Office of the Vice President
Government and Regulatory Affairs

600 14th Street, N.W., Suite 300
Washington D.C., 20005

November 9, 2018

Mr. Travis Hall, Telecommunications Policy Analyst
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W., Room 4725
Washington, DC 20230
Attention: Privacy RFC

Subject: IBM Comments in NTIA's Request for Comment on Administration's Proposed Approach to Consumer Privacy, Docket No. 180821780-8780-01

Dear Mr. Hall,

I am writing on behalf of International Business Machines Corporation ("IBM") in response to the National Telecommunications and Information Administration's (NTIA) inquiry about a proposed approach for protecting individuals' privacy while fostering innovation, as set forth in the Request for Comment (RFC).

IBM supports national legislation to protect consumers' privacy. The key question is how best to develop such legislation. We believe that the best approach to privacy in the United States is to involve a wide range of stakeholders, to take the time necessary to build consensus, and to build from the "ground up" through government-industry consultation and cooperation. We believe a framework approach – as proposed in the RFC -- in which industry, government, and civil society collaborate to produce best practices and standards that are eventually incorporated into law is the most effective approach. These best practices and standards can be developed through NTIA's proposed approach of user-centric

privacy outcomes for consumers and high-level goals to create the ecosystem to provide these protections, as well as through the complementary work already underway at the National Institute for Standards and Technology (NIST) to develop an enterprise risk management tool for protecting consumers. National legislation also should reduce fragmentation and facilitate global interoperability of privacy standards, including by pre-empting inconsistent state or local law when necessary.

We arrive at this view in favor of an inclusive, collaborative approach for two reasons. First, evolving privacy legislation around the world, including the European Union General Data Protection Regulation, is focused on the principles of transparency and accountability. Recognizing that no one regulatory regime can serve as one-size-fits-all, we support a flexible U.S. framework that is grounded in these global principles but that is tailored to and appropriate for the U.S. regulatory context – in other words, a framework that is workable for U.S. consumers, businesses, and regulators. A collaborative approach where all stakeholders work together to develop draft privacy legislation will result in an adaptable, dynamic system for protecting consumer privacy that also will foster innovation and preserve America's competitive advantage in emerging technologies. Our company has long recognized the power data holds for our clients. Therefore, privacy policy, especially legislation, must take into account its effect on emerging technologies and the impact on U.S. competitiveness, while achieving greater protections for U.S. consumers.

Second, this same collaborative public-private approach has been used previously to strengthen U.S. cybersecurity protections, and we believe it also will be successful for strengthening U.S. privacy protections. In the aftermath of comprehensive cybersecurity legislation failing in Congress and cyber intrusions into critical infrastructure increasing, the Obama Administration in 2013 issued an executive order calling on NIST to lead a collaborative effort between government, industry, and academia to develop cybersecurity standards. A year later, the NIST Cybersecurity Framework was released and quickly became the blueprint for cybersecurity in the private sector. In 2014, the bipartisan Cybersecurity Enhancement Act of 2014 supported NIST's continued work on this voluntary Framework. And in 2017, President Trump mandated use of the NIST Framework by U.S. Government agencies to manage their cyber risk.

IBM recognizes that these collaborative processes take time and that consumers are rightfully concerned right now about their privacy. IBM urges the Federal Trade Commission to use its regulatory enforcement tools to strengthen protections for consumers, especially in areas of acute public concern.

As more and more organizations interact with and manage data, all have an obligation to do so responsibly, especially with respect to privacy. The difficulty of addressing such a complex issue across the breadth of the U.S. economy through legislation should not be underestimated. IBM strongly urges a bottom-up, collaborative approach for developing a framework for protecting consumers' privacy and then reflecting the best practices and standards developed through this process in law. This is the most effective way to develop legislation tailored to America's needs.

Sincerely,

Christopher A. Padilla
Vice President
Government and Regulatory Affairs