opportunities_and_Challenges_in_Online_Marketplace_Lending_white_paper.pdf.

[13] *See, e.g.,* "Updated draft bill," INTEL CORP. (Jan. 28, 2019), Sec. 3(j)(5) (including "adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment . . . credit and insurance . . . housing, education, professional certification, or the provision of health care and related services" in the definition of privacy risk), *available at* https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill-01-28-19.pdf.

[14] Maureen K. Ohlhausen, "Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases," remarks at Fed. Comm'cns Bar Assoc. Luncheon (Sept. 9, 2017), *available at* https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

[15] SB 5376 Sec. 8(3).

[16] 15 U.S.C. 45(n).

"do their homework," better enabling enforcement authorities like state attorneys general (AGs) and the FTC to enforce the law.

Although we support a provision requiring risk assessments, the Subcommittee should be aware of potential practical issues with unclear requirements in this regard. For example, how many risk assessments should a small business conduct? The Washington bill says there should be one for "each of their processing activities involving personal data . . .."[17] This may be difficult to put into practice without further guidance because nothing tells us where to draw the line between distinct "processing activities." Moreover, risk assessments for processing involving *any* personal data could be unnecessary, at least in written form. It may be that processing activities involving personal data should be subject to risk assessments, but written assessments may only be useful to enforcement authorities if they cover processing activities involving *sensitive* personal data.

V. Preemption and Enforcement

The prospect that congressional action on privacy alone might establish a single national standard is not a guarantee. Therefore, we recommend that privacy legislation the Subcommittee drafts include a provision explicitly preempting state laws and rules dealing with privacy within the framework of the legislation. We acknowledge that some members of the Subcommittee want to avoid a discussion of preemption until after other provisions have been addressed. From a small business standpoint, however, preemption is one of the most important elements of a federal privacy framework. If legislation does include a preemptive provision, we agree with many advocates that state attorneys general should be authorized to enforce the provisions of the law. Similar laws like the Child Online Privacy Protection Act (COPPA) have benefited from empowering state attorneys general to police for prohibited conduct. Moreover, we agree with you that Congress should authorize additional funds for the FTC to police privacy practices under a new federal privacy framework.

VI. Rulemaking

Some advocates have argued that Congress should authorize the FTC to have general rulemaking authority using procedures set forth in the Administrative Procedure Act (APA). The FTC is authorized to promulgate rules under a modified process dubbed the Magnuson-Moss rulemaking procedures, which require live hearings, among other things not present in APA procedures.[18] The extra hurdles in the Magnuson-Moss procedures are significant but enabling and encouraging the Commission to undertake rules using expedited APA procedures without meaningful guidance or limitations is unlikely to produce better privacy outcomes. The FTC is not designed to be a rulemaking agency, in part because the swath of the economy and range of economic activities it oversees is too broad for it to promulgate generally applicable rules that successfully balance the finer conflicts of purpose in the many sectors that would be subject to those requirements. In contrast to the Federal Communications Commission (FCC), which closely regulates a defined set of capital-intensive industries, the FTC's purview reaches more broadly and prohibits intentionally less defined unfair or deceptive acts or practices in or affecting commerce.

---

[17] SB 5376 Sec. 8(1).

[18] *See* FED. TRADE COMM'N ADMIN. STAFF MANUAL, *available at* https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch07rulemaking.pdf.

Although the FTC likely does not possess the purposes or characteristics that make it a good fit for general APA rulemaking authority, we would support giving the FTC the ability to promulgate rules using APA procedures in limited circumstances under a broad privacy bill. While the FTC has generally relied on case law, consent orders, and guidance to develop and evolve its approaches to new products, services, and other activities, rulemaking may be a more appropriate tool in some areas. For example, Congress could authorize the Commission to use APA procedures to further define or add to certain terms Congress provides in statute, within statutory limits or guidelines.

VII. Conclusion

We appreciate this opportunity to comment on the record in this hearing. We commend the Subcommittee for its focus on small business responses to current and proposed privacy laws and regulations. We stand ready to assist the Subcommittee's members as they develop a federal privacy framework.

Sincerely,

Morgan Reed
President

ACT | The App Association
1401 K Street NW (Suite 501)
Washington, District of Columbia 20005