Remarks of Kelly R. Welsh
U.S. Department of Commerce General Counsel
Network Advertising Initiative Member Summit
New York, NY
5.21.15

Thank you to the Network Advertising Initiative (NAI) for giving me the opportunity to speak at today's Member Summit. I am Kelly Welsh, General Counsel of the U.S. Department of Commerce.

Under Secretary Penny Pritzker, the Department has made fostering the digital economy central to our mission to promote innovation, growth, and jobs. As NAI members know well, the rapid expansion of the digital economy contributes significantly to economic growth. The bureaus at the Department of Commerce advise the Secretary and President Obama on Internet policies, facilitate international trade and support open Internet policies, and develop research and standards to assist the digital economy.

Today, I will talk about the Obama Administration's recent review of the extraordinary benefits---and the risks to personal privacy---from big data. Finding the right balance between enabling big data and protecting privacy rights will pose challenges. Meeting these challenges holds great promise. And, when combined with borderless, secure data flows and an open Internet, big data can have a transformative and positive effect on the global digital economy.

The Impact of Big Data

The impact of big data will become pervasive as the amount and types of data collected continue to increase and the costs to analyze and store data continue to fall. Big data will drive new cross-disciplinary business models that will disrupt existing industries and create new ones. Energy companies will create adaptive power grids. Cities and municipal services will become smarter. Transportation and manufacturing will become more efficient. Consumers will have better, more-personalized goods and services. And individuals will interact with data of all types, through cloud-based applications and devices and the internet of things. From the largest corporations to the smallest start-ups, companies will be evaluated by how well they leverage data.

Last year, Secretary Pritzker and the Department of Commerce participated in the Obama Administration's in-depth review of the topic of big data, including its implications for privacy.

The Administration review team's Big Data Report affirmed that big data analysis has a tremendous opportunity to drive economic growth and innovation. This economic growth largely will be driven by innovation, entrepreneurship, and investment by the private sector. And this growth will be driven by digital economy innovations not just in northern California, but in New York, Chicago, Stockholm, Berlin, and throughout the

world. The United States is a leader in data analytics, and we need to ensure that continues.

The public sector can support this growth in a number of ways, including by remaining committed to open data initiatives. For example, at the Department of Commerce, we historically have used only a small slice of the data that our weather satellites, ocean sensors, and demographic surveys collect. Today, we are learning how to open up more of this information to businesses and individuals so that they can analyze and apply it in new, beneficial, and profitable ways. For example, last month we announced a public-private partnership with Amazon, IBM, Microsoft, Google, and the Open Cloud Consortium to release vast amounts of data from the National Oceanic and Atmospheric Administration (NOAA). In addition, we recently hired our first-ever Chief Data Officer to ensure that we are making the best use of our data and unleashing more of it in more accessible ways to promote economic growth.

The Department of Commerce also is facilitating collaborative efforts among communities and innovators to use data-driven technologies. For example, the Department's National Institute of Standards and Technology (NIST) is currently conducting a Global City Teams Challenge to foster the development of "smart cities." This effort is focused on taking advantage of networked technologies to better manage resources and improve urban quality of life using the massive amounts and types of data generated by the Internet of Things.

Big Data Benefits in Healthcare

In the Administration's Big Data review, we also found that big data poses new challenges for our deeply held values around privacy and autonomy.

One area where both the benefits and the risks of big data are starkly apparent is in the field of healthcare. As we described in the Big Data Report, big data can help identify diet, exercise, and other lifestyle factors that contribute to better health and reduce the need for professional attention.

From a cost-efficiency perspective, big data analysis also can be used to ensure medical professionals have strong performance records and are reimbursed based on the quality of patient outcomes rather than on the quantity of care delivered.

The emerging practice of predictive medicine is the ultimate application of big data in healthcare. This powerful medical research draws insights from large data sets---from genomic data to the heart rates monitored by our phones---that allow doctors to better anticipate whether individuals will develop an illness and how specific individuals might respond to therapies. In addition, real-time health monitoring will allow diagnoses to be made and treatment to be provided with life-saving speed and coordination.

The United States is encouraging this type of research through programs such as the "Big Data Research and Development Initiative," a whole-of-government effort to improve the tools and techniques needed to access, organize, and analyze large volumes of data. This Big Data Initiative is currently working on a strategic plan to guide big data research.

