

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION**

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

COMMENTS OF AT&T INC.

David L. Lawson
Alan Charles Raul
Edward R. McNicholas
Elisa K. Jillson
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

James J.R. Talbot
Gary L. Phillips
Peggy Garber
AT&T Inc.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-2055

Kelly Murray
AT&T Services Inc.
208 S. Akard Street
Dallas, TX 75202
(214) 757-8042

Counsel for AT&T Inc.

July 13, 2012

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY1

I. THE MOBILE MARKET IS COMPLEX AND EVOLVING RAPIDLY.5

II. A COMPREHENSIVE AND FLEXIBLE PRIVACY FRAMEWORK WILL BEST SERVE THE INTERESTS OF CONSUMERS IN THE MOBILE MARKET.8

 A. The Benefits of a Comprehensive, Flexible Approach.....8

 B. The Commission Should Encourage Participation in NTIA and FTC Processes. .10

III. AT&T HAS INDUSTRY LEADING POLICIES AND PROGRAMS TO SAFEGUARD CUSTOMER PRIVACY AND TO PROTECT CUSTOMER DATA.13

 A. AT&T’s Privacy Policies and Practices.....14

 B. AT&T’s Security Policies and Practices.....16

 C. AT&T’s Application of Its Privacy and Security Practices to CIQ.....19

IV. SAFEGUARDING THE PRIVACY AND SECURITY OF CONSUMER INFORMATION REQUIRES THE ACTIVE INVOLVEMENT OF ALL RELEVANT INDUSTRY PARTICIPANTS IN THE MOBILE MARKET21

 A. AT&T Incorporates Privacy Protections and Education into Our Apps Developer Program.....22

 B. AT&T Participates in Various Industry Efforts to Develop Privacy Principles and Guidelines.23

CONCLUSION.....25

**BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION**

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

COMMENTS OF AT&T INC.

Pursuant to the Commission’s Notice dated May 25, 2012, DA 12-818 (“*Notice*”), AT&T Inc. (“AT&T”), on behalf of itself and its affiliates, submits these comments addressing privacy and security issues relating to information stored on mobile communications devices.

INTRODUCTION AND SUMMARY

The defining reality in today’s wireless marketplace is that consumers use and enjoy an extraordinarily broad variety of location-based services and other mobile features that generate and store data on a consumer’s device. In today’s mobile market, an array of industry participants—device manufacturers, operating system providers, platform providers, browsers, search engines, application store owners, and application developers—all provide services directly to consumers over their wireless devices. In light of the rapidly burgeoning array of industry participants involved in the provision of services available via mobile handsets and the corresponding variety of company-specific privacy and security arrangements, President Obama, members of Congress and other policymakers increasingly recognize the need for a single, consistent, and flexible set of policies to govern all of these arrangements. In particular, in February 2012, the White House issued a Consumer Privacy “Blueprint”—the first time any administration has ever so directly and comprehensively addressed consumer privacy issues—

calling for precisely such a framework,¹ and the National Telecommunications and Information Administration in the U.S. Department of Commerce (“NTIA”) has recently sought to facilitate a multi-stakeholder process for the development of voluntary codes of conduct.² Notably, the first multi-stakeholder process convened by NTIA is focused on developing a code of conduct to provide transparency about how mobile application developers and providers of interactive services handle personal data³—a topic the Blueprint specifically identified as highly amenable to multi-stakeholder participation.⁴

In its opening statements, the Blueprint calls for “consistent protections for consumers and lower compliance burdens for companies,” realized through voluntary industry codes of conduct that would be enforced by the one federal agency with jurisdiction over all of the relevant parties—the Federal Trade Commission (“FTC”).⁵ This “comprehensive,” “flexible” and “innovation-enhancing” approach⁶ is far preferable to one in which individual agencies pursue siloed approaches for arbitrarily defined subcategories of data within their jurisdiction—a result that would artificially skew marketplace dynamics and distort competition.⁷ A flexible privacy framework that relies on the development of voluntary codes of conduct with a first layer of self-enforcement by market-based accountability mechanisms, with the backstop of FTC

¹ Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> [hereinafter “Blueprint”].

² Request for Comment, *Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct*, Dep’t. of Commerce, Nat’l Telecomm. Info. Admin., 77 Fed. Reg. 13098 (Mar. 5, 2012), available at http://www.ntia.doc.gov/files/ntia/publications/fr_privacy_rfc_notice_03052012_0.pdf.

³ NTIA Press Release, *First Privacy Multistakeholder Meeting: July 12, 2012* (June 15, 2012) <http://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012> [hereinafter “NTIA Mobile Notice”].

