Written Testimony of Edward Britan

Vice President, Associate General Counsel, and

Head of the Salesforce Global Privacy Team

Salesforce, Inc.

Before the

House Energy & Commerce Subcommittee on Innovation, Data, and Commerce

Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information

April 27, 2023

I. Introduction

Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee, thank you for providing me the opportunity to share my views on addressing gaps in U.S. privacy law through comprehensive federal privacy legislation. Comprehensive federal regulation of personal information is urgently needed to protect individuals, empower businesses, and advance responsible innovation.

My name is Ed Britan. I lead Salesforce's Global Privacy Team, a team of professionals located across the U.S., Europe, and Asia-Pacific regions. I have spent almost two decades focused on helping companies comply with global privacy and data protection laws, including the past two years at Salesforce, the seven years before that at Microsoft, and the previous seven years helping a range of companies as a lawyer at Alston & Bird, LLP.

U.S. Leadership in Privacy

Global privacy laws have changed significantly during my career, with a particular inflection point being effectuation of the EU General Data Protection Regulation (GDPR) in May 2018.[1] Since then, comprehensive privacy laws, frequently modeled on GDPR, have passed all over the world. The U.S. is now one of the few developed countries lacking a comprehensive national privacy law. The UK, Japan, Brazil, China, Kenya, and Thailand have all passed comprehensive privacy laws since GDPR went into effect.

[1] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing 95/46/EC (General Data Protection Regulation).

This is disappointing because the U.S. had been a thought leader in this space. In fact, the core concepts in GDPR and most other global privacy laws build upon ideas introduced in a 1973 report published by the U.S. Department of Health, Education and Welfare (the "HEW Report").[2] The HEW report introduced rights to access, delete and correct data, the data minimization and accuracy principles, and restrictions on automated decision-making. Further, it called for these concepts to be included in comprehensive federal privacy legislation. Had the U.S. taken that action, our industry, a crucial driver of global innovation and economic growth, might not be facing the current "crisis of trust" that led our CEO Marc Benioff to call for a comprehensive federal privacy law beginning in 2018.[3] But it is not too late for Congress to act. The world has advanced the concepts that the U.S. first introduced. Now, as we approach the 50th anniversary of the HEW report, the U.S. can reassert its leadership by passing a comprehensive federal law that builds on the current global standard and advances global privacy law for the next 50 years and beyond.

I am honored to have this opportunity to share with you the importance of passing a comprehensive federal privacy law and the features and concerns that such a law should address.

II. Why We Need a Comprehensive Federal Privacy Law

Salesforce Perspective

Salesforce is a cloud computing company offering customer relationship management (CRM) and other business-focused software to businesses, governments, non-profits, and other

[2] U.S. Dep't of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* viii (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

[3] Marc Benioff, Time for Silicon Valley to Get Behind a National Privacy Law, Politico (June 19, 2018), https://www.politico.com/agenda/story/2018/06/19/silicon-valley-national-privacy-law-000679.

organizations around the world. Our online and mobile services help our customers connect with their customers, being consumers, employees or citizens. Our customers use our services to work with some of their most sensitive data, which is why trust has been our number one value since our founding almost 25 years ago. A loss of that trust would jeopardize our ability to continue innovating and remain competitive. Therefore, Salesforce is committed to continuously proving to our customers that we are trustworthy custodians of their data.

To that end, we have developed a comprehensive privacy and data protection program that accounts for the ever-evolving landscape of global data protection laws. But we do not stop there. We also build our products using privacy by design principles and educate our customers regarding how they can use our products responsibly.

Privacy Is a Fundamental Human Right

Beyond the business imperative, Salesforce recognizes privacy as a fundamental human right that is crucial to upholding other rights, such as freedom of life, liberty, speech and protection against discrimination. To this end, we apply legal requirements that further the fundamental right to privacy, including from GDPR and other laws, globally. For us, protecting privacy is not merely a business strategy, but a moral responsibility. We urge Congress to help fulfill this responsibility by passing a comprehensive privacy law in the U.S. that applies to all Americans in all contexts.

Americans Are Demanding Privacy Protection Louder Than Ever

Americans want the government to hold companies accountable for how they process their personal information. This is borne out in a recent KPMG study in which 90% of

respondents indicate that government has a role to play in ensuring accountability.[4] Further, this belief does not seem to vary significantly according to political party, as a recent Pew Research Center study indicates that a majority of Americans – regardless of political affiliation – strongly favor increased legal protections governing companies' use of their personal information.[5]

A Broad Federal Privacy Law Should Support Existing Sectoral Laws

The U.S. has not yet taken the same comprehensive approach to privacy as was recommended by the HEW report and effectuated with GDPR. Rather, privacy protection in the U.S. is sectoral and driven by issue-specific laws at the federal level. However, while U.S. law regulates privacy differently from the EU, these U.S. sectoral laws are also effective and influential. What is missing is comprehensive regulation of personal information that should support these sectoral laws.

