February 18, 2011

VIA HAND AND ELECTRONIC DELIVERY

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex N)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: ***FTC Staff Preliminary Report on Protecting Consumer Privacy - File No. P095416***

I. INTRODUCTION

CTIA – The Wireless Association® ("CTIA")[1] submits these comments in response to the FTC Preliminary Staff Report: Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policy Makers (the "Report").

Competition and innovation in the wireless economy are strong. There are now over 630 different wireless handsets or devices available to U.S. consumers.[2] The marketplace is still growing at a remarkable pace—the wireless subscriber base is growing at over 20 million new accounts per year,[3] 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.[4] Industry experts have estimated productivity gains from wireless broadband services to amount to more than $860 billion in 10 years,[5] with

[1] CTIA-The Wireless Association® (www.ctia.org) ® 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] Written Ex Parte Communications of CTIA-The Wireless Association, WT Docket No. 10-133 (July 30, 2010), at ii, http://files.ctia.org/pdf/filings/100730-CTIA_15th_Mobile_Comp_Report_Comments_FINAL.pdf
[3] CTIA Semi-Annual Wireless Industry Survey, Mid-Year 2010, http://files.ctia.org/pdf/CTIA__Survey_Midyear_2010_Graphics.pdf
[4] Data from market research firm, Gartner. Erick Schonfeld, *Gartner Forecasts Mobile App Store Revenues Will Hit $15 Billion in 2011*, TechCrunch (Jan. 26, 2011), http://techcrunch.com/2011/01/26/mobile-app-store-15-billion-2011/
[5] 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.

businesses generally expecting a 15% improvement in their bottom line.[6] Overall wireless industry economic contributions have grown five times faster than the overall economy over the last decade.[7] These changes are fueled by an industry where the average job pays 50% more than the national average of other production workers.[8]

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.

The mobile industry has responded to this rapidly changing technology and rapidly expanding marketplace by developing and voluntarily adhering to guidelines based on Fair Information Privacy Principles ("FIPPs"). These voluntary industry guidelines, which include CTIA's Best Practices and Guidelines for Location Based Services,[9] CTIA's Consumer Code for Wireless Service ("CTIA Consumer Code")[10] and efforts by other associations (such as the "MMA Mobile Privacy Guidelines"[11]) have proven to be a useful model for promoting sound privacy practices within the wireless industry while at the same time preserving a competitive landscape. We also encourage the FTC's work with other agencies supporting the development of privacy best practices informed by current and emerging business models and technological capabilities and limitations.

CTIA recognizes that the 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.

CTIA encourages FTC staff ("Staff"), as it works with stakeholders in developing its own framework to address these challenges, to consider an approach that (i) allows companies reasonable flexibility in implementing any guidelines or

---

[6] *Wireless Means Business: The Wireless Road to Prosperity*, http://www.ctia.org/advocacy/research/index.cfm/AID/11531.
[7] Harold Furchtgott-Roth, *The Wireless Services Sector: A Key to Economic Growth in America 2008 Report* (January 2009).
[8] *Id.*
[9] 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.
[10] CTIA's Consumer Code is available at http://files.ctia.org/pdf/ConsumerCode.pdf.
[11] Mobile Marketing Association's Global Code of Conduct for Mobile Marketing (July 15, 2008), http://mmaglobal.com/codeofconduct.pdf.

practices in a manner appropriate to each unique company and the needs of its consumers**,** (ii) is neutral to technologies, business models and platforms, (iii) fosters technological innovations that benefit consumers and the economy, (iv) recognizes the complex mobile ecosystem, and (v) minimizes unproductive burdens on businesses and consumers. In implementing any such framework as applied to the mobile industry, CTIA urges the Staff to further educate companies about best practices and promote greater participation by companies to supplement and voluntarily adhere to codes of conduct developed by CTIA and other industry associations. Safe harbors for companies that voluntarily adhere to industry guidelines should also be considered as a possible means to further encourage privacy compliance efforts.

