FTC Topic #4:
The intersection between privacy, big data, and competition

Of particular interest to the Commission: (a) data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market; (b) competition on privacy and data security attributes (between, for example, social media companies or app developers), and the importance of this competition to consumers and users; (c) whether consumers prefer free/ad-supported products to products offering similar services or capabilities but that are neither free nor ad-supported; (d) the benefits and costs of privacy laws and regulations, including the effect of such regulations on innovation, product offerings, and other dimensions of competition and consumer protection; (e) the benefits and costs of varying state, federal and international privacy laws and regulations, including the conflicts associated with those standards; and (f) competition and consumer protection implications of use and location tracking mechanisms.

Workday, a leading provider of enterprise cloud applications for finance and human resources, is pleased to submit comments in advance of the Federal Trade Commission's hearings on competition and consumer protection in the 21st century. Founded in 2005, Workday delivers financial management, human capital management, and analytics applications designed for the private sector, educational institutions, and government agencies and we work with organizations representing more than 31 million workers. Workday is headquartered in Pleasanton, California, with offices and customers across the U.S. We empower enterprises to process a wide variety of HR and finance-related transactions, gain new insights into their workforces and financial performance, and manage employees and financial outcomes consistently on a company-wide basis through our cloud-based applications. Workday's applications give customers real-time insights into their organizations, allowing them to make decisions based on data rather than guesswork. Being in the cloud also means that customers have access to their financial and workforce data whenever and wherever they need it, on any device. For employers, this translates to an ability to better manage the business, and for employees, it simplifies many daily transactions and democratizes access to critical data.

b. Competition on privacy and data security attributes

Workday believes that increasingly competition on privacy and security attributes plays an important part in markets for cloud services. From the very beginning, Workday has implemented strong privacy and security protections into our cloud service. We did so for two reasons. The first was customer demand. To convince enterprises to place their human resources data in a cloud service, we needed to give them confidence that their information would be protected. After all, in addition to being confidential personal information of their employees, it constitutes sensitive business information of our customers. We—and other tech companies—have consistently marketed our privacy protections and competed on the basis of how our services enable compliance with privacy laws and regulations worldwide as well as best practices. Given our business, this is a discussion we have with every customer of our service, often in significant depth.

The second reason was the need to comply with privacy laws and regulations around the world, in order to provide a global service. Beginning with the European Union's Data Protection Directive in 1995, privacy laws has proliferated globally, with significant legislation in Argentina, Australia, Canada, Israel, Japan, the Philippines, and New Zealand, just to name a few countries. Voluntary privacy frameworks, such as the APEC Cross-Border Privacy Rules have also gained currency across regions. Our customers, many of which are large multi-nationals, expect features and functionality to enable their compliance with this plethora of privacy regulations.

Our privacy-related features and our privacy compliance program, evidenced via our SOC reports and compliance with international standards, are an important differentiator in the market. As noted above, privacy protections have been a fundamental component of our services from the very start. When we develop new offerings we implement privacy by design from the very beginning. And we have built numerous features that enable our customers to meet their privacy obligations, including the ability to restrict managers' access to data, a privacy purging function, and an audit trail of every change made.

Our third-party audit reports and standards certifications provide tangible evidence of how we protect our customers' data. Workday provides our customers with independent third party audit reports such as Service Organization Control (SOC) 1 and SOC 2, as well as certifications to ISO/IEC 27001, ISO/IEC 27018, and PCI-DSS. Our most recent SOC 2 report covers all of the available AICPA Trust Services Principles: privacy, security, confidentiality, availability, and processing integrity. In addition, 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

d. The benefits and costs of privacy laws and regulations

Workday further believes that privacy law and regulations bring important benefits. Privacy is an important shared value, one government and industry must work together to protect. While we are proud of Workday's industry-leading privacy program, because privacy is a fundamental value, it is incumbent on the U.S. to lead by having a modern legal framework protecting the privacy of its citizens. As described below, a Federal privacy law based on the OECD Fair Information Principles will ensure fair treatment of individuals and their personal information, regardless of where they live or with whom they interact.

We think that the U.S. should adopt a comprehensive Federal privacy law based on the OECD Fair Information Principles. The U.S. has a long privacy law tradition, stretching back to the 19th century. Modern Federal privacy rules began with the Department of Health, Education, and Welfare publishing the Fair Information Practices Principles in 1973. The development of these principles was driven by concerns about the increased computerization of personal records and the trend—which has only grown since—of using Social Security Numbers as universal identifiers. Importantly, these principles served as the foundation of the Organization for Economic Development and Cooperation's Fair Information Principles, adopted in 1980, which in turn underpin privacy laws around the globe, including the EU's General Data Protection Regulation. While U.S. privacy law must reflect our legal and political traditions,

the OECD principles reflect a common international baseline and are sufficiently flexible to support country-to-country variation.

Privacy legal protections are essential if people are to feel comfortable with their information being used for new technologies like machine learning and artificial intelligence. Artificial intelligence, machine learning, and big data analytics hold the potential to transform our world, opening up new insights and possibilities for companies, employees, and individuals alike. For example, Workday's Opportunity Graph helps workers advance in their career by showing where prior holders of the role went next, and what skills they needed to get there. But individuals will not feel comfortable with these uses of their data unless they are sure that strong privacy protections apply. A comprehensive Federal privacy law based on the OECD Principles will create an environment that facilitates new developments that will help everyone.

e. The benefits and costs of varying state, federal and international privacy laws and regulations

The divergence of privacy laws, both internationally, among states, and among the separate sector-specific regimes at the Federal level, impose two significant costs on business. The first is an increase in the cost of compliance, as differing requirements—everything from notice requirements, to data retention, to access and deletion—require changes in processes and technology to enable compliance. To mitigate this, we believe that international convergence is important, which is why we support Federal privacy legislation based on the OECD Principles, which underlay most data privacy laws today. Similarly, Federal legislation, by pre-empting conflicting state requirements, will help ensure uniformity within the United States.

The second cost is challenges to the ability of data to flow freely across borders. Free flow of data is essential to the continued growth of cloud services, and international convergence around privacy laws will help enable cross-border data flows. While the U.S. has strong privacy protections, the disparate structure of U.S. privacy law makes it difficult for other countries to determine whether gaps exist in protection. As a result, the EU requires U.S. companies to certify to the EU-U.S. 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.

The OECD Principles are sufficiently strong to provide international harmonization to ensure that personal data can flow freely across borders in a cloud-enabled world. They 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. Federal legislation should help U.S. law to be deemed adequate by the EU and thereby facilitate the continued free flow of personal data.

* * *

Thank you for the opportunity to submit comments in advance of the hearings. We stand ready to provide ! further information and to answer any questions you may have. Please do not hesitate to reach out to ! Jason Albert if we can be of further assistance.