Without such comprehensive rules there will be significant gaps in protection. For instance, the Health Insurance Portability and Accountability Act (HIPAA) protects data related to a physical or mental health condition, provision of health care, or payment, as processed by certain entities, including health care providers, health plans and health care clearinghouses. This excludes a vast amount of health-related data processed by non-covered entities, such as through connected devices and online services designed to monitor and improve health and fitness. A law carrying forward concepts from GDPR and recently-passed state laws would strictly regulate this data and the companies that process it.

---

[4] KPMG LLP, The new imperative for corporate data responsibility (2020), https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2020/consumer-data-report-kpmg.pdf.

[5] Pew Research Center, *Americans and Privacy: Concerned and Feeling Lack of Control Over Their Personal Information* (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Similarly, while the Fair Credit Reporting Act (FCRA) effectively regulates consumer reporting agencies that furnish consumer reports, it does not cover similar types of profiling conducted by other companies for other purposes such as delivering personalized content or conducting e-commerce. Such profiles could be used in ways that impact an individual's reputation and privacy and should also be regulated.

Following passage of GDPR in 2018, the states have been filling this gap in U.S. privacy law by passing comprehensive laws of their own. California was the first state to take such action with the California Consumer Privacy Act of 2018 (CCPA). Since then, comprehensive privacy laws have also been passed in Virginia, Colorado, Connecticut, Montana, Utah, Iowa, Indiana, and Tennessee. While CCPA focused on restrictions around sharing personal information with third parties, the eight states that have subsequently passed laws, as well as a subsequent California law amending CCPA, the California Consumer Privacy Rights Act (CPRA), more closely adhere to the global standard set into motion by the HEW report and effectuated with GDPR.

Salesforce welcomes the passage of strong comprehensive privacy laws at the state level. These state-level efforts are important, as they demonstrate the need and demand for comprehensive privacy law. However, one's level of privacy should not depend on a ZIP code. Congress should be inspired to build upon these state-led efforts in setting a national standard which ensures that these privacy protections apply to all Americans.

III. What a Comprehensive Federal Privacy Law Should Address

Sensitive Data

The broad regulation of personal information should include enhanced protections for specific types of sensitive data, such as data related to race, gender, ethnicity, religion, disability, and health-related data not governed by HIPAA. Such regulation would be directly beneficial for promoting equality and civil rights by forcing companies to proactively identify, evaluate, and counter potential discriminatory impacts.

Emerging Technology – Mandatory Assessment

Salesforce has publicly raised concerns that certain types of technology, like facial recognition, currently pose a high risk of harm and discriminatory impacts, particularly for underserved communities. Because of these concerns, we don't offer facial recognition capabilities in our products.[6] But we continue to engage with these emerging technologies and have established guidelines for the responsible and ethical development of generative AI, which we're committed to following as the technology continues to advance.[7]

We believe that thoughtful regulation can enable development of appropriate safeguards that allow companies to responsibly innovate and unlock the economic and growth opportunities for themselves and for all Americans. In particular, we believe there's substantial value in

---

[6] Salesforce, Why We've Never Offered Facial Recognition (June 15, 2020), https://www.salesforce.com/news/stories/why-weve-never-offered-facial-recognition/.

[7] Paula Goldman, Generative AI: 5 Guidelines for Responsible Development, Salesforce (February 7, 2023), https://www.salesforce.com/news/stories/generative-ai-guidelines/.

performing data impact assessments and/or algorithmic impact assessments, as proposed under the American Data Privacy and Protection Act (ADPPA), when there's a high potential or risk of harm. We know that data sets used to train AI models are often discriminatory, and that unfortunately, discriminatory training data will yield discriminatory model outputs. To counter this, U.S. law should mandate that companies undertake assessments to purposefully and proactively identify and analyze data sets and how they will be used as a means to counter any latent discrimination or bias that may exist in the data.

Core Privacy Principles and Civil Rights

Salesforce strongly supports U.S. adoption of the core principles that underlie most global privacy laws, including GDPR. These principles, which were highlighted in the National Telecommunications and Information Administration's 2018 request for comments,[8] include transparency, control, data minimization, security, individual rights of access, correction, and deletion, risk management, and accountability.