II. SCOPE

CTIA encourages Staff in considering the scope of data and practices subject to its proposed framework to take an approach that is not unnecessarily broad. Accordingly, CTIA applauds efforts to outline commonly accepted practices where choice mechanisms are not needed but proposes that any expansion of FIPPs to areas such as access be proportional to the data and data uses and comport with existing laws.[12]

A. Data Subject to Framework

Regulation of all data collected from computers or devices[13] would be overly burdensome on business, can overwhelm consumers and could effectively "lock down data" rather than focus on protection of data that genuinely impacts individual privacy.[14] In the mobile space, consumers expect and demand a user experience that promotes privacy, while enabling the ease of use and speed of access to mobile services.

Industry should be encouraged to take an approach that proportions its efforts based on sensitivity of consumer data and how the data is used. CTIA recognizes that industry should take reasonable precautions with all consumer data and be educated about unexpected pitfalls such as consumer data thought to be anonymous that may become re-identified when tied to "linkable data."

---

[12] For example, CAN-SPAM includes exceptions for certain types of transactional communications that consumers might expect to receive and might fall under "commonly accepted practices." Staff in developing its framework should ensure that existing laws such as CAN-SPAM are considered to ensure harmonization and lack of conflict with existing rules and guidelines.

[13] CTIA also urges the Staff to clarify that the proposed framework would focus exclusively on consumer data (i.e., not employee data or business contact data).

1. Linkable Data

The type and amount of privacy protection needed for "linkable data," should depend on the context of how that data is used on a case-by-case basis. Just because data *may* be capable of being linked to an identified individual does not mean that a company *will* create such link. Consideration should be given to how a company actually uses and protects potentially linkable data rather than to theoretical possibilities. For example, a company may use linkable data in ways that do not identify a specific individual and may have policies or contractual obligations in place to prevent identifying specific individual consumers. Practices and policies should encourage responsible creation and use of linked data profiles, but companies should also be free to exercise their reasonable judgment on the best policies and practices to protect against improper data linkage in their organizations.

Requiring that all potentially "linkable data" be afforded the same level of protection as clearly sensitive customer data also undermines incentives companies currently have to de-link or de-identify data in the first place. Many companies today take affirmative steps to de-link data so data is in a form that protects the privacy of the underlying data subjects and avoids regulatory action but can still be used for legitimate business purposes. Non-linked uses of individual data points are also much less likely to raise privacy concerns than use of linked data. Moreover, subjecting potentially "linkable data" to the same privacy framework as linked data is likely to de-sensitize consumers.

With respect to the collection and storage of potentially linkable data, it is inappropriate to treat this information as though it were already linked and therefore made more sensitive. A one-size-fits-all approach could result in companies diverting a disproportionate amount of resources away from protecting sensitive linked data more likely to negatively affect individuals to protect unlinked data that has far less of a privacy impact. Collection and storage guidelines should focus instead on existing general principles of transparency, accountability and security that take a sliding scale approach to data protection based on sensitivity and use.

2. Location Data

Similarly, Staff should recognize that not all location data is equally sensitive. First, there are varying methods for determining location. For example, Global Positioning System or GPS, which locates users when a device communicates with multiple satellites; wireless positioning, which locates a device via personal and public WiFi access points that have been mapped; cell tower triangulation, which measures distance from cell towers to locate a mobile phone; and IP addresses are all different methods that may be used to determine location. Not all techniques yield precise geo location coordinates. IP address derived from Wi-Fi or G3, for example, may only yield zip code, neighborhood or city level data; in rural and suburban fringe areas, cell tower triangulation may only be accurate to within several miles; and even

GPS location fixes can vary greatly in granularity.[15] Thus, not all location data is precise enough to locate or identify an individual.

Second, as with potentially linkable data, how a company actually uses location data can affect its degree of sensitivity. "De-precision" techniques that convert precise geo-location coordinates to city, state and country level location data, anonymization, and other data minimization practices that reduce the likelihood of identifying an individual should be considered. How location data is shared, how long location data is retained and whether it is tracked over time are also important use factors that should be considered.

