

January 28, 2011

Via email: privacynoi2010@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW., Room 4725
Washington, D.C. 20230

**RE: Commercial Data Privacy & Innovation in the Internet Economy: A
Dynamic Policy Framework
Docket No. 101214614–0614–01**

I. INTRODUCTION

CTIA – The Wireless Association® (“CTIA”)¹ submits these comments in response to the Department of Commerce Internet Policy Task Force’s Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework.

President Obama in his most recent State of the Union address called on America to maintain greatness through innovation. To that end, the Department of Commerce, along with executive and independent agencies with jurisdiction over privacy policy and enforcement, should work together to promote consistency, parity and harmonization efforts in the creation, interpretation and enforcement of privacy principles and regulations. Innovative wireless technologies deserve to be treated at least as well as a salmon² and not be subjected to potentially duplicative and conflicting requirements.

Competition and innovation in the wireless economy are strong. There are now over 630 different wireless handsets or devices available to U.S. consumers.³ The marketplace is still growing at a remarkable pace—the wireless subscriber base is

¹ CTIA—The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization covers Commercial Mobile Radio Service (“CMRS”) providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

² We live and do business in the Information Age, but the last major reorganization of the government happened in the age of black-and-white TV. There are 12 different agencies that deal with exports. There are at least five different agencies that deal with housing policy. Then there’s my favorite example: The Interior Department is in charge of salmon while they’re in fresh water, but the Commerce Department handles them when they’re in saltwater. (Laughter.) I hear it gets even more complicated once they’re smoked. (Laughter and applause.)’ President Barack Obama, 2011 State of the Union Address (January 25, 2011), available at <http://www.whitehouse.gov/the-press-office/2011/01/25/remarks-president-state-union-address>.

³ Written Ex Parte Communications of CTIA-The Wireless Association, WT Docket No. 10-133 (July 30, 2010).

growing at over 20 million new accounts per year,⁴ and in the relatively new arena of wireless applications, revenues generated from consumer downloaded mobile applications are predicted to triple from \$5.2 billion last year to \$15 billion in 2011 and to \$58 billion by 2014.⁵ Industry experts have estimated productivity gains from wireless broadband services to amount to more than \$860 billion in 10 years,⁶ with businesses generally expecting a 15% improvement in their bottom line.⁷ Overall wireless industry economic contributions have grown five times faster than the overall economy over the last decade.⁸ These changes are fueled by an industry where the average job pays 50% more than the national average of other production workers.⁹

The mobile industry has nimbly and effectively responded to this rapidly expanding and changing marketplace by developing and voluntarily adhering to guidelines based on Fair Information Privacy Principles. These voluntary industry guidelines, which include CTIA's Best Practices and Guidelines for Location Based Services,¹⁰ CTIA's Consumer Code for Wireless Service ("CTIA Consumer Code")¹¹ and efforts by other associations (such as the "MMA Mobile Privacy Guidelines"¹²) have proven to be an effective model for promoting sound privacy practices within the wireless industry while at the same time preserving a competitive landscape.

CTIA recognizes that the rapidly evolving wireless industry, while continuing to contribute greatly to an innovative and competitive U.S. economy, will also continue to face new challenges. It looks forward to addressing these new challenges by continuing to evolve and supplement its guidelines and by encouraging greater education and participation among the growing number of companies in the wireless industry.

⁴ CTIA Semi-Annual Wireless Industry Survey, Mid-Year 2010

http://files.ctia.org/pdf/CTIA_Survey_Midyear_2010_Graphics.pdf.

⁵ Data from market research firm, Gartner. *Gartner Forecasts Mobile App Store Revenues Will Hit \$15 Billion in 2011*, <http://techcrunch.com/2011/01/26/mobile-app-store-15-billion-2011/>.

⁶ Roger Entner, *The Increasingly Important Impact of Wireless Broadband Technology and Services on the U.S. Economy: A Follow up to the 2005 Ovum Report on the Impact of the US Wireless Telecom Industry on the US Economy, A Study for CTIA-The Wireless Association* (2008), http://files.ctia.org/pdf/Final_OvumEconomicImpact_Report_5_21_08.pdf.

⁷ *Wireless Means Business: The Wireless Road to Prosperity*, <http://www.ctia.org/advocacy/research/index.cfm/AID/11531>.

⁸ Harold Furchtgott-Roth, *The Wireless Services Sector: A Key to Economic Growth in America 2008 Report* (January 2009).

⁹ *Id.*

¹⁰ CTIA's 'Best Practices and Guidelines for Location Based Services' is available at http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf

¹¹ CTIA's Consumer Code is available at <http://files.ctia.org/pdf/ConsumerCode.pdf>.

¹² Mobile Marketing Association's Code of Conduct for Mobile Marketing (July 15, 2008), <http://mmaglobal.com/codeofconduct.pdf>.

