

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)
Privacy and Security of Information Stored on) CC Docket No. 96-115
Mobile Communications Devices)

COMMENTS OF THE INTERACTIVE ADVERTISING BUREAU

The Interactive Advertising Bureau (“IAB”) provides these comments in response to the Federal Communications Commission’s (“Commission”) request for comments regarding the privacy and data security practices of mobile service providers with respect to customer information stored on users’ mobile communications devices, CC Docket No. 96-115. As the Commission contemplates new technologies and business practices that contribute to the explosive and innovative growth of the mobile Internet, we ask the Commission to consider the tremendous value created by mobile marketing for both consumers and the economy, and the positive impact that self-regulation and education have collectively had on consumer privacy.

Founded in 1996 and headquartered in New York City, IAB (www.iab.net) represents over 500 leading companies that engage in and support the sale of interactive advertising. Collectively, our members are responsible for selling over 86% of online advertising in the United States. Recognizing the swift expansion of the mobile smartphone market, IAB launched the Mobile Marketing Center of Excellence (“Mobile Center”) in December 2010. The IAB Mobile Center is charged with driving the growth of the mobile marketing, advertising, and media marketplace. IAB devotes resources to market and consumer research, mobile advertising case studies, executive training and education, supply chain standardization, creative showcases, and best practice identification in the burgeoning field of mobile media and marketing. Members of the Mobile Center Board of Directors include representatives from AT&T, Google,

Microsoft, Millennial Media, Mojiva, New York Times, The Weather Channel, Time Inc., Univision, and Yahoo! Inc.

As the Commission updates its record to the 2007 *Further Notice*, IAB encourages the FCC to promote a policy approach that continues to allow the mobile marketplace to innovate and flourish. A still nascent and evolving marketplace with consumer smartphone adoption just now reaching 50% penetration, mobile has become an important and consumer-empowering contributor to the economy.¹ Mobile is an incredible economic opportunity not only because it is intimate, interactive, personalized, and localized; but, because the same features that make mobile an opportunity also make the consumer the primary gatekeeper to its success.

I. Consumer Control and Self-regulation

The mobile marketplace is no longer limited to service providers and handset manufacturers. The launch of Apple's iOS, and subsequently Android, Windows Mobile, and Blackberry Apps World transformed the mobile industry by putting the consumer in control. The mobile Internet economy flourished thanks to an open environment built on choice: multiple platforms, operating systems, applications, and browsers placed exciting content and services at the consumer's fingertips.

Much of that innovation was made possible by a rich data economy fueled by interactive advertising. The revenue generated by online advertising supports the creation and entry of new businesses, communication channels (e.g., micro-blogging sites and social networks), and free or low-cost services and products (e.g., photo sharing apps, weather, news, and games). Interactive advertising enables consumers to compare prices, learn about products, and find out about new

¹ "Smartphones Account for Half of All Mobile Phones, Dominate New Phone Purchases," *NielsenWire*, March 29, 2012: http://blog.nielsen.com/nielsenwire/online_mobile/smartphones-account-for-half-of-all-mobile-phones-dominate-new-phone-purchases-in-the-us/

local opportunities. These successful ventures provide jobs and strengthen the U.S. economy.² The mobile Internet is especially important for small businesses, enabling them to compete where costs would otherwise hinder their entry into the market. Consumers value ad-supported products and services and benefit from the diversity of mobile Internet companies.

Companies collect data for numerous operational purposes including ad delivery, ad reporting, site rendering, accounting, and network efficiencies and optimization, and site or application customization. These operations are necessary for a seamless mobile Internet experience and a functioning mobile economy, as well as to support and monetize the applications and services expected by customers in the marketplace today.