We also encourage Staff to consider the many beneficial uses of location data to consumers, industry and to the public. Consumers are demanding more location based services ("LBS"). Spending on LBS is predicted to grow from $2.2 billion in 2009 to $12.7 billion in 2013.[16] Consumers are excited about LBS applications that help them with navigating and mapping, finding useful retail stores and services near them and staying better connected with friends and family. Location information is also essential to the wireless carriers to manage networks and improve coverage. The public benefits of LBS data also cannot be underestimated. Use of LBS data is critical for effective traffic planning and management, emergency services and preparedness and personal safety.[17]

B. Commonly Accepted Practices

We appreciate that Staff recognizes that certain categories of uses of information be considered "commonly accepted practices," thus eliminating the need to provide choice. CTIA proposes that the Staff's current categories of commonly accepted practices should be broadened to provide flexibility and encompass the full range of commonly accepted practices. Any such list must provide a starting point for evolving standards, not a rigid or static definition of acceptable practices.

CTIA concurs with Staff's conclusion that consumers view first-party recommendations of products and services[18] to be within the scope of "commonly accepted practices." Staff asks whether there should be restrictions on use of

---

[15] In tests by Qualcomm, location fixes varied as follows depending on the type of method used: Cell site: 800 to 2000 meters; A-GPS: 10 to 20 meters; GPS: 10 to 80 meters; Cell site + WiFi: 60 to 250 meters.

[16] *San Jose firm's technology helps to find lost cars, pets and more*, Silicon Valley/San Jose Business Journal, http://www.bizjournals.com/sanjose/stories/2010/01/18/smallb3.html (citing Gartner, *Dataquest Insight: Consumer Location-Based Services, Subscribers and Revenue Forecast, 2007-2013*).

[17] Carriers and mobile device manufacturers have been legally required to support the provision of location data to support e911.

[18] CTIA assumes that this exception would apply equally to a company that collects information from its customers with whom it interfaces to market its own products and services as well as to interface directly with those same customers to market third-party products and services so long as its customer information is not shared with such third parties.

"sensitive information" for first party advertising or marketing. Whether information is sensitive is a context specific question. There are circumstances where sensitive data, such as location information tied to an individual, might be considered "commonly accepted" for first-party recommendations where use of location information for that marketing purpose is obvious or implicit. For example, when a user requests a wireless service that will display nearby restaurants or shops and discounts, a user will understand that the service relies on the location of his or her device.

Other commonly accepted practices that the Staff should consider including in its list are as follows:

a. The transmission of certain system and header information (browser type and version, language, device, IP address, etc.) when using a web browser.

b. Efforts to protect intellectual property such as automatically acquiring licenses/updating licenses for protected content (i.e., music, video, etc.).

c. Automatic verification of digital signatures.

d. Uses, disclosures, or permitted access of network data (Customer Proprietary Network Information ("CPNI") that do not require consent under the FCC's customer proprietary network rules.[19]

e. Further clarification on sharing of customer information with a third-party service provider would also be helpful. Service fulfillment should include using data that a service provider such as a carrier or application vendor needs to provide a customer services he or she requests. In other words, if a customer requests driving directions or other tracking information, then a customer should know location-based information is needed. Also, if a customer agrees to separate terms of a third-party application developer, the manufacturer of the device, the platform developer and the carrier providing network connectivity should not be responsible for that third party data collection.

CTIA agrees with Staff that use of information for "Internal Operations" is a commonly accepted practice for which companies do not have to get consumer consent. CTIA notes that for the wireless industry, internal operations include network management, maintenance and testing and use of location information and device usage data to develop new, and improve existing, mobile products and services, and to understand and meet the needs and preferences of mobile customers. In addition to analytics information collected by websites cited by Staff, wireless applications that collect similar usage data should also be noted.

[19] *See* 47 C.F.R. § 64.2009.

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

CTIA appreciates that in its consideration of expanding FIPPs to provide greater access rights to consumers, Staff recognizes that the degree of access should be proportional to the sensitivity of the data and the nature of its use. CTIA also appreciates that Staff advocates a sliding scale approach to access. Broad access rights would be overly burdensome on industry and disproportionate to the minimal consumer value.

The ability of consumers to access 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 Act,[20] and the right of an individual denied application for credit or insurance to access free credit data under the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act.[21]

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's need to verify and correct data. As Staff recognizes in the Report, many companies already proactively provide a variety of means for consumers to access and update this type of information.[22] 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 customer service. In other low risk contexts, simply providing clear notice about the types of data collected should suffice.

