Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, District of Columbia 20515

Re: Morgan Reed's Responses to Additional Questions for the Record

Dear Ms. Herron,

Thank you for inviting me to testify on behalf of ACT | The App Association on April 27, 2023, at the hearing, "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information."

Pursuant to the Committee on Energy and Commerce's Rules, I am attaching my answers to additional questions for the record in the required format.

Please let me know if you have any additional questions or if it would help for us to meet with Subcommittee staff as you continue your work on privacy legislation.

Sincerely,

Morgan Reed
President
ACT | The App Association

The Honorable Kelly Armstrong

1. **The Federal Trade Commission (FTC) advance notice of proposed rulemaking (ANPR) on "Trade Regulation Rule on Commercial Surveillance and Data Security" refers to "different kinds of consumers" and appears to consider employees as a type of consumer. The statement of Chair Khan regarding the ANPR also references "…tracking, collection, and analysis of consumer data in the workplace…", which seems to be a reference to employee data. The dissenting statement of then-Commissioner Noah Phillips disagrees that the Federal Trade Commission Act confers jurisdiction on the FTC to "regulate any aspect of the employer-employee relationship that happens to involve data." It is evident that the employer-employee relationship is fundamentally different compared to a business-consumer relationship. An employer must process employee data for several purposes, including compliance with state and federal labor laws and other purposes related to professional activities. How would FTC action to regulate employee data impose challenges on the employer-employee relationship and existing laws governing that relationship?**

I agree with the premise that the employer-employee relationship is fundamentally different compared to a business-consumer relationship. In our advocacy on privacy, the App Association has consistently urged lawmakers to ensure that however they decide to establish prohibitions on net harmful privacy conduct, those rules must respect the context of the business-consumer relationship. Employees' relationships with their employer are different enough from the business-consumer context that applying the same rules to both scenarios would result in awkward and ultimately harmful outcomes that policymakers would have to clean up later down the road. The contractual relationships at issue in these scenarios necessarily lead to differing privacy considerations. Whereas consumers pay companies for a given product or service (either monetarily or by allowing access to data about themselves), businesses pay employees for services in furtherance of the employer's production goals. Respect for context necessitates separate legislative—and regulatory—processes to consider the privacy issues that flow from these relationships.

The American Data Privacy and Protection Act (ADPPA) appropriately excludes "employee data" from the scope of "covered data." Likewise, the Federal Trade Commission (FTC) shouldn't seek to regulate privacy and security practices involving employee data under the same regime as consumer data. For example, mandating that employers respond to employee requests for access, deletion, or correction of data about themselves as if they were consumers of the company's products or services creates several obvious problems. An employee might disagree with their supervisor's characterizations of their performance and giving them a federally enforceable right to access any of their supervisor's communications about them or correct any of that information would obviously have a dramatically negative effect on the ability for businesses to operate. Although the FTC's Advance Notice of Proposed Rulemaking (ANPR) does not specifically ask questions about imposing requirements to respond to such consumer requests, any privacy framework policymakers ultimately pursue will likely include such requirements. Employers may also need to surveil employee activity—for example, to ensure safety or make timely adjustments to supply or staffing—in ways that would be inappropriate or at least communicated or conducted differently in the consumer-business context.

The Honorable Russ Fulcher

1. **Does the ADPPA provide better and clearer guardrails on the use of data to allow for ensuring companies can engage in identifying for fraud protection, contractual issues, and yet, provide avenues for these same companies to work with their partners by sharing user information?**

Yes. Section 102 of ADPPA, which limits the data minimization principles in Section 101, appropriately allows for collection, processing, and transfer specifically for "fraud and identity fraud detection and prevention," and contractual issues.

2. **I want to understand better data processing requirements of the ADPPA and again how it might differ from the GDPR. This is due to many B2B companies (like technology platforms) that work with application partners or other fulfillment partners. How does the service provider relationship with your companies work currently within the sectoral laws? Or is this not an issue?**

There are lessons to be learned from how sectoral laws and the General Data Protection Regulation (GDPR) deal with the "controller" / "service provider" relationship. In general, the structure contemplated in the Health Insurance Portability and Accountability Act (HIPAA) appropriately delineates responsibilities between "controllers" (covered entities (CEs) under HIPAA) and "service providers" (business associates (BAs) under HIPAA). Under HIPAA, CEs are responsible for defining the scope of processing, collection, and transfer activities and communicating directly with patients about how they collect, process, and transfer protected health information. BAs may only process PHI provided to them through a CE via the contractual relationship they have with the CE and the contract defines the scope of what they are allowed to do with respect to that PHI. It is via that contract that HIPAA's requirements apply to BAs. This is a logical construct for privacy, and it works similarly in GDPR. Many of my member companies have operations that put them under a BA agreement and operations that put them under the FTC Act. Likewise, I have member companies that are "controllers" under GDPR for some of their activities, but "service providers" for some of their other projects. Although the arrangements are complex, especially for small companies, having obligations flow via contracts through "controllers" to "service providers" is a better reflection of reality than making no distinction between those two categories.

3. **Is there a worry over the lack of certainty for businesses in not having clarity over what obligations they will have to comply with when it comes to information collected from children that may not be protected under FERPA? Mr. Reed, how do your businesses view these challenges?**

Yes, the legal landscape applicable to collection, processing, and transfer of children's data is complicated, whether the Family Educational Rights and Privacy Act (FERPA) applies or not. While the FTC has sought to clarify how FERPA and the FTC Act fit together, it is inevitable that the obligations that apply to education tech companies are ambiguous. In general, my member companies that provide education tools subject to FERPA pay closest attention to the

Children's Online Privacy Protection Act (COPPA) with respect to any of their activities that fall outside the scope of FERPA.

COPPA does operate a little differently from FERPA since FERPA regulates school districts (as opposed to businesses and their relationships with consumers). For example, COPPA's requirement for companies to obtain verifiable parental consent (VPC) prior to collecting PII from children does not apply "to the extent permitted under other provisions of law," (presumably, including FERPA's provisions). This could lead to the two regimes applying slightly unevenly or confusingly, even though there might be good reasons for their overlapping structure, but the FTC has addressed the issue. Under FERPA, schools need not obtain parental consent for disclosing children's education records to educational apps on contract with the school. The FTC has clarified in a frequently asked questions (FAQ) section that an education technology company may rely on "consent obtained from the school under COPPA instead of the parent," when such collection is for the "use and benefit of the school and for no other commercial purpose." Conversely, if the same children (if they are 12 or younger) sought to use the same educational apps outside the school context, the app must obtain VPC directly from those children's parents. Thus, while the edges around sector-specific privacy laws may seem less regulated, in this case, more regulatory privacy barriers arguably exist under the FTC framework than under the sector-specific law.

Ultimately, the takeaway for this Committee is that as it contemplates updates to children's privacy as part of ADPPA, there should be at least some focus on the burdens associated with VPC. As FTC Commissioners have pointed out, updates to privacy laws should avoid placing the burden on consumers wherever possible and instead place the burden of compliance on companies. VPC is an example of a requirement that places an inordinate burden on parents since it requires them to take seriously time-consuming steps to verify their identities with each and every service with which a child under 13 may interact. As a parent myself, I know that this is not a realistic burden to place on people as they seek to access educational services for their kids. And yet the current statute does not enable the market to provide VPC solutions in a convenient, organized way. It is often said that the notice-and-consent regime has failed because it doesn't fit real-world interactions between consumers and businesses. The same is true for VPC. A consumer privacy law can only ameliorate conditions for consumers to the extent it reflects reality and respects the ways consumers want to interact with and access digital goods and services.