The mobile device specifically is diverse with many parties responsible for fueling the consumer experience, and the IAB strongly believes that self-regulation has an important role to play in its continued growth. Coupled with the strong privacy regulations that exist today, self-regulatory programs can adequately meet evolving consumer privacy expectations in the mobile marketplace. IAB is one of six trade associations spearheading the effort to self-regulate data collection and interactive advertising through the Digital Advertising Alliance (DAA).³ The DAA program was recognized by the Obama Administration as a model of success in the creation of “enforceable codes of conduct”.⁴ This program is designed to give consumers enhanced control over the collection and use of data. With the support of the six stakeholder associations – representing more than 5,000 U.S. companies – the program promotes the use of the Advertising Option Icon, a universal symbol found within or near online advertisements or on web pages where data is collected and used to deliver online advertising that is based on

² The App Economy now is responsible for roughly 466,000 jobs in the United States, up from zero in 2007 when the iPhone was introduced. This total includes jobs at ‘pure’ app firms such as Zynga. App Economy employment also includes app-related jobs at large companies such as Electronic Arts, Amazon, and AT&T, as well as app ‘infrastructure’ jobs at core firms such as Google, Apple, and Facebook. “Where the Jobs Are: The App Economy,” Dr. Michael Mandel, South Mountain Economics, LLC, February 7, 2012: <http://www.technet.org/wp-content/uploads/2012/02/TechNet-App-Economy-Jobs-Study.pdf>

³ www.AboutAds.info

⁴ February 23rd White House Press Conference announcing the release of the Administration’s privacy report.

inferences derived from the collected data. By clicking on the icon, consumers are provided a simple, easy to understand disclosure statement regarding the participating company's data collection and use practices, as well as a link to a simple, comprehensive opt-out mechanism.

The IAB, in collaboration with the other trade associations and DAA participants, including major U.S. commercial mobile service providers is nearly complete with the extension of these principles to the mobile platform. Specifically, the principles will provide transparency and consumer control for precise location information, mobile multi-site data, and mobile cross-app data, encompassing all parties in the mobile device ecosystem.

While the IAB supports efforts to improve transparency and consumer control, we oppose establishing prescriptive requirements for the form or substance of consumers' notice and control. Given the complexity of today's mobile devices and mobile Internet operations, companies need flexibility in how they communicate with their customers and must be able to tailor notices for the underlying technology involved and needs of their customers. Companies also require the flexibility to adapt their communications as practices and technologies evolve. Imposing rigid or one-size fits all legal standards that impact all participants across media channels could have unintended consequences for new and emerging channels. Self-regulation strikes a measured balance by ensuring meaningful communication with consumers and providing companies flexibility in how they provide this information.

II. Telecommunications Carriers' Obligations Under Section 222(a) – Ensuring Consistency in a Complex Ecosystem

The Commission seeks comment on telecommunications carriers' Section 222(a) duty to protect the confidentiality of proprietary customer information in light of the changed mobile ecosystem. Today's mobile communications device market did not exist at the time of the Commission's last CPNI review in the *2007 Further Notice*. Since that time, consumers have taken over considerable control of the mobile device, as well as the operating system and

applications software that are installed on the device. The wireless service provider and handset manufacturer are no longer the only parties or entities with access to information that relates to the mobile device or the consumer's use of the device; and, any expansion of a telecommunications carrier's duty under Section 222(a) will result in inconsistency in the mobile marketplace, as well with as the FCC's prior decisions, with the adverse consequence of stifled innovation.

Historically, the statutory scope and application of the Commission's CPNI rules provided that "a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances: (1) as required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service."⁵ Not only does Section 222(c)(1) apply to CPNI obtained by virtue of its provision of a telecommunications service, but the use, disclosure, and access requirements apply to *individually identifiable* customer proprietary network information.⁶

We do not read the definition of CPNI in Section 222(h)(1) to apply to any information collected at the carrier's direction regardless of telecommunications transmission. Indeed, the plain language of the statute demonstrates that Congress did not intend for the FCC to extend its regulatory purview to information services such as those involved in mobile data communications. Specifically, Section 222(h)(1)(A) states, in relevant part that:

The term "customer proprietary network information" means— information that relates to the quantity, technical configuration, type, destination, location, and

⁵ See *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931 ¶ 5, (2007) ("2007 Further Notice").