⁴ Blueprint, *supra* n. 1, at 15, 21.

⁵ *Id.* at i-ii.

⁶ *Id.* at 2, 7, 9.

⁷ The Blueprint notes that a uniform approach, by contrast, will actually *enhance* competition, as privacy notices become “a more salient point of competition among different products and services.” *Id.* at 14.

oversight, can best take account of the role that each participant plays in the mobile marketplace. These new standards should focus on transparency and clarity so that consumers are given “usable tools and clear explanations” and can exercise responsibility “to make meaningful choices” to safeguard their privacy and security.⁸

AT&T strives to be a market leader on consumer privacy and security, and is committed to advancing best industry practices and working cooperatively with government, industry and other stakeholders to protect consumers and to promote valuable new products and services. For example, AT&T participates in the Digital Advertising Alliance’s (“DAA”) Advertising Choice program, a program that applies to a wide swath of players in the online marketplace (*e.g.*, advertising agencies, ad networks, sellers of goods and services, publishers, and technology companies). AT&T employs well known third-party enforcement services, to verify compliance with this program, and believes that such industry-wide third-party accountability mechanisms are effective in promoting compliance. They also help to assure that government resources can be properly focused on the more serious and harmful violations.

Whatever level of government oversight is ultimately deemed appropriate to safeguard consumer privacy, it must apply equally and fairly to all market participants. Otherwise, the regulatory disparity will skew competition and deny consumers the full benefits of a vigorously competitive marketplace. In short, the best approach—in line with President Obama’s regulatory Executive Orders encouraging agencies to promote flexibility, simplicity, harmonization, and coordination⁹—is to encourage participation of government, industry and interested persons in

⁸ *Id.* at 13.

⁹ The President’s Executive Order 13579 requests that independent agencies apply the regulatory reform principles applicable to other federal agencies pursuant to Executive Orders Nos. 13563 and 12866. Exec. Order No. 13,579, 76 Fed. Reg. 41587 (July 11, 2011), available at <http://www.gpo.gov/fdsys/pkg/FR-2011-07-14/pdf/2011-17953.pdf>. Executive Order No. 13563 provides, *inter alia*:

multi-stakeholder processes to develop mobile privacy codes of conduct.¹⁰ Government and non-government organizations and other stakeholders should actively support and encourage robust participation in the NTIA’s ongoing effort to facilitate development of voluntary codes of conduct on a broad range of mobile (and other) privacy issues.¹¹ Codes of conduct can and should “[b]uild on the successes of Internet policymaking” by “[p]rivate-sector standards-setting organizations” and the substantial privacy and security efforts already taken by AT&T, other market participants and NGOs, to ensure that all stakeholders in the mobile marketplace are committed and obligated to respect consumer privacy and security.¹² As the Blueprint predicts, this process will result in real advances in privacy and security options for consumers. Third-party accountability mechanisms and FTC backstop enforcement will ensure consistent

Sec. 3. Integration and Innovation. Some sectors and industries face a significant number of regulatory requirements, some of which may be redundant, inconsistent, or overlapping. Greater coordination across agencies could reduce these requirements, thus reducing costs and simplifying and harmonizing rules. In developing regulatory actions and identifying appropriate approaches, each agency shall attempt to promote such coordination, simplification, and harmonization. Each agency shall also seek to identify, as appropriate, means to achieve regulatory goals that are designed to promote innovation.

Sec. 4. Flexible Approaches. Where relevant, feasible, and consistent with regulatory objectives, and to the extent permitted by law, each agency shall identify and consider regulatory approaches that reduce burdens and maintain flexibility and freedom of choice for the public. These approaches include warnings, appropriate default rules, and disclosure requirements as well as provision of information to the public in a form that is clear and intelligible.

Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 18, 2011), available at <http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf>.

¹⁰ Notably, Chairman Genachowski has been a vocal proponent of precisely this sort of regulatory reform. He welcomed Executive Order 13579, noting his intention to make “regulatory reform a top priority, improve[e] FCC processes and decisions to support innovation, economic growth, and America’s global competitiveness . . . [and to] . . . incorporat[e] cost-benefit analysis into our decision-making.” See FCC News Release, *Statement from FCC Chairman Julius Genachowski on the Executive Order on Regulatory Reform and Independent Agencies* (July 11, 2011), <http://www.fcc.gov/document/chairman-genachowski-welcomes-regulatory-reform>.