In all cases, access 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. Other exceptions to access similar to those adopted in other countries such as Canada[23] and the UK[24] should also

---

[20] *See* 45 C.F.R. § 164.524.

[21] *See* FCRA § 612 (a)(1)(A), (B), 15 U.S.C. 1681j.

[22] *See e.g.*, "Access and Choice" section of Privacy Policy of T-Mobile, 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" at the AT&T Privacy FAQ, http://www.att.com/gen/privacy-policy?pid=13692#controls.

[23] Personal Information Protection and Electronic Documents Act (2000, c. 5) (available at http://laws.justice.gc.ca/eng/P-8.6/).

be considered. Access should be limited where it could (1) reveal information about another individual, (2) threaten the life or security of another individual, or (3) where collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws.

Staff also proposes requiring entities to provide consumers access to information about "the identity of those with whom the company has shared data about the consumer, as well as the source of the data." Read broadly, this presents burdensome record-keeping challenges for companies disproportionate to the consumer benefit. Customers may affirmatively agree to allow their information to be shared broadly with multiple companies who offer products and services that may also be of interest to the user. Few customers typically request detailed information about with whom their data is shared. Instead, customers more often expect that upon request, entities stop future sharing of their information. It is also unclear whether Staff intended to include sharing of data with third-party agents acting on behalf of a company. We would seek clarification that this was not intended.

III. PRIVACY BY DESIGN

The Privacy by Design concept has different meanings among different entities. CTIA encourages a flexible concept that will not stifle innovation of future technology and advanced mobile services and products that benefit consumers. Staff should consider a framework based on technology-neutral principles. Regulatory neutrality should also apply to different technology platforms and business models. Technology is ever evolving and privacy principles should be adaptive enough to continue to protect consumer privacy regardless of technological changes.

Companies should be encouraged to think about privacy in the early stages of development as products, services and internal practices and processes are designed. Although not all companies have the resources to develop formal programs, privacy by design as a practice is not a new concept. Many companies regularly and consistently incorporate privacy by design into their practices, including user-friendly privacy notices and technologies that embed transparency and control features into the service experience.

Although these and other examples of privacy by design solutions cited by the FTC, such as privacy impact assessments and encryption, have been used successfully by companies as internal tools, prescriptive tools may not always be appropriate or necessary for every company or for every situation. Companies should be given the flexibility to determine what tools and approaches are appropriate for

---

[24] *See, e.g.*, *Access to Personal Data*, U.K. Information Commissioner's Office, http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_6/access_to_personal_data.aspx.

assessing their own privacy practices and to account for different technologies, business models and company cultures. A prescriptive approach would be overly burdensome and could stifle product innovation as well as innovations in the area of privacy enhancing technologies and solutions. A useful framework should focus on an outcome that companies meet their privacy obligations and not the method for doing so.

IV. DO NOT TRACK

CTIA agrees with Staff that positive steps have been made by industry in its self-regulatory efforts to develop new privacy enhancing tools in the area of online behavioral targeting. The FTC should similarly recognize that privacy enhancing tools can be effective methods for self-regulation in the mobile space.

In assessing methods for self-regulation in the mobile space, the FTC should consider the unique challenges faced by the wireless industry and allow the mobile industry time to address those unique challenges.

First, the methods for remembering unique users for the purpose of personalized mobile advertising do not typically involve cookies as they do in the online space. The way mobile platforms are typically designed, cookies are wiped more frequently from users' phones. Cookies are, thus, a less reliable mechanism for tracking in the mobile space. Mobile ad networks instead rely on a variety of other methods for remembering users, including mobile device IDs and other more persistent identifiers. Because mobile ad networks vary widely in their methods for tracking, coming up with a one-size-fits all opt-out mechanism that works for all methods of tracking will be more challenging in the mobile space.