⁶ 47 U.S.C. § 222(c)(1).

amount of use of a *telecommunications service* subscribed to by any customer of a telecommunications carrier⁷

“Telecommunications service” is defined as “the transmission . . . of information of the user’s choosing, without change in the form or content of the information as sent and received.”⁸ In 1980, the FCC issued its *Computer II* decision,⁹ in which it addressed technological developments that blurred the boundary between traditional telecommunications and data processing services. The FCC adopted a regulatory framework that distinguished between the offering of “basic transmission service” and “enhanced service.” The FCC defined “basic service” as “limited to the common carrier offering of transmission capacity for the movement of information.”¹⁰ In offering this capacity, a communications path is provided for the analog or digital transmission of voice, data, video, etc. information,” and “the carrier’s basic transmission network is not used as an information storage system.”¹¹ In other words, “a carrier essentially offers a pure transmission capability over a communications path that is virtually transparent in terms of its interaction with customer supplied information.”¹² In contrast, the FCC defined “enhanced service” as “any offering over the telecommunications network which is more than basic transmission service.”¹³ The FCC further determined that only basic services were subject to mandatory Title II regulation, whereas enhanced services were not.¹⁴

Congress substantially amended the Communications Act of 1934 when it passed the Telecommunications Act of 1996. The Telecommunications Act of 1996 introduced two new important regulatory classifications that paralleled the basic and enhanced services distinction

⁷ 47 U.S.C. § 221(h)(1)(A) (emphasis added).

⁸ 47 U.S.C. § 153(43).

⁹ *Amendment of § 64.702 of the Commission’s Rules and Regulations*, 77 F.C.C.2d 384 (1980) (“*Computer II*”).

¹⁰ *Id.* at 387, 419, ¶¶ 5, 93.

¹¹ *Id.* at 419-420, ¶¶ 93, 95.

¹² *Id.* at 420, ¶ 96.

¹³ *Id.* at 420, ¶ 97.

¹⁴ *Id.* at 387, ¶¶ 5, 7.

established in *Computer II*: “telecommunications service” and “information service.”¹⁵ Only telecommunications service is subject to mandatory regulation under Title II.¹⁶ Consistent with these decisions, the FCC determined that mobile wireless broadband Internet access service is an information service, rather than a telecommunications service.¹⁷ Thus, all mobile Internet activities, including e-commerce transactions, data collection, and online advertising, are information services that are not subject to Title II regulation, including the CPNI requirements set forth in Section 222.

Moreover, the statutory language specifically states that CPNI only encompasses information “that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship.” As discussed above, the carrier-customer relationship under this section is only for the provision for telecommunications service to the customer. A telecommunications carrier may have more than one business relationship with a customer unrelated to the provision of telecommunications services; specifically, in the mobile ecosystem for example, a telecommunications carrier may also act separately as a third-party advertising network, a first-party publisher, or an information service for the distribution of content. The application of Section 222 to information services and other Internet-related activities would be inconsistent with the FCC’s prior decisions regarding the treatment of mobile Internet access.

A broadened reading of the definition of CPNI would result in an expansion of the Section 222(c) duty beyond its intended and stated purpose to protect the confidentiality of individually identifiable proprietary information, and reach into all information collected by a carrier on a mobile device.

¹⁵ 47 U.S.C. § 153(20) & (46).

¹⁶ *Time Warner Telecom, Inc. v. FCC*, 507 F.3d 205, 213 (3d Cir. 2007).

¹⁷ *Reexamination of Roaming Obligations of Commercial Mobile Radio Service Providers*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 15817, 15846 ¶ 81 (2007) (citing *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*, 22 FCC Rcd 5901 (2007)).

Not only does this place telecommunications carriers at an unfair competitive disadvantage in the mobile ecosystem, but it is also contrary to the intended purpose of Section 222. In 2007, the Commission recognized that Section 222 applies different privacy protections and carrier obligations based on the sensitivity of the information collected. Specifically, the Commission distinguished between individually identifiable CPNI, aggregate customer information, and subscriber list information, and accorded CPNI the greatest level of protection. Not all data and information collected on a mobile device at the carrier's direction would constitute CPNI, and data and information related to Internet access, or exclusively in the control of the customer, need be extended the same statutory protections.¹⁸

Just as in the desktop Internet environment, the mobile Internet should have consistent regulation that allows all parties to innovate and compete while ensuring consumer transparency and choice regarding data collection practices. Expansion of the Section 222(a) duty in an environment where the consumer controls what entities, products, and services reside on the mobile device would create enormous regulatory uncertainty, and subject telecommunications carriers to penalty for the actions of parties for which they have no control.

