Response to the National Telecommunications and Information Administration's Request for Comment on Developing the Administration's Approach to Consumer Privacy

Docket No. 180821780-8780-01
November 9, 2018

Workday is pleased to have the opportunity to provide input in response to the National Telecommunications and Information Administration's Request for Comment on Developing the Administration's Approach to Consumer Privacy.

At Workday, privacy protections have been a fundamental component of our services from the very beginning. Our third-party audit reports and standards certifications provide tangible evidence of how we protect our customers' data. When we develop new offerings we implement privacy by design from the very beginning. We have received approval from EU privacy regulators for our Binding Corporate Rules and were among the first companies to certify to the EU-U.S. Privacy Shield protecting personal data transferred from the EU. And we've built features that enable our customers to comply with the European Union's General Data Protection Regulation. In addition, we were the first U.S. company to be certified under the APEC Privacy Recognition for Processors system.

As we look forward, much of the current discussion around privacy is driven by new possibilities unlocked by artificial intelligence (AI), machine learning, and big data analytics. To power these technologies, multiple data sources are brought together to generate insights and make predictions across a wide range of use cases. Over the last few years, these technologies have initiated changes in ways unfathomable just a few years ago. At the same time, however, we've seen some cases involving misuse of consumers' data, resulting in questions about whether data technologies respect individuals' privacy. But in the enterprise context, data-fueled AI and advanced analytics are quietly improving business processes, increasing worker productivity, and surfacing patterns that help business leaders make better decisions—all while incorporating strong privacy protections.

As a proponent of AI and advanced analytics, we have reaffirmed Workday's continued commitment to privacy. First and foremost, the personal data our customers share with us is their data. We believe strong privacy protections can live in harmony with the data needs of advanced analytics and increased data-driven decision making. In fact, strong privacy protections can empower greater innovation. To that end, we have committed to three core privacy principles:

- Put Privacy First
- Innovate Responsibly
- Safeguard Fairness and Trust

Workday also believes that privacy rights must be protected through strong legislation and enforcement that ensures ethical use of individuals' information. As we have noted, and the Request For Comment describes, the U.S. has a long privacy law tradition, stretching back to the 19th century and providing the doctrinal foundation for the Organization for Economic Cooperation and Development Fair Information Principles. In addition to this heritage, the U.S. currently has a number of strong sector-specific privacy laws governing financial institutions, health providers, educational institutions, and children, in addition to all 50 states' data breach notification laws. Overlaying all of these, the Federal Trade Commission enforces prohibitions on unfair and deceptive trade practices.

While the U.S. privacy framework is stronger than it is often given credit for, from the outside, the disparate structure of U.S. privacy law makes it difficult for other countries to identify strengths or determine whether gaps exist in protection. As a result, the EU requires U.S. companies to certify to the Privacy Shield or enter into other arrangements to ensure data transferred to the U.S. benefits from substantially similar protections as under European privacy law.

In our view, the U.S. and other countries around the world should adopt privacy laws based on the OECD Fair Information Principles. As privacy is a fundamental value around the globe as well as in the U.S., it is incumbent on the U.S. to lead by having a modern legal framework protecting the privacy of its citizens. While we recognize that the RFC does not itself call for enactment of legislation, we believe that desired levels of protection, and the outcomes sought by the RFC, can only be achieved via a comprehensive Federal data privacy law.

Most importantly, a law based on the OECD principles will ensure fair treatment of individuals and their personal information, regardless of where they live or with whom they interact. The OECD principles provide a widely-shared common baseline for the 35 countries that are OECD members. The voluntary OECD principles cover all the core tenets of data privacy rights—data collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. Enacting these principles in U.S. national legislation should result in U.S. law being deemed adequate by the EU and will facilitate the continued free flow of personal data.