Second, the wireless marketplace is an open environment and consists of numerous platform providers and advertising networks. Achieving consensus on a one-size-fits-all approach amongst this large pool of mobile browser platforms and advertising networks will be challenging. Allowing alternative methods of implementation of Do Not Track may be a more realistic approach in the mobile marketplace. Because of these unique challenges in the mobile space, CTIA encourages the FTC to support industry efforts to innovate and develop many different solutions that would allow consumers to exercise meaningful choices.

V. MEANINGFUL CHOICE/CONSENT

With respect to meaningful choice and consent, CTIA supports maintaining industry flexibility to address new privacy issues as wireless technology evolves and new consumer use patterns emerge, including protecting children's online privacy and consumers' rights to informed consent for location-based wireless services. Industry best practices and guidelines provide flexibility to address evolving wireless technology.

Given the diverse and large number of players in the mobile space and the wide diversity of platforms, device formats and wireless services, a one-size-fits-all approach to consent is not a viable model for the wireless industry. A "uniform and comprehensive" format for choice will not work well in a mobile environment that has traditionally embraced openness and diversity rather than technological uniformity.

Requiring that choice be offered "just in time" at every point of data collection can also cause an unwieldy customer experience in the mobile space. For example, a pop-up asking whether location data can be collected for every type of application or service can result in consumer frustration. A one-time question about collecting location data may be appropriate for a service that obviously relies on location of a device to perform the service. CTIA asks Staff to consider an approach for a form of consent similar to that taken by CTIA in its "Best Practices and Guidelines for Location-Based Services (the "Guidelines").[25] The Guidelines do not dictate the form, placement, terminology used, or manner of obtaining consent as long as the consent is informed and based on adequate notice.[26] The Guidelines also recognize that pre-checked boxes that automatically opt users into location information disclosure or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent.[27]

The Report proposes that all entities involved in the information collection and sharing—carriers, operating system vendors, applications, and advertisers—be required to provide consumers with meaningful choice prior to collection. In the mobile context, taken literally, this would create a very poor consumer experience as multiple entities are frequently involved with the mobile services that consumers choose to receive. For example, a free, ad-funded application that lets a jogger track a run will involve collection of email address and other registration data by the developer of the application itself, collection of analytics data by the platform provider who provides the software development kit used by the developer to develop the application, GPS data by the carrier and others that provide GPS services to allow location tracking, and demographics based on the type of app and phone by the advertising network that serves up the ads and sometimes also the advertiser. The FTC should clarify that companies have the freedom to freely contract to decide who in the chain of data collectors might be in the best relation with the user to present a single, clear and conspicuous notice and choice of all these data collection activities on behalf of each partner rather than four or five separate experiences by each partner.

A "take it or leave it" approach to consent should be appropriate for certain products and services that are dependent on the collection, sharing, and use of

---

[25] Guidelines, *supra* note 9.
[26] Guidelines, *supra* note 9 at 5.
[27] *Id*.

information in order to provide their utility. This is particularly true, for example, of beneficial free mobile applications that are primarily dependent on advertising revenue. As long as consumers are presented with the appropriate level of notice and/or consent commensurate with the type of data collected and its intended use, consumers should be allowed to choose for themselves whether to take a product or service or leave it.

VI. OTHER SPECIFIC ISSUES

A. Transparency and Consumer Notices.

We concur with Staff's opinion that privacy policies should "enable better comprehension and comparison of privacy practices." CTIA's Best Practices and Guidelines for Location Based Services reflect its members' commitment to promoting and protecting user privacy through technology-neutral notices that inform customers about how their information will be used, disclosed and protected, so that they can make informed decisions and give customer's ultimate control over their information.

Many different but effective vehicles for communicating privacy issues and practices beyond the standard online privacy policy have been adopted 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,[28] how their location data is used,[29] and ability to set strong passwords.[30] Other mobile-friendly privacy notices and educational materials have been voluntarily developed to enhance user trust such as FAQs,[31] and privacy resource pages,[32] learn more links,[33] videos,[34] and prominent notice experiences.[35]

---

[28] *See, e.g.*,http://www.microsoft.com/windowsphone/en-us/howto/wp7/web/changing-privacy-and-other-browser-settings.aspx .

[29] *See, e.g.*,http://support.apple.com/kb/HT1975.