II. CTIA SUPPORTS A FLEXIBLE, YET CONSISTENT AND PREDICTABLE APPROACH TO PRIVACY FRAMEWORKS.

CTIA encourages the Department of Commerce as it develops a privacy framework to ensure that the framework is sufficiently flexible and fosters an environment that promotes the types of technological innovations that benefit consumers and the economy.¹³

Should a Privacy Policy Office ("PPO") within the Department of Commerce be developed within the Department of Commerce, CTIA would support efforts by the PPO "to help provide the Administration with greater expertise and a renewed focus on commercial data privacy." CTIA trusts those efforts would be moderated to contribute to consistency and predictability of privacy best practices and not detract from that goal.

A. CTIA's Best Practices and Guidelines for Location Based Services and Other Self Governing Efforts are Examples of Effective and Adaptive Frameworks for Protecting Consumer Privacy.

CTIA supports industry-developed best practices based on Fair Information Practice Principles (FIPPs) that are appropriately applied to the data and use cases that are subject to these best practices. CTIA's Best Practices and Guidelines for Location Based Services, the CTIA Consumer Code and other voluntary industry efforts (such as "MMA Mobile Privacy Guidelines") are all based on FIPPs and have proven to work effectively for the wireless industry.

CTIA recommends that the Department of Commerce further consider encouraging voluntary adoption by industry of guidelines and codes based on FIPPs.

B. Expansion of FIPPs Should Focus on Outcomes that Increase Consumer Trust and Allow Industry to Develop Solutions that Evolve to Meet Consumer Expectations and Technological Innovations.

While companies should be encouraged to expand privacy protections offered to consumers, any proposed expansion of FIPPs should balance consumer expectations of privacy versus consumer demand for ease of use and availability of rapidly improving technological innovations. The Department of Commerce should also ensure that any expansion of FIPPs would not negatively impact the economic benefits of wireless technology to the U.S. economy.

To help achieve this balance, the Department of Commerce should consider a framework based on technology-neutral principles. Regulatory neutrality should also apply to different technology platforms and business models. Technology is ever

¹³ E.g., Entner, *supra* n.6.

evolving and privacy principles should be adaptive enough to continue to protect consumer privacy regardless of technological changes.

For example, in considering privacy principles as applied to mobile technology, there needs to be an understanding of "mobile" that encompasses more than just phones. The scope of "mobile devices" is rapidly expanding with increasing varieties of form factors and types of devices having connectivity such as notebook computers, tablets and e-readers. In addition, numerous machine-to-machine communication technologies are being developed—some of which have no user interface at all, as the "Internet of Things" progresses. Overly prescriptive frameworks would quickly be outpaced by these and other new advancements in technology.

Many different but effective vehicles for communicating privacy issues and practices beyond the standard online privacy policy have been developed by the mobile industry. Privacy notices take different forms to adapt to typically smaller form factor of mobile devices, the varying mobile platforms and wide range of mobile services. Mobile devices typically include options to allow users to control their privacy settings such as their mobile browser settings,¹⁴ how their location data is used,¹⁵ and ability to set strong passwords.¹⁶ Other mobile-friendly privacy notices and educational materials have been voluntarily developed to enhance user trust such as FAQs,¹⁷ videos,¹⁸ and prominent notice experiences. Companies should be encouraged to continue in these innovative efforts to develop a wide variety of notice experiences appropriate to the mobile environment.

Similarly, companies must have the flexibility necessary to use and explore a wide variety of tools and solutions to manage information systems and help protect consumer privacy. Privacy impact assessments have been used successfully by companies as internal tools.

CTIA does not support, however, the notion of privacy impact assessments as external tools. Exposure of privacy impact assessments used by companies can reveal trade secrets, confidential company information about products under development and possibly even processes to protect personal information from being misused or compromised that to be effective should not be revealed. For these reasons, privacy impact assessments should continue to be encouraged but as internal tools.

Additionally, privacy impact assessments and other prescriptive tools may not always be appropriate or necessary for every company or for every situation.

¹⁴ See, e.g., <http://www.microsoft.com/windowsphone/en-us/howto/wp7/web/changing-privacy-and-other-browser-settings.aspx>

¹⁵ See, e.g., <http://support.apple.com/kb/HT1975>.

¹⁶ See, e.g., http://docs.blackberry.com/en/smartphone_users/deliverables/18577/Set_a_device_password_60_1094208_11.jsp.

¹⁷ See, e.g., T-Mobile Fraud, Security, and Privacy FAQs, <http://support.t-mobile.com/doc/tm23333.xml>.

¹⁸ See, e.g., The Google Privacy Channel, <http://www.youtube.com/user/googleprivacy#p/search/1/u9H4xaTspaQ>.

Companies should be given the flexibility to determine what tools and approaches are appropriate for assessing their own privacy compliance efforts and to account for different technologies, business models and company cultures. A useful framework should focus on an outcome that companies meet their privacy compliance obligations and not the method for doing so.

C. Expansion of a Privacy Framework to Include Broad Principles, such as Access and Verification, Should Be Proportional.