¹¹ The Commission asked whether it should take steps to encourage privacy by design for software for mobile devices. We believe that this topic, in particular, is best addressed through the NTIA multi-stakeholder process and similar self-regulatory initiatives. Participants in the mobile industry operate in a global market and are highly responsive to the rapidly evolving needs and demands of consumers and other market participants. Interposing rigid regulation as industry standards are developing would be premature and hamper continued innovation.

¹² Blueprint, *supra* n. 1, at 25.

compliance with uniform standards.¹³ Given how rapidly the mobile marketplace as well as consumer uses and expectations are changing, a flexible approach, rather than a “rigid set of requirements,”¹⁴ will yield the greatest advances in privacy and security as well as the continued mobile wireless innovation that is a major driver of economic growth.

I. THE MOBILE MARKET IS COMPLEX AND EVOLVING RAPIDLY.

The Commission has asked about the evolution of the privacy and security practices of mobile wireless carriers with respect to information on customer mobile communication devices since the Commission last solicited comments on this issue in 2007. The Notice observes that, since 2007, “technologies and business practices have evolved dramatically” as “[t]he devices consumers use to access mobile wireless networks have become more sophisticated and powerful.”¹⁵

This is indisputably true. The past five years have seen a rapid expansion of smart phone adoption by customers and a corresponding explosion in the use of mobile applications that provide an ever-increasing array of services, including myriad location-based services (“LBS”).¹⁶ As customers enjoy the increased functionality of smart devices and applications, the amount of information customers are accessing, storing and sharing (with friends, family and various

¹³ *Id.* at 32 (stating that “[t]he Administration encourages stakeholders to work together to identify globally accepted accountability mechanisms when developing codes of conduct”).

¹⁴ *Id.* at 2.

¹⁵ Notice at 1.

¹⁶ See, e.g., FCC Release, *Remarks of Chairman Genachowski to Georgetown Center for Business and Public Policy* (Nov. 7, 2011), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-310876A1.pdf (“Perhaps the biggest area where changes in technology require a rethinking of FCC rules is mobile communications. The world is going mobile. There are now more active cell phones in the U.S. than there are people, and the majority of new phones being activated each day are smart phones. In fact, mobile broadband is being adopted faster than any computing platform in history – creating a uniquely powerful platform for innovation and job creation.”); Prepared Statement of the FTC, *Protecting Mobile Privacy: Your SmartPhones, Tablets, Cell Phones and Your Privacy*, Before the U.S. Senate Comm. on the Judiciary, Subcomm. for Privacy, Technology and the Law, at 1-2 (May 10, 2011), available at <http://www.ftc.gov/os/testimony/110510mobileprivacysenate.pdf> [hereinafter “FTC Statement”] (“Mobile technology is exploding with a range of new products and services for consumers....Companies are increasingly using this new mobile medium to provide enhanced benefits to consumers, whether to provide online services or content or to market other goods and services.”).

service providers) has greatly expanded. The data practices of mobile wireless service providers—and the many other participants in the mobile marketplace—have necessarily evolved in response to the changing market.

The popularity of data services and mobile applications has revolutionized what consumers expect from their mobile devices. Mobile devices are no longer viewed solely, or perhaps even primarily, as a vehicle for traditional telecommunications services offered by the mobile provider. Rather, consumers today increasingly view mobile devices as vehicles for engaging in a wide range of activities, including, among many others, social networking, navigation, news and weather, conferencing, gaming, music, video, and cloud-based storage.¹⁷ Consumers can choose from *millions* of applications for these and other services from a number of different application stores. And, consumers are clearly using these applications: they have downloaded more than *25 billion* applications from Apple’s “App Store” alone.¹⁸

As a result, a wide range of industry participants, including device manufacturers, providers of browsers, operating system providers, platform providers, applications and numerous other services,¹⁹ are forming customer relationships based on mobile services. To name just a few examples, Apple, Groupon, LivingSocial, Facebook, Foursquare, Yelp!, Twitter, Skype, Google, Fandango, and OpenTable, all offer popular mobile services that both collect and use customer data. Indeed, customers today often expect their devices to be “location aware” to provide the location-based services they desire. As the Commission recently reported, “7,200 location-based applications were offered in February 2010, compared to 3,300 location-

¹⁷ FCC Wireless Telecomm. Bureau Report, *Location-Based Services: An Overview of Opportunities and Other Considerations*, at 10-11, available at <http://www.fcc.gov/document/location-based-services-report> [hereinafter “LBS Report”]; FTC Statement, *supra* n. 16, at 2-3.

¹⁸ LBS Report, *supra* n. 17, at 9.

