November 9, 2018

Mr. David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Attn: Privacy RFC
Washington, DC 20230

Re: Developing the Administration's Approach to Consumer Privacy
Docket No. 180821780– 8780–01

Comments of Salesforce.com, Inc.

Salesforce.com, Inc. ("we," "us," or "Salesforce") appreciates the opportunity to respond to the National Telecommunications and Information Administration's ("NTIA") Request for Comments on Developing the Administration's Approach to Consumer Privacy ("RFC")[1]. We welcome the efforts of the Administration to address what our CEO, Marc Benioff, has described as "a crisis of trust in our industry"[2] and work with diverse stakeholders to advance consumer privacy.

Salesforce is a cloud computing company offering customer relationship management and other business-focused software to businesses, governments and other organizations around the world. We help our customers connect with their customers — or employees or citizens — in a whole new way, via cloud, social and mobile technologies. Our customers use our services to work with with some of their most sensitive data, which is why trust has been our number one value since our founding almost 20 years ago. If we lose that trust, as a company or as an industry, it will jeopardize our ability to continue innovating and remain competitive. Therefore, Salesforce is committed to proving to our customers that we are trustworthy custodians of their data.

To that end, we have undertaken significant efforts towards developing a comprehensive privacy program that accounts for the ever-evolving landscape of global data protection laws. But we do not stop there. We also go to great lengths to educate our customers regarding how they can use our products responsibly.[3] While some companies view privacy as a burden, we look at it as a strategic enabler of innovation and, ultimately, a competitive advantage — an opportunity to educate consumers about how their data is being used and how it is being protected.

That is why we believe that the time has come for a national basic privacy law in the US, one that protects consumers regardless of zip code and that is based on fundamental principles of transparency,

---

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

[2] 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.

[3] For example, we offer publicly-available interactive modules that make learning about our services and data ecosystem simple, fun and easy. Our "Learn Privacy and Data Protection" (at https://trailhead.salesforce.com/en/content/learn/trails/learn-privacy-and-data-protection-law) module has been widely viewed by our employees, customers and interested members of the public.

participation and accountability. This law should provide a foundation to support, not preempt, other federal laws that address uniquely-positioned sectors such as banking and health care. US consumers and businesses both will be optimally served by a unifying privacy framework that is fragmented neither by geography nor industry sector. We strongly support the Administration's risk- and outcome-based approach to privacy[4] and agree that being "overly prescriptive can result in compliance checklists that stymie innovative privacy solutions [and] … does not necessarily provide measurable privacy benefits."[5] Throughout our comments below, we will echo this conviction that any privacy legislation or framework should first consider the outcomes desired by consumers and align with the public's understanding of meaningful data protection.

Salesforce is aligned with the Privacy Outcomes set forth in the RFC.

1. *Transparency*

   Consumers should have a right to timely, accessible, meaningful and easily understandable notice of how their personal data is being used, and of the privacy and security practices of the companies that are using it. In keeping with the Administration's risk-based approach, if a company collects sensitive personal data from a consumer, the company should provide meaningful notice of its data processing practices directly to the consumer. If the collected data is not sensitive and direct notice imposes an undue burden (for example, in circumstances where there is no privity between the company that collects the data and the individual from whom the data is collected), the company should be required to post a notice of its practices in a clear, conspicuous and publicly accessible manner.

   For notices to be meaningful, the terms that companies use (which will necessarily track the terms used in applicable data protection laws) should be defined to comport with consumers' intuitive understanding of such terms. For example, "personal data" should be defined as exactly that — data that identifies or relates to a person, not (as we have seen in certain instances) a device or a household. "Sensitive personal data" should be defined as data the exposure of which poses material, heightened risks to a consumer's legal rights and vital interests — for example, medical records.

   Expanding the definition of personal data, as some have suggested, to include devices would lead to strange outcomes such as the protection of any data collected by an internet-connected vending machine in a shopping mall, regardless of whether that data related to a specific consumer. Similarly, expanding the definition of personal data to include households could lead to different members of a single household having the right to access one another's data, an outcome that in some circumstances could be dangerous.

   Relatedly, it is just as important to properly define what personal data is not. We believe that when data is anonymized such that it cannot reasonably be reassociated with a particular consumer, it should no longer be considered personal data — nor would it be by most

[4] *See* RFC at 48602.

[5] *Id.*

consumers. Some privacy law frameworks, notably the EU General Data Protection Regulation ("GDPR"), set the bar for anonymization so high (and require that the likelihood of reassociation be so low) that privacy research is in fact disincentivized. Companies will see no benefit in taking reasonable, effective steps towards better anonymization and encryption if those steps go unrewarded because the results are imperfect.

2. *Control*

Consumers should have a right to meaningfully participate in decisions regarding their personal data. If a company collects sensitive personal data from a consumer, it should do so on the basis of informed, opt-in consent or some other compelling legal justification. If the collected data is not sensitive, a company should be permitted to process the data if it has a legitimate interest in doing so and the risks to the consumer do not outweigh such interests.

If a company is processing a consumer's personal data solely on the basis of opt-in consent and the consumer withdraws that consent, the company should not discriminate against that consumer in service level or price. However, if the personal data is being processed on the basis of the company's legitimate interests (e.g., to engage in innocuous activities like suggesting similar products or services to a consumer who has previously purchased from or engaged with the company, or to monitor website access for technical issues or security threats), the company should not be required to continue offering services to a consumer who has opted out of providing his/her data. This requirement would hamstring many of our customers that offer free services underwritten by advertising and, if such companies respond by converting to subscription-based business models, potentially curtail the broad accessibility of their services.