While an expanded privacy framework should be broad and flexible enough to adapt to changes in technology and consumer expectations, any enhanced principles within the FIPPs framework should be reasonable and proportional to the data and data uses involved. For example, while the ability for consumers to verify the accuracy of their information can be important in some circumstances, the extent and degree of the consumer access required or granted for given purposes should include a reasonableness element. Broad access rights would be overly burdensome on industry and disproportional to consumer value. Instead, the degree of access should be proportional to the type and sensitivity of the data in question.

The ability for consumers to verify the accuracy of information is critical to consumers in contexts where inaccuracy of data can affect the granting or denial of a significant benefit such as proper medical treatment and financial services. Those rights exist today in the form of the right of an individual to access protected health information, which may be necessary to obtain proper treatment and care, under the Health Insurance Portability and Accountability Act¹⁹ and the right of an individual denied application for credit, insurance to access free credit data under the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions (FACT) Act.²⁰

In other contexts, access to information is less critical and limitations on means and scope of access are appropriate. In many cases, access in the form of a means to update contact information and preferences adequately serves the consumer need to verify and correct data. Many companies already proactively provide a variety of means for consumers to access and update this type of information.²¹ Online preference pages that invite users to update their contact information and contact preferences quickly and easily are becoming more the norm supplementing traditional methods for consumers to access information in writing or with a call to

¹⁹ See 45 C.F.R. § 164.524.

²⁰ See FCRA § 612 (a)(1)(A), (B); 15 U.S.C. § 1681j.

²¹ See, e.g., "Access and Choice" section of the T-Mobile Privacy Policy, <http://www.t-mobile.com/company/website/privacypolicy.aspx>; "How to Limit the Sharing and Use of Your Information and Other Important Information" sections of the Verizon Privacy Policy, <http://www22.verizon.com/privacy/>; "Information Choices and Changes" section of the Sprint/Nextel Privacy Policy, <http://www.sprint.com/legal/privacy.html?INTNAV=ATG:FT:Privacy>; "Consumer Privacy Control and Choices" section of the AT&T Privacy Policy, <http://www.att.com/gen/privacy-policy?pid=2506>; "Questions about Consumer Control" of the AT&T Privacy FAQ, <http://www.att.com/gen/privacy-policy?pid=13692#controls>.

customer service. In other low risk contexts, simply providing clear notice about the types of data collected should suffice.

In all cases, access and verification should be limited to data that is reasonably accessible in the ordinary course of business. Further, access should also be limited to exclude internally generated information that businesses may happen to associate with a consumer's account such as internal IDs or trade secrets.

D. Any Efforts to Create U.S. Legislation and Multi-National Frameworks Should Be Aimed at Promoting Greater Consistency among the Current Conflicting Privacy Laws and Regulations.

Inconsistent and conflicting laws aimed at consumer privacy protection, whether at the federal or state levels, create inefficiencies for companies and disparate protection of consumer privacy. Efforts to create new legislation and multi-national frameworks should focus on harmonizing the implementation of commonly supported privacy principles.

CTIA advocates greater consistency and predictability in the implementation of privacy rules, should it be that federal laws and regulations are to be developed. Parity in the application of privacy regulations and enforcement should guide any such efforts, regardless of the underlying technology in use or the type of business entity involved in specified data collection and use practices.

At the state level, the development by each state of privacy and security laws with differing standards and requirements has presented implementation challenges and inefficiencies for companies. While CTIA applauds state efforts to combat identity theft, these goals can be met with greater efficiency via a federal data breach notice law based on the best of these laws to replace the patchwork of existing regulation. Key elements CTIA would want to see in a supportable federal breach notice law include a definition of the data that requires breach notification that is focused on the types of sensitive data likely to lead to identity theft, a harm-based, breach-notice trigger and broad federal preemption.

CTIA advocates greater consistency and predictability in the implementation of privacy rules, should it be that federal laws and regulations are to be developed. Parity in the application of privacy regulations and enforcement should guide any such efforts, regardless of the underlying technology in use or the type of business entity involved in specified data collection and use practices.

III. CONCLUSION

A flexible regulatory approach to the mobile industry has fostered the development of innovative mobile devices, platforms and applications and strong competition that has yielded a wide array of choices and better value as compared to other more highly regulated global marketplaces. U.S. consumers have come to

expect and demand these choices. This flexible approach has also fostered proactive self-governance efforts by the mobile industry to develop robust and adaptive guidelines responsive to consumer demands for greater protection of privacy.

In recognition of the effectiveness of this model and the President's call for solutions that promote greater U.S. competition, the DOC should promote a self-regulatory approach and voluntary industry codes that continue to promote tech innovation, broader consumer choices and economic growth, while protecting consumer privacy.

Respectfully submitted,



By: _____

Andrea D. Williams
Vice President of Law &
Assistant General Counsel

Michael F. Altschul
Senior Vice President and
General Counsel

CTIA – The Wireless Association®
1400 Sixteenth Street, NW, Suite 600
Washington, DC 20036
(202) 785-0081
www.ctia.org