In fact, perhaps the best way to ensure that U.S. industry continues to serve as global leaders is by ensuring personal data can flow seamlessly across borders and removing any unnecessary frictions. While U.S. privacy law must reflect our legal and political traditions, The OECD principles are sufficiently flexible to ensure U.S. privacy law reflects our legal and political traditions as well as support country-to-country variation while enabling and sufficiently strong to provide the global interoperability necessary in a cloud-enabled world. international harmonization to ensure that personal data can flow freely across borders in a cloud-enabled world.

Turning to the specifics of the consultation, we appreciate the thought that NTIA has put into the proposed outcomes of Federal action related to privacy. The outcomes correlate well with the OECD FIPS – in particular

workday.com 6230 Stoneridge Mall Road, Pleasanton, CA 94588 +1.925.951.9000

they reflect the Collection Limitation, Security Safeguards, Openness, Individual Participation, and Accountability Principles. That said, there are some omissions:

- The Data Quality Principle, which requires that personal data "be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date," doesn't appear to be reflected. Data quality is a separate concept from data minimization (which is reflected in the OECD's Collection Limitation Principle) and should form part of any Federal privacy framework.
- Similarly, while the proposed outcomes include both a Transparency and a Reasonable Minimization prong, they fall short of the Use Limitation and Purpose Specification Principles, which provides that data should not be used for incompatible purposes. The Transparency prong requires users to understand how an organization uses their data, while the Reasonable Minimization prong requires that data use and sharing should be minimized as appropriate. But still missing is a restriction on using personal data for new unanticipated purposes.

With respect to the goals for Federal legislation, we broadly share the goals outlined in the RFP. Workday supports comprehensive Federal legislation in order to ensure a harmonized legal environment in the U.S. that protects all individuals. The current sector-specific approach is hard to navigate, leads to different protections depending upon the entity collecting and using the data, and has significant gaps. The legal clarity that a comprehensive Federal law would bring would not only address these challenges, but would empower individuals and also help incentivize further innovation by providing consumers confidence that their personal data will remain protected even as that data is used to enable new technologies like artificial intelligence and machine learning.

Similarly, Workday believes that interoperability with other legal regimes is essential in a world where data flows across borders. The Workday service processes transactions in the HR and Finance areas, as well as enables analyses across a company's workforce. We also provide enhanced data analytics through our Prism Analytics and Workday Benchmarking offerings. To do all this, customers have to bring data together in a single tenant in a single data center region, so that transactions can be processed and analyses run across the entire data set. Without free flow of data, the full potential of cloud services such as Workday's cannot be realized. To that end, we think that any Federal legislation should be sufficiently robust and aligned with privacy norms worldwide – as set forth in the OECD FIPS – so as to be a credible candidate for an adequacy determination by the European Commission.

Part of that involves strong and effective enforcement. We agree with the RFP that the Federal Trade Commission has established itself as a strong and effective privacy regulator. We further agree that additional resources and statutory authority – including rulemaking authority – would position the FTC to continue to provide effective accountability, as well as enhance legal clarity without waiting for caselaw to develop.

workday.com 6230 Stoneridge Mall Road, Pleasanton, CA 94588 +1.925.951.9000

Lastly, we agree that comprehensive application should be a hallmark of federal action on privacy and congratulate the NTIA on recognizing the nuance of the tech industry. The RFC notes that differences in business models should be addressed. The tech industry is far from monolithic and replete with varying business models including enterprise-based companies like ourselves that operate in the cloud. Rather than monetize personal data, cloud-based enterprise companies often operate predominantly in the business-to-business market and provide subscription-based services that protect data privacy, streamline processes, and increase efficiencies for companies throughout the U.S. and global economy. Both recognizing and addressing such differences will be key to the successful application of any federal privacy action that seeks to maintain prosperity and innovation while protecting personal data.

Thank you for the opportunity to provide input in response to the Request for Comment on Developing the Administration's Approach to Consumer Privacy. We stand ready to provide further information and to answer any questions. Please do not hesitate to reach out to Chandler C. Morse at chandler.morse@workday.com for further assistance.

workday.com 6230 Stoneridge Mall Road, Pleasanton, CA 94588 +1.925.951.9000