3. *Reasonable Minimization*

Consumers should have a right to expect that companies will not collect personal data about them unless they have a legitimate interest in and specific purpose for doing so. Companies should delete a consumer's personal data upon request, unless the data is necessary to, for example, perform a contract, prevent fraud, or comply with a legal obligation. However, privacy outcomes should be compatible with other outcomes important to US consumers - therefore, deletion should not be mandated when the data concerned is a matter of public record, or when doing so would conflict with the freedom of expression or journalistic purposes. Exceptions should also be available for uses of data that are clearly for the public good - for example, scientific and medical research, which have benefited greatly from the availability of large data sets from which new insights may be drawn and against which hypotheses may be validated.

4. Access and Correction

Consumers should have a meaningful right to view their personal data and to challenge the accuracy and completeness of that data. However, requiring companies to produce each and every piece of data they maintain related to a given individual would simultaneously impose undue administrative burdens on companies and yield no meaningful privacy benefits to consumers. Instead, in keeping with the Administration's risk-based approach, a company should be required to describe to a

consumer, upon request, the categories of personal data regarding him or her that are being processed. Equipped with this information, the consumer would then have the right to follow up with the company to request more detailed access to data that is sensitive or poses particular risks. This type of proportionate and collaborative engagement between companies and consumers provides opportunities to address privacy concerns in a simple, direct and streamlined manner.

5. *Accountability*

Consumers should have a right to substantive privacy enforcement, including, when appropriate, the imposing of penalties when violations occur. However, any privacy legislation or framework should clearly distinguish between data controllers, which collect and process personal data for their own purposes, and data processors, which collect and process personal data on behalf of data controllers.

Due to the nature of our business and the services we provide, Salesforce normally acts in the role of a processor with respect to the data uploaded to our cloud software by customers. We take the confidentiality and protection of our customer's data very seriously, because we know that they themselves have made privacy commitments to the consumers from whom the data was collected. As a result, we impose strict internal controls on when (in rare circumstances) we may access customer data and when (in even rarer circumstances) we may process that data without express instructions from the customer.

Processors should be expected to assist controllers in fulfilling the latter's obligations towards consumers. However, other than in extraordinary circumstances, expecting processors to directly fulfill obligations towards consumers would require processors to make decisions regarding data into which they have limited visibility and over which they have no legal authority, breaching the contractual commitments they have made to, and the trust of, their controller customers.

In addition to the internal access controls we impose on customer data, our services implement the foregoing principles in a number of ways. For example, we enable our customers to put individuals in control of their own data by building functionalities that allow customers to track consent preferences; to tag, find, and delete, correct or anonymize personal data; and to encrypt data they upload to our systems. And we post our data processing addendum on our website so that our practices regarding customer data are transparent and accessible.[6]

Salesforce supports the Administration's high-level goals. In particular, we (i) favor harmonization of terms among data protection laws, (ii) recommend that the Administration proceed in a collaborative process with stakeholders and (iii) agree that the FTC is the appropriate federal agency to enforce consumer privacy.

Salesforce supports the administration's high level goals. We believe that many of these goals, including providing legal clarity while maintaining the flexibility to innovate, promoting interoperability, and incentivizing privacy research can be met by paying proper attention to how terms are defined.

[6] https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf

As discussed above, we are convinced that privacy protections should respond to consumers' actual concerns and, therefore, the terms of any legislation or framework should be defined to comport with consumers' intuitive understanding of such terms. Furthermore, we believe that doing so will promote interoperability between the regulatory landscape in the US and that in other countries, as would including commonly accepted legal concepts such as the controller/processor distinction.

Privacy is a concept that varies from culture to culture, and any national legislation or framework in the US should be based on this country's unique values. Although the substance of the GDPR may not always be the appropriate guide for how personal data should be protected in the US, we should look to the process by which that legislation was developed as a model for our own efforts. The EU spent years carefully considering, editing and revising the proposed text in a deliberative process that included stakeholders across government, civil society, traditional private business, the tech industry and academia. Although we believe that the time has come for a national basic privacy law in the US, we caution against any process that does not leverage the insights of diverse partners and leads to legislation that is not readily interoperable with existing protections across the globe.

We agree that the FTC is the appropriate federal agency to enforce consumer privacy. The FTC has a strong track record of aggressively investigating and sanctioning companies that violate consumer protection laws and doing so in a professional and unbiased manner. Further, FTC rulemaking would be a responsive and effective vehicle for addressing evolving privacy concerns and sensitivities. We believe that the FTC has the authority, expertise and institutional experience necessary to protect consumers' personal data and would welcome discussions regarding how the FTC could adjust or augment those resources to effectively assume new responsibilities.

* * * * *

We are encouraged by the Administration's efforts and look forward to further engagement with the NTIA. Salesforce remains committed to the success of our customers and we view our active participation in this important national discussion as advancing that success. We would be please to serve as a resource to the Administration as it further develops its consumer privacy approach.

Respectfully submitted,
Lindsey Finch
Senior Vice President,
Global Privacy & Product Legal