III. Expanded Reading of CPNI Definition Impacts Parties Outside Commission's Subject Matter Jurisdiction

The definition of CPNI in Section 222(h)(1) should not be expanded beyond its current statutory reach to encompass business practices not intended for regulation by Section 222. An expanded reading of Section 222(h)(1) would impact an enormous range of parties outside the Commission's subject matter jurisdiction by virtue of the joint venture, independent contractor,

¹⁸ "Practically speaking, CPNI includes personal information such as the phone numbers called by a consumer, the length of phone calls, and services purchased by the consumer, such as call waiting. Congress accorded CPNI - which includes personal, individually identifiable information - the greatest level of protection." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Third Report and Order and Third Further Notice of Proposed Rulemaking, 17 FCC Rcd 14860, 14864 ¶ 3 (2002). *See also*, 2007 *Further Notice*, 22 FCC Rcd at 6930 n.2 ("CPNI includes personally identifiable information derived from a customer's relationship with the provider of the communications services.")

third party disclosure requirements, and result in unprecedented Commission regulation of data collection and use.

Mobile technologies are utilized today in ways that were not envisioned when the CPNI statute and rules were initially passed and implemented, and have led to innovations that benefit customers and businesses alike. For example, companies have leveraged crowdsourcing data and the widespread use of mobile data in order to provide relevant, real-time information to users. Such uses include mobile applications that provide the current price of gasoline at nearby stations, the amount of traffic congestion on a currently traveled route, and the availability of a product at a lower price within a user's vicinity. Social media applications provide information and connectivity in ways that could never be accomplished through conventional communications technologies. These and other advances that rely on the unique nature, availability, and usage of mobile data would not have been possible had non-regulated third parties been burdened with the obligations set forth in Section 222(h)(1).

We ask the Commission to recognize the value that an all-encompassing self-regulatory program can continue to provide from the desktop to the mobile device, and beyond. Unlike formal regulations, which can quickly become outdated in the face of evolving technologies, a self-regulatory code of conduct can allow industry to respond rapidly to new challenges presented by the evolving Internet ecosystem.

Today, all parties including commercial mobile service providers are subject to multiple regulatory regimes.¹⁹ The White House, Department of Commerce, and Federal Trade Commission recognized the DAA program as having the greatest success in providing consumer notice regarding collection practices and the opportunity to exercise choice with respect to the

¹⁹ Including broad Federal Trade Commission enforcement authority under Section 5 Unfair or Deceptive Acts or Practices of the FTC Act 15 U.S.C. §45, the Children's Online Privacy Protection Act 15 U.S.C. §§6501-6506, and the Fair Credit Reporting Act 15 U.S.C. §§1681 *et seq.*, among many other statutory regimes.

entire array of products and services on the device.²⁰ By putting the information and choice directly in consumers' hands, the DAA is able to provide consumers with the ability to opt-in or out of collection based on individual services and trusted relationships as opposed to one global device opt-in that diminishes the functionality and consumer experience on the device.

As the Commission's Chief of the Wireless Telecommunications Bureau Rick Kaplan observed in his welcoming remarks at the Commission's June 28, 2011 forum on location-based services, advances in the wireless ecosystem have been tremendous and the environment thus far has been conducive to innovation. Consumers want to be in control. Consumers want to access their information and entertainment on-the-go, and the burgeoning mobile marketplace presents an enormous opportunity for advertisers to stay connected with their audiences.

In the right regulatory environment, the mobile marketplace will continue to mature, and adoption will continue to rapidly spread as consumers gain trust in the ecosystem. Enforceable self-regulation will help ensure that all parties in the ecosystem together will provide consumers with transparency and choice as they embrace smart mobile devices.

We thank the Commission for the opportunity to submit these comments, and look forward to working closely with the FCC on these important issues.

Respectfully submitted,
/s/
Michael Zaneis
Senior Vice President & General Counsel
Interactive Advertising Bureau
575 7th St. NW, Ste. W3016
Washington, DC 20004
Tel: (202) 253-1466

Date: July 13, 2012

²⁰ "White House, DOC and FTC Commend DAA's Self-regulatory Program to Protect Consumer Online Privacy," *PRNewsWire*, February 23, 2012: <http://www.prnewswire.com/news-releases/white-house-doc-and-ftc-commend-daas-self-regulatory-program-to-protect-consumer-online-privacy-140170013.html>