[30] *See, e.g.*, http://docs.blackberry.com/en/smartphone_users/deliverables/18577/Set_a_device_password_60_1094208_11.jsp.

[31] *See, e.g.*, T-Mobile Fraud, Security, and Privacy FAQs, http://support.t-mobile.com/doc/tm23333.xml.

[32] *See, e.g.*, T-Mobile Privacy and Security Resources, http://www.t-mobile.com/Company/PrivacyResources.aspx?tp=Abt_Tab_IdentityTheft.

[33] *See, e.g.*, AT&T's "Things you should know about how your information is shared on buzz.com," http://buzz.com/sharing.

[34] *See, e.g.*, The Google Privacy Channel, http://www.youtube.com/user/googleprivacy#p/search/1/u9H4xaTspaQ.

[35] *See, e.g.*, AT&T's Buzz.com Privacy Preference Experience, Statement of Dorothy Attwood, Senior Vice President, Public Policy & Chief Privacy Officer, AT&T Inc. Before: United States Senate Committee On Commerce, Science And Transportation Hearing: Consumer Online Privacy, July 27, 2010.

Companies should be encouraged to continue in these innovative efforts to develop a wide variety of notice experiences appropriate to the mobile environment. Although CTIA does not encourage an approach that dictates the form, placement, terminology used or manner of delivery of notices, CTIA does encourage industry to adhere to general principles in developing notices. Users should have an opportunity to be fully informed of information practices. Any notice must be provided in plain language and be understandable. Notices must not be misleading, and if combined with other terms or conditions, the location based services portions of those terms must be conspicuous.[36]

CTIA notes that due to threat of regulatory action, industry is dissuaded from producing shortened privacy policies recommend by Staff. Often privacy policies become lengthy to avoid omitting any material practices, such that their omission might be considered unfair or deceptive under Section 5 of the FTC Act and at the encouragement and warning of the FTC to describe practices more fully.

The FTC should also consider that the complexity of business practices and the types of consumers can vary widely from company to company. A company should be allowed to consider its own risks, its respective consumer audience and its own unique business considerations as it determines the form of privacy policy that best conveys the information that its consumers are most interested in understanding.

B. Teens

Staff asks whether enhanced consent should be required for the collection and use of information about teens. When Congress enacted the Children's Online Privacy Protection Act[37] in 1998, it decided that special consent requirements should apply only to children under the age of 13. While the Staff's concerns are well intentioned, expansion of COPPA to teens would not be effective and would present a number of practical challenges.

First, COPPA restrictions are based, in part, on information collected on websites with content targeted at children under the age of 13. Even with children, particularly older children, it can be difficult to find the line between what content is targeted to children versus content of interest to a general audience. With teens, because their interests are maturing, the type of content they are drawn to is the same as or much closer to the type of content of interest to those over the age of 18. Thus, where to draw the line of content attractive to teens is even more blurred than it is for children. Second, there is no good way to verify an online user's age as a method to age gate to ensure COPPA compliance. While young children are more likely to correctly state their age, teens are savvy enough to get past age-gating obstacles. For wireless carriers, often only the age of the main account holder is known. Additional information would need to be collected from all members of a family plan account or

[36] Guidelines, *supra* note 9, at 3.
[37] 15 U.S.C. § 6501 *et seq.*

other multi-user account, which would create additional privacy concerns. Third, numerous benefits of mobile devices to teens may be hindered if teens are restricted from access to mobile content and services. Teens benefit greatly from use of mobile devices to gain access to resources relating to education, health care, accessibility and safety.[38]

Because of these challenges, CTIA believes that innovative forms of parental control and education are still the most effective means to encourage teens to use cell phones in smart, safe, fair and responsible ways.

CTIA and its members provide effective, innovative solutions that give parents choice and control over the mobile content and services their teens are using. Wireless carriers offer a variety of service plans that can help parents regulate how children use their wireless devices, including limits on text and picture messages, Internet access, pre-approved outbound and inbound calls and more. In the open mobile ecosystem, parents can also find content control tools that are built into a device or service or downloadable from a manufacturer, service provider or third party.