As an example of this type of research, the Cancer Genome Atlas, a program funded by the U.S. National Institutes of Health, is using large data sets to map the genetic changes in more than 20 cancer types.

Privacy Risks in Healthcare

Obviously, the potential benefits of big data in the healthcare field are enormous. Yet healthcare also highlights the risks of big data for privacy values and the need to protect those values---ultimately finding a balance between the benefits and risks of big data.

All privacy risks and concerns are not equal. For most people, whether a marketer knows what cereal you like best is a trivial concern compared to maintaining the confidentiality of your health records. Privacy with respect to one's medical information is a deeply held value. In the United States, a Pew Research Center study recently found that 55% of adults considered the state of their health and the medications they took to be very sensitive information. Fewer than 10% of adults said the same thing about the media they liked or their basic purchasing habits.

Nevertheless, the critical importance of being able to use big data to advance medical science requires all of us to think hard about how to maintain fundamental notions of personal medical privacy without unduly inhibiting medical research based on big data. As we chart new ways to maximize the benefits of data, we should consider carefully the risks and potential harms of various approaches and find a balance that we are comfortable with.

Big data analysis also will challenge how we think about what makes data sensitive. For example, changes in how we interact with others through social media could help indicate the early onset of conditions such as depression.

No matter how useful this information might be for making diagnoses, there are obvious and significant implications from a personal privacy perspective. Among other things, we will need to consider how analyzing this type of information fits with traditional notions of medical notice and consent. Big data will be able to drive life-saving advances, but the medical community must be able to have, and keep, the trust of patients and the public.

In the U.S., one of the ways privacy is protected is through strong sector-specific laws. For example, the Health Insurance Portability and Accountability Act places limits

on the use and disclosure of an individual's "Protected Health Information" by certain entities and provides ways to access and correct inaccurate health information.

In the future, we should examine ways to strengthen and expand such protections. For example, we should consider better ways to control access to information across many different types of health records. Work in this area should focus on protecting personal privacy without stifling innovation.

Big Data & Privacy in Education

Education is another field in which the benefits of big data are dramatic. Children will increasingly learn in digital classrooms. Schools will be able to apply big data analyses to the data students generate, thereby learning which lesson plans work best for which children.

The Obama Administration is committed to using data to drive technological advances in education. For example, though the ConnectED Initiative, students will receive next-generation Internet access, teachers will receive better training on the use of technology, and private-sector innovation will facilitate better, more-personalized learning opportunities.

Using big data, digital textbooks will help students visualize and interact with complex concepts, and educational devices and online courses will be able to adapt to the ability levels of individual students in real-time. Teachers and parents when appropriate---and the students themselves---will be better able to assess how well students are learning.

Data-driven technology also can make education more affordable and accessible, and it can focus students on the skill sets businesses will require in the future.

At the same time as we recognize the value of these innovations, it is also obvious that the convergence of big data and education has important implications for privacy. Digital education will generate massive amounts of data about school children, including data regarding their responses and behavior as they learn.

Learning is personal and the data will be too. Some student-related data---including data that could be very useful in improving educational performance---will push the boundaries of what we think of as educational information. For example, big data analyses could be applied to keystrokes and eye movements that reveal how engaged students are as they read, and who might be struggling with the material.

Moreover, learning-related data will be able to be shared and stored with ease, which could allow students' educational histories to follow them throughout their school years and into the workforce. And education data could be used to develop consumer profiles of students and market commercial products and services to them.

In the U.S., student privacy is protected through a number of laws. At the federal level, the Family Educational Rights and Privacy Act restricts the disclosure of certain educational records and information, and the Children's Online Privacy Protection Act provides parental notice and consent requirements, and limits marketing to young children.

In January, building on the recommendations in the Big Data Report, the President released a legislative proposal called the Student Digital Privacy Act. The proposal is designed to provide teachers, parents, and students with confidence in education technology by ensuring that data collected in the educational context is used only for educational purposes. The goal is to restrict the sale of student data to third parties for purposes unrelated to the educational mission and to place limits on targeted advertising to students based on data collected in school---while still permitting important research to improve student learning.

