January 14, 2019

Katie MacFarland
National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, MD 20899

Re: Developing a Privacy Framework
Docket No. 181101997-8997-01

Comments of Salesforce.com, Inc.

Salesforce.com, Inc. ("we," "us," or "Salesforce") appreciates the opportunity to respond to the National Institute of Standards and Technology's ("NIST") Request for Information ("RFI") on the NIST Privacy Framework: An Enterprise Risk Management Tool (the "Privacy Framework")[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 we look forward to working 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 20 years ago.

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, participation and accountability. US consumers and businesses alike will be optimally served by an integrated Privacy Framework that is no longer fragmented by geography and industry sector, but offers instead a single, uniform approach.

In the comments below, we share the lessons we've learned, challenges we've overcome and best practices we've implemented over the course of two decades of securely, responsibly and transparently processing personal data on behalf of our customers. We hope that this information will help NIST "identify, understand, refine, and guide development of the Privacy Framework."[3] Salesforce strongly agrees with NIST that the Privacy Framework should be founded upon the attributes identified in the RFI.[4] Our comments are therefore set forth below as responses to, and discussions of each of, the identified

[1] Notice and Request for Information, Developing a Privacy Framework, 83 FR 56824 (Nov. 14, 2018) ("RFI").

[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] RFI at 58624.

[4] Id at 58624-5.

attributes and incorporate details regarding our organizational considerations, program structure and specific practices relating to privacy.

Consensus-driven and developed and updated through an open, transparent process

Privacy is a concept that varies from culture to culture, and the Privacy Framework should be grounded in American values. That said, we recommend that NIST mirror the process used by the European Union to develop its General Data Protection Regulation. The EU carefully considered, edited and revised the proposed text in a deliberative process that included stakeholders across government, civil society, traditional private business, the tech industry and academia. We support NIST's inclusive approach to the development of the Privacy Framework and recognition that parties with diverse viewpoints may nonetheless be aligned in their desire to enhance privacy protections for American consumers.

Salesforce views the protection of personal data as an opportunity to leverage a mutuality of interests between business and consumers. Trust among consumers, governments and businesses is the foundation of prosperity and innovation in a digital economy. Consumers expect products and services that are smart, personalized and responsive, and businesses rely on consumers' personal data to build these products and services. Governments have responsibilities to protect consumers and foster the conditions necessary for innovation and competition. At Salesforce, we proactively educate our customers about how their data is being used[5] and frequently receive feedback from our customers commending our outreach and transparency. We believe that the Privacy Framework, by providing further information and certainty to consumers, governments and business alike, will and should contribute to efforts to bolster public trust and confidence in personal data processing.

Common and accessible language

We agree that that the Privacy Framework should be "understandable by a broad audience, including senior executives and those who are not privacy professionals." Consumers cannot make informed decisions regarding their personal data without timely, accessible and meaningful notice of how their data is being used, and of the privacy and security practices of the businesses that are using it. Businesses, furthermore, need clear guidance from consumers regarding what can and cannot be done with their personal data, including how, why, when and where their personal data can be used or shared.

For notices to be meaningful and guidance to be clear, the terms that the Framework uses should be defined to comport with consumers' intuitive understanding of such terms. As was noted repeatedly during the October 16, 2018 workshop hosted by NIST in Austin, Texas, definitions matter.[6]

For example, "personal data" should be defined as exactly that — data that identifies or relates to a person, and not (as we have seen in certain instances) data about a device or a household. "Sensitive

---

[5] 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.

[6] https://www.nist.gov/news-events/events/2018/10/kicking-nist-privacy-framework-workshop-1.

personal data" should be defined as data the exposure of which poses material, heightened risks to a consumer's legal rights and vital interests (e.g., medical records).

Expanding the definition of personal data, as some have suggested, to include devices would lead to unintended 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 would undermine the notion of that data being "personal." Unorthodox definitions such as these would also impose significant monetary and bureaucratic costs and create consumer uncertainty by upending years of organizational, technical and administrative efforts among businesses like Salesforce to comply with longstanding data protection laws founded on traditional definitions.

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 consumers. Some privacy law frameworks set the bar for anonymization so high (and require that the likelihood of reassociation be so low) that privacy research may be disincentivized.[7] Businesses will see no benefit in taking reasonable, effective steps towards better anonymization if those steps go unrewarded because the results are imperfect.

Adaptable to many different organizations, technologies, lifecycle phases, sectors, and uses

We agree that widespread adoption of the Privacy Framework is only possible if the Privacy Framework is broadly applicable, but we caution against an inflexible approach. Rigid and undiscriminating language that attempts to address the circumstances of everyone will ultimately fail to address the circumstances of anyone; the best one could hope for with such an approach is to identify the lowest common denominator of privacy protections.

Instead, the Privacy Framework should acknowledge and clearly distinguish between, among other things, businesses in different sectors, marketing different technologies and using data in different ways. For example, a key distinction that should be incorporated throughout the Privacy Framework is 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 acts in the role of a processor with respect to the data uploaded to our cloud software by customers. We take the confidentiality, integrity and availability of our customer's data very seriously, because we know that they, in turn, have made privacy commitments to the consumers from whom the data was collected. As a result, we impose strict internal

[7] The European Union's Article 29 Data Protection Working Party, in its Opinion 05/2014 on Anonymization Techniques (available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf), states EU data protection law "clearly sets a very high standard [for anonymization]" (p. 6). Among the strictest frameworks, "the French Data Protection Law provides that data remains personal data even if it is extremely hard and unlikely to re-identify the data subject" (fn. 3).

controls on when (either with customer permission or as required by law) we may access or process customer data.

