



May 25, 2023

Jessica Herron
Legislative Clerk
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Ms. Herron,

I want to thank the Subcommittee for including Salesforce expertise and perspective in its April 27, 2023 hearing entitled “Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information”. We hope that Members and staff found the hearing informative and helpful as they continue their work developing a national privacy standard. Please let us know if Salesforce can be of service in the future.

Pursuant to the Rules of the Committee, please find responses to questions for the record attached.

Sincerely,

Edward Britan
Head of Global Privacy
Salesforce



Questions for the Record

The Honorable Kelly Armstrong

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?

In the U.S. we have a consumer-oriented privacy culture. The FTC should focus its ANPR on “Commercial Surveillance and Data Security” on protections for consumers. This will enable the ANPR and future rules stemming from it to gain more traction and be more effectively implemented.

There is a separate, well-developed field of employment law with which organizations must comply to protect employees. Salesforce believes that new employee-specific laws should be introduced to protect employee privacy. These laws could be enforced by the FTC with clear statutory guardrails to ensure that enforcement does not conflict with the existing employment legal structure.

Protecting employees in an ANPR primarily aimed at protecting consumers seems like a forced fit. Further, it would have unintended consequences in the employment context where obligations for consumer-facing companies and/or rights intended for consumers may come into conflict with data that employers need to maintain for legal compliance and/or to operate as an organization.



The Honorable Russ Fulcher

At our hearing in early March, we saw how the European Union is more characterized by economies that have large businesses continuing to grow, but with fewer startups as a result of the implementation of the GDPR. In a privacy briefing for my staff, a company privacy security officer noted how GDPR is putting more emphasis on businesses to explain how they are using consumer's data and subsequently, consumers receive more pop ups as a result. Compared to ADPPA which focuses more on data minimization as its base, do sectoral laws have notice and consent fatigue as well?

Notice and choice fatigue is real, and yes, this is an issue with the existing sectoral laws, which rely too much on opt-in or opt-out consent. Notice and choice places too much burden on the individual to protect their own privacy.

Notice, as envisioned by the GDPR's requirements around transparency, is good - it helps to set expectations and enable individuals that are so inclined to act to protect their data. Choice or consent, however, has been used in problematic ways, such as when consumers are burdened with too many choices that are too granular or layered in nature. This often leads to consumers agreeing to things without fully understanding what they are agreeing to.

The intent of GDPR was to move away from notice and choice by making consent a much more difficult standard to achieve. However, it has unintentionally resulted in the opposite effect, as more companies have sought to apply simple pop-up consent experiences to demonstrate compliance.

That is not to say that there isn't a place for notice and choice. Giving people an ability to control how their data may be used is helpful. But that should not be the end of the story.

The sorts of obligations that ADPPA would impose on organizations, including the data minimization principles and impact assessments would protect people without forcing them to make complicated decisions that they may not entirely understand or have the time to address.