Last month, Congress took an important step forward for student privacy by introducing a bipartisan bill along these lines. The Administration looks forward to working with Congress to advance legislation that provides meaningful privacy protections and help spur innovation in the way we educate.

Consumer Privacy

At the Department of Commerce, we have worked for several years on how to address big data and privacy in the broader commercial context.

The United States has a robust privacy regime. We go to great lengths to make sure that consumers' privacy is protected, while allowing our entrepreneurs to build and grow businesses that lead the world economy.

In this digital age, where nearly every commercial interaction involves the use of personal data, it has come time to consider ways to broaden and enhance our privacy regime. Even though responsible companies provide us with tools to decide how our personal information is used, many of us still feel a loss of control over our data. As the digital economy expands, we will need to consider more comprehensive privacy protections in order to empower consumers and sustain their trust.

Consumers derive tremendous benefits from data-driven services. But these services can only thrive if consumers are comfortable that their personal data will be handled responsibly. For example, recent studies by the design firm Frog reported in the Harvard Business Review reveal that Internet consumers generally worry about their personal data and have low awareness of what types of data they are sharing when they go online and how they are sharing it. However, consumers who trust the companies they interact with and understand the value that they receive for their data are more willing to provide their data and participate in the digital economy. This of course matters not only for consumer-facing companies that require data to fulfill

transactions, but also for third parties that facilitate digital transactions through data-driven advertising.

For years, the legislative debate over how to provide consumers with more confidence, and businesses with more clarity, about the rules of the road for the use of private information has been stalled.

In February, the Obama Administration released a discussion draft of legislation with the aim of pushing the discussion and moving forward toward comprehensive legislation.

Privacy legislation must reflect a balance between enhancing consumers' practical privacy protections and control over their data, which they deserve, while at the same time fostering digital innovation that has grown the economy and created jobs. We attempted to achieve that balance through our draft legislation.

The discussion draft would apply to most companies that collect certain amounts of personal data. It would provide commonsense protections to personal data collected online or offline regardless of how data is shared. The goal is to promote responsible practices that can maximize the benefits of data analysis while taking important steps to minimize risks.

The draft would provide consumers with a number of benefits. For example, consumers would receive up-front notices telling them how their information will be collected, used, and shared. Consumers also would have the opportunity to correct inaccurate information and to cancel their accounts and remove their data. Companies would be allowed to collect and use personal data in ways that consumers reasonably expect, and they would provide heightened controls if their data practices present serious risks or would cause surprise and concern. The draft also would establish reasonable data security measures to address the risk of harmful data breaches.

At the same time, the discussion draft recognizes the dynamic nature of the digital economy by making clear that companies can collect and use data for customary business purposes, and to protect consumers, respond to their preferences, and improve services.

In part, the draft strikes a balance by pairing high-level protections with the ability for companies to develop codes of conduct for specific business contexts. The intent is to avoid a top-down approach that imposes onerous regulations ill-suited to a rapidly evolving environment. Instead, we favor encouraging a bottom-up approach driven by data users as well as the full range of stakeholders who understand how protections can best be applied to particular situations---NAI itself has encouraged the use of strong, scalable, and enforceable industry driven standards that emphasize consumer education and control. These codes of conduct could be developed through multi-stakeholder processes and, when approved by the Federal Trade Commission, they

would provide a safe harbor for companies that follow them. This flexible approach would evolve with changes in technology, business practices, and consumer behavior.

The Department of Commerce's National Telecommunications and Information Administration (NTIA) has contributed to this area by conducting a multistakeholder process on mobile app transparency that resulted in a code of conduct currently being implemented by a number of tech companies.

One of the objectives of the Administration's discussion draft of privacy legislation is to advance the conversation on how companies can best meet consumer demands and innovate in today's increasingly big data-fueled economy. The right mix between empowering companies to responsibly use data to offer new products and services and fostering a sense of consumer trust in how companies use their data is a topic for ongoing consideration.

Some people may not be comfortable with collecting and using certain types of data. Others will favor experimental uses of big data if the benefits are great and the privacy risks can be minimized. As we make these decisions, we should remember that the benefits and risks we are balancing will continue to change.