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.

Risk-based, outcome-based, voluntary, and non-prescriptive; Readily usable as part of any enterprise's broader risk management strategy and processes; Compatible with or may be paired with other privacy approaches

Salesforce strongly supports the development of a uniformly applied Privacy Framework that focuses on achieving meaningful privacy outcomes, rather than prescribing specific protocols. We want the Privacy Framework to augment, rather than conflict with, the extensive data protection efforts we currently undertake in compliance with the multiple regulatory regimes applicable to us as a global company.

We also strongly support a risk-based approach as a critical, common sense component of the Privacy Framework. For example, Salesforce believes that consumers should have a meaningful right to view their personal data and to challenge the accuracy and completeness of that data. However, requiring business to produce each and every piece of data they maintain related to a given individual would simultaneously impose undue administrative burdens on businesses and yield no meaningful privacy benefits to consumers. Instead, a business 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 business to request more detailed access to data that is sensitive or poses particular risks. This type of proportionate and collaborative engagement between business and consumers provides opportunities to address privacy concerns in a simple, direct and streamlined manner.

Salesforce protects personal data through a variety of organizational, technical and administrative measures.

Organizational measures

Salesforce's management of privacy risk is overseen by the Board of Directors (the "Board"). This oversight is conducted primarily through committees of the Board. Specifically, the Audit Committee oversees enterprise risks associated with data security and regularly discusses and provides guidance to senior management regarding Salesforce's data security strategy, risk monitoring and mitigation. The Board also includes a Privacy Committee, which is tasked with providing guidance regarding Salesforce's approach to personal data protection, including conducting assessments of acquisition targets and strategic initiatives.

We incorporate privacy and data protection concepts into our product lifecycle from the design phase to the marketing of new services and features. Salesforce's Privacy team regularly educates and trains

product managers and engineers on how to incorporate the principles of privacy by design into our products and features. In addition, each Salesforce service is supported by at least one product attorney knowledgeable about data protection who reviews and advises on the product's functionality. And each of those attorneys is supported by a privacy attorney who specializes in data protection full-time. The product release cycle also contains multiple checks where additional people can provide comments on the service or features' protection of personal data. Finally, when a service or feature is released, it is described in product documentation and release notes so that customers can perform their own evaluations.[8] Salesforce regularly considers input from its customers when designing and refining product functionality.

Salesforce's Security team is responsible for security-related technology policies and procedures. Salesforce's Privacy team is responsible for designing, implementing and ensuring compliance with Salesforce's privacy program.

Technical measures

As a data processor, we respect the confidentiality of our customers' data and do not access any customer's instance without that customer's permission or as required by law. Further, our customers may configure their instances to meet their specific business needs. Therefore, we go to great lengths to empower our customers to put individuals in control of their own data by building functionalities into our services 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.

We have also directly implemented an array of technical measures to help secure our services. These measures, which may vary by service, include protections against system vulnerabilities, logical separation of Customer Data, network security, encryption of data and identity authentication protocols.

Administrative measures

When a customer submits data to our services, we process that data in accordance with that customer's instructions to us and we have implemented procedures designed to ensure the customer's data is processed only as instructed throughout the entire chain of processing activities by Salesforce and its sub-processors. In particular, Salesforce and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the organizational and technical measures implemented by Salesforce and its sub-processors are subject to regular audits and certification by multiple third parties.

Our standard data processing addendum is publicly available[9] and includes (i) an obligation for Salesforce to use and disclose personal information only in accordance with our customers' instructions; (ii) a commitment to assist customers in responding to the exercise of rights by individuals whose personal

[8] https://help.salesforce.com/articleView?id=000181590&type=1.

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

information is processed by customers on Salesforce's services; (iii) provisions related to confidentiality obligations of Salesforce's personnel; (iv) obligations regarding Salesforce's use of subcontractors engaged in the processing of personal data; (v) information about Salesforce's security controls; (vi) security breach notification commitments; (vii) provisions governing the cross-border transfer of personal data; and (viii) details regarding Salesforce's return and deletion of customer data.

We further manage privacy risk by developing and continually improving our comprehensive privacy impact assessment program. The program promotes and institutionalizes fundamental privacy principles by requiring that services or features that may use personal data in novel ways first undergo an assessment of the risks posed to individuals whose data will be processed. We also maintain a robust inventory of core processing activities and data assets to support the privacy impact assessment program and to rapidly respond to requests from individuals regarding our use of their personal data.

Salesforce also communicates with our customers and end users about privacy topics through a number of channels, including publicly available interactive learning modules, a landing page on the European Union General Data Protection Regulation[10] and our Trust landing page[11].

A living document

Salesforce agrees that the Privacy Framework should updated periodically to address new challenges and opportunities posed by technological innovation and emerging trends in data governance and use, and to incorporate lessons learned.

* * * * *

We are encouraged by NIST's efforts and look forward to further engagement. 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 pleased to serve as a resource to NIST as it further develops the Privacy Framework.

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

[10] https://www.salesforce.com/gdpr/overview.

[11] http://trust.salesforce.com.