Additionally, we believe that comprehensive federal privacy legislation should include provisions prohibiting the use of personal information to discriminate on the basis of protected characteristics. So we strongly supported inclusion in the ADPPA of "the first significant, nationwide expansion of civil rights protection in over a decade"[9] and would hope to see such protections included in future privacy legislation.

---

[8] Notice and Request for Comments, Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018) ("RFC").

[9] Bertram Lee, Federal privacy legislation the protects civil rights is critical for all Americans, The Hill (July 21, 2022), https://thehill.com/opinion/congress-blog/3568525-federal-privacy-legislation-that-protects-civil-rights-is-critical-for-all-americans/.

Controller/Processor Distinction

It is a current best practice in global data protection laws and regulations to make important distinctions between companies that decide how and why to collect and process personal data, who act as controllers of that data, and companies that provide services and process data on behalf of controllers, who act as processors of the data.[10] These distinctions date back 40 years and have been enshrined in GDPR and other leading data protection laws and regulations around the globe.[11] They are also reflected in the ADPPA, which recognizes that companies have different responsibilities when operating in different capacities. When companies focus on their role in handling personal data about individuals, they can more effectively identify and implement controls to help protect the privacy of those individuals.

In most global data protection frameworks, controllers and processors each have equally important obligations to ensure consumers' privacy. Controllers determine the purpose and means for collecting and using data, so they have direct responsibilities to consumers. For example, controllers are expected to disclose how they will use the data they collect and how long they will retain the data, and promptly respond to consumer requests to access or delete their personal information. Processors provide services to controllers under legal and contractual obligations that require them to only handle data at the specific direction of the controller, protect the data with adequate security measures, and allow controllers to meet their direct obligations.

---

[10] Kate Goodloe, Why the Controller-Processor Distinction Matters to Privacy, Business Software Alliance (November 8, 2022), https://techpost.bsa.org/2022/11/08/why-the-controller-processor-distinction-matters-to-privacy/.

[11] Business Software Alliance, Controllers and Processors: A Longstanding Distinction in Privacy (October 12, 2022), https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

For example, processors are contractually obligated to provide functionality within their services that enable controllers to honor consumer requests to access or delete their personal information. When Salesforce provides our software to our customers, we operate as a data processor, handling customer data on behalf of and pursuant to the instructions of those customers.

Encouraging Utilization of First Party Data

Companies shouldn't rely on third-party ad tech companies and third-party cookies to learn about their customers. Rather, we believe utilizing first party data obtained directly from customers is the best approach for customer engagement because this data exchange is known and expected by the customer, opens up the possibility for direct communication, and allows companies to build trusted relationships with customers through effective and transparent personalization. For example, marketers and salespeople can use a unified view of their first party data to honor an individual's contact preferences across internal systems and give the individual easy-to-use controls to manage and update their preferences. Customer success departments (who help customers implement and get the most out of their purchases) can be aware of recent purchases and tailor their support accordingly. Business departments can recognize what a person likes about a product to provide a personalized experience or enable internal development teams to determine what new features to prioritize.

Companies have more data than ever, and it's imperative that they're able to integrate it, analyze it, and understand it - in a trusted and secure way. In an environment where a majority of individuals feel like they've lost control over how their data is used but still expect personalized experiences and engagement, these intentional first party interactions can build trust by delivering relevant, personalized interactions to individuals who have chosen to share their data.

For example, individuals should be empowered to provide companies with clear instructions on how their data can be shared and used to create a better customer experience.

U.S. law should encourage these sorts of first party engagements. Such an approach is in-line with global regulatory trends and market changes and would help to decrease reliance on less privacy protective third-party tracking techniques. It also allows consumers to more easily and effectively exercise their individual privacy rights. If consumers understand which companies process their data and how it will be used, they know who to contact to exercise their rights in a meaningful way.

IV. Conclusion

Congress has made great strides toward passing a comprehensive federal privacy law. Last year, this committee passed ADPPA by a resoundingly bipartisan vote of 53-2. While there are undoubtedly aspects of ADPPA that every stakeholder would like to change, ADPPA reflected a hard-fought compromise that would meaningfully protect privacy, increase trust in industry, and position the U.S. as a world leader on tech issues.

ADPPA not only lines up well against the global standard envisioned first by the US with the HEW report and effectuated by GDPR, but it would return the U.S. to its global leadership role, especially on impactful issues like algorithmic impact assessment, application of civil rights to data protection, and restriction of third-party targeted advertising.

Thanks to decades of work and the significant advancements made last Congress, the path to providing world-leading privacy protections for all Americans is clear. Now is the time

for Congress to pass a comprehensive privacy law that builds upon the existing global standard and reasserts U.S. leadership on privacy and data protection.