In a year or two, the advantages of engaging certain types of big data analysis may outweigh the disadvantages we perceive today; or vice versa. Accordingly, we should keep open the lines of communication between innovators and entrepreneurs on the one hand and privacy organizations and professionals on the other. The era of big data will be dynamic, and we will need to work with and understand the latest and best science and technology. We also should preserve sufficient flexibility in our legal standards to be able to incorporate future advances into our legal determinations.

Privacy-Enhancing Technologies

In addition to policy, we should focus on how we can leverage technology to improve privacy protections. It is important not to view the privacy challenges posed by big data as frozen in time. Just as the benefits and risks of big data are changing at an extraordinary pace due to innovation, new ways to minimize the risks can be developed. Privacy protections, like many other aspects of our economy, can benefit from innovation.

For example, the Department of Commerce's National Institute of Standards and Technology is engaging with technologists, businesses, academia, and civil society to work on privacy engineering. The goal of this open process is to bridge the communication gap between policy and design engineering in the privacy space. Using lessons learned in the cybersecurity space, NIST is exploring privacy risk management models, privacy design objectives, and privacy-enhancing systems development.

Research on privacy-enhancing technology is ongoing. For example, we are looking at the concept of differential privacy, which recognizes that granting access to

personal data in a particular context or with respect to certain information is not all or nothing. Differential privacy attempts to minimize privacy risks while maximizing the benefits of data analysis.

In practice, this can be done by introducing random data into data sets and employing algorithms to ensure certain types of searches can be performed on large data sets while minimizing the risk that a particular individual can be identified. On the other hand, researchers are also looking at ways to address risks from privacy from the increasing capability to re-identify individuals from anonymized data---the so-called "mosaic effect."

In the past, protecting data often meant encrypting it, essentially walling it off from access by others. Using data typically meant releasing decrypted data, essentially exposing the data to others. Cryptographers, however, are working on ways to preserve the protections of encryption while still permitting certain portions of the data to be shared.

Borderless, Secure Data Flows

The United States should also continue to work on better ways to share data, because borderless, secure data flows across an open Internet are essential for global trade. For example, our economic ties with Europe account for nearly one-third of world trade flows, linked to approximately 15 million jobs.

Today, the U.S.-EU Safe Harbor Framework serves as a vital bridge between United States and European data protection frameworks. The Safe Harbor enables data transfers to occur in an efficient and protected way so that businesses on both sides of the Atlantic can conduct their global business operations.

The Safe Harbor Framework provides important privacy protections for the data of EU citizens. It requires companies to develop a conforming privacy policy, commit to comply with the Safe Harbor principles and guidance, and self-certify annually to the Department of Commerce. It also provides for enforcement by the Federal Trade Commission.

Today, over 3,900 companies self-certify their adherence to the Safe Harbor's data privacy principles. U.S. companies and U.S. subsidiaries of European companies alike rely on the Safe Harbor, which contributes directly to the growth and innovation of Europe's digital economy.

The United States, with the Department of Commerce in the lead, has engaged collaboratively with the European Commission over the past year and a half to address questions raised regarding the Safe Harbor Framework. Those talks have resulted in significant progress on enhancing the program's operation. We look forward to successfully concluding these discussions.

The digital economy provides the EU and the United States a unique opportunity for promoting innovation, growth, and jobs. For example, we understand that the European Commission's recent Digital Single Market proposals are intended to create the regulatory and market conditions to help companies to innovate, collaborate, invest, and drive growth. We applaud such efforts and favor a program that would create the conditions for a robust transatlantic digital economy in which EU and U.S. businesses will prosper and find new opportunities. It is important, however, to ensure a regulatory environment that encourages growth, rather than creating bureaucratic obstacles to innovation.

Throughout the world, we should continue to work hard to ensure the digital economy remains a global economy. Requirements that force companies to store data or hardware in specific geographic locations increase barriers to trade and are ultimately self-defeating. Data localization requirements hurt small enterprises by raising costs, and they decrease competition and economic growth. Moreover, a nationally fragmented approach to the Internet sends the wrong message to less open societies, where governments put limits on the openness of the Internet and the digital economy.

The global digital economy of course will continue to reflect national and regional differences, including with respect to privacy. However, if we work toward balanced privacy and data protection regimes, we will capitalize on the secure data flows and big data analysis that will drive economic growth and innovation in the future.

Thank you.