A significant component of the Wireless Carrier Content Guidelines[39] is the voluntary content classification standards for carrier content—those materials that are offered specifically on the carrier's managed content portal, also known as the carrier's "deck," or any third-party content whose charges are included on a carrier's bill. Carrier Content is divided into two classifications: "Generally Accessible Carrier Content" and "Restricted Carrier Content." Generally Accessible Carrier Content is available to consumers of all ages. Restricted Carrier Content is accessible only to consumers age 18 years and older or to a consumer less than 18 years of age when specifically authorized by a parent or guardian.

CTIA has also been very involved in a series of educational initiatives and partnerships. CTIA, along with The Wireless Foundation, launched the "Be Smart. Be Fair. Be Safe: Responsible Wireless Use" campaign in March 2010 to help parents, educators and policymakers teach kids about responsible mobile behavior, driving and eco-friendly initiatives.[40] The campaign website provides parents with a list of CTIA members and the parental features and filters they offer; a checklist with tips on what to do when your child has a wireless device; and an example of family rules. CTIA's numerous other educational outreach efforts include *Get Wise about Wireless*,[41] the Model Family Cell Phone Agreement,[42] Wireless Safety Week,

---

[38] Comments of the CTIA-The Wireless Association, *In the Matter of Empowering Parents and Protecting Children in an Evolving Media Landscape*, MB Docket No. 09-194 (February 24, 2010), http://files.ctia.org/pdf/filings/100224_-_FILED_CTIA_Empowering_Parents_NOI_Comments.pdf

[39] The Guidelines for Carrier Content Classification and Internet Access are voluntary guidelines developed by the CTIA and participating wireless carriers. *See* http://www.ctia.org/content/index.cfm/AID/10394.

[40] *See* http://www.besmartwireless.com/.

[41] *See* http://www.ctia.org/consumer_info/safety/index.cfm/AID/11411.

CTIA's "S-A-F-E-T-Y" tips,[43] *On Road, Off Phone* campaign,[44] public service announcements, and the wireless safety websites of its various carrier members.[45] CTIA and its members also participate in partnerships that promote and help ensure safety of children and teens such as the National Center for Missing and Exploited Children, the National Coalition for the Protection of Children and Families, Family Online Safety Institute, National Crime Prevention Council and the National Safety Council.

CTIA and its members, through these numerous efforts, have effectively responded to consumer demand for parental controls and solutions relating to children and teen privacy and safety. Through educational efforts and technological innovations, CTIA and its members will continue to voluntarily explore and provide solutions that go above and beyond any goals that may be achieved by prescriptive regulations.

C. Retention

Any prescriptive approach to limit data retention would be too rigid and would not allow the flexibility companies need to assess their own unique business needs for keeping data for legitimate purposes. There are a number of legitimate business reasons for retaining and using customer information including preventing and detecting fraud, understanding wireless device and application usage, improving wireless device and services, protecting consumers from malicious privacy and security threats and developing new products in response to consumer demands. Moreover, what is a "reasonable" data retention period or "business purpose" will vary widely and will depend in part on each company's customers and business models and objectives. Staff should also take into consideration challenges faced by the wireless industry due to competing requirements to affirmatively retain data for purposes of law enforcement purposes.

D. Legacy Systems

The Staff also requested comments regarding updating legacy systems to help upgrade privacy protections. In considering any proposals, Staff should consider and explore practical considerations to updating legacy systems including, time, costs, and disruption to business. If proposals are made, companies should be encouraged to prioritize focus and resources on legacy systems handling and processing sensitive data.

---

[42] *See* http://www.wirelessfoundation.org/WirelessOnlineSafety/FamilyCellPhoneContract.pdf.
[43] *See* http://www.ctia.org/consumer_info/safety/index.cfm/AID/11648.
[44] *See* http://www.onroadoffphone.org.
[45] *See, e.g.*, AT&T's "Be Sensible" campaign, http://www.wireless.att.com/learn/articles-resources/be-sensible.jsp; Verizon Parent Control Center, http://parentalcontrolcenter.com/.

VII. 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 adopt 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, Staff should promote a self-regulatory approach and voluntary industry codes that continue to promote technological innovation, broader consumer choices and economic growth, while also 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