¹⁹ *Id.* at 27.

applications in July 2009” and in “June 2011, Foursquare, the location-based social networking company, reported that it had exceeded ten million users who have “checked-in,” posting their location to friends over *750 million times*.²⁰

In short, traditional telecommunications services face growing and intense competition from a host of online services, including Google Voice, Skype, Apple’s Face Time and iMessage services, and other services offered as mobile applications. An increasingly wide array of participants in the mobile wireless ecosystem—with varying degrees of sophistication in privacy and security offerings—have thus become prominent players in the mobile marketplace.²¹ Consumers certainly are not cognizant of fine legal distinctions between telecommunications services and other types of services as they choose among the wide variety of service offerings that are available to them in today’s mobile market.

A driving force of this increasing competition in the mobile ecosystem over the last five years has seen the emergence of large online platforms as the entry point for consumers to access communications, content and social networking services. Companies such as Google, Apple and Facebook have relationships with hundreds of millions of mobile users.²² These relationships involve the provision of a growing set of vertically integrated services. These large platform providers are playing a central role in consumers’ online experiences and in the management of consumers’ personal data. Moreover, platforms typically offer services that are available across multiple device types (*e.g.*, PCs, smartphones, tables, set-top boxes) and different modes of

²⁰ *Id.* at 8 (emphasis added).

²¹ *Id.* at 12, 27

²²For smart phones alone, the U.S. subscriber base hit 101.3 million in 2012, according to ComScore, with the following OS market shares: Google – 48.6%, Apple – 29.5%, RIM – 15.2%, Microsoft – 4.4%, Symbian – 1.5%. See Press Release, *ComScore Reports January 2012 U.S. Mobile Subscriber Market Share* (Mar. 6, 2012), [http://www.comscore.com/Press Events/Press Releases/2012/3/comScore Reports January 2012 U.S. Mobile Subscriber Market Share](http://www.comscore.com/Press%20Events/Press%20Releases/2012/3/comScore%20Reports%20January%202012%20U.S.%20Mobile%20Subscriber%20Market%20Share). Facebook reported having approximately 450 million mobile users worldwide in April 2012. See Julianne Pepitone, *Facebook Coughs Up Details on its Mobile Problem*, CNN Money (May 10, 2012), <http://money.cnn.com/2012/05/10/technology/facebook-mobile-users/index.htm>.

Internet access. For example, a mobile user may switch their wireless carrier while seamlessly keeping the same mobile operating system and application store platform provider. As a result, these large platform providers have developed deep relationships with consumers, which often may be accessed from a variety of devices and underlying Internet access connections.

II. A COMPREHENSIVE AND FLEXIBLE PRIVACY FRAMEWORK WILL BEST SERVE THE INTERESTS OF CONSUMERS IN THE MOBILE MARKET.

A. The Benefits of a Comprehensive, Flexible Approach.

Given the wide range of industry participants collecting and using customer data, a single, comprehensive approach that encompasses all mobile services would be far superior to a piecemeal regulatory approach in which individual agencies impose different rules for whichever small slice of data falls within their jurisdictions. Moreover, a single, comprehensive approach is the *only* approach consistent with President Obama’s Executive Order requiring federal agencies to “remove outdated regulations that stifle job creation and make our economy less competitive ... and help bring order to regulations that have become a patchwork of overlapping rules[.]”²³

Rules that single out telecommunications services, while ignoring the large majority of other services and service providers that obtain and use substantially the same (or more) consumer information, are anachronistic in the new mobile landscape. As such, they are neither effective in protecting consumer privacy and security, nor conducive to job creation and innovation. They are ineffective for several reasons. The most obvious is that they fail to reach the services that most implicate consumer privacy, so that, even in the best case scenario, they have limited impact. And the real world does not present the best case scenario. Rules that apply only to a shrinking subset of mobile services fail to offer consumers a uniform approach to

²³ Barack Obama, *Toward a 21st Century Regulatory System*, Wall St. J. (Jan. 18, 2011) [*hereinafter* “Obama Editorial”]; *accord* Blueprint, *supra* n. 1, at 38 (calling for a uniform approach that will “avoid creating duplicative regulatory burdens”).

privacy and security. Consumers do not think in terms of the arbitrary statutory distinctions that place similar data into different regulatory categories; rules that apply only to a fraction of the relevant data will confuse consumers, who are likely to believe that the same rules apply uniformly and consistently to all services and providers throughout the wireless ecosystem. In contrast, eliminating the current “patchwork of overlapping [and “outdated”] rules”²⁴ that “treat similar technologies within the communications sector differently” would allow a clear, uniform approach to privacy and security.²⁵

A siloed approach subjecting different services to different regulatory frameworks also would skew competition, leading to inefficient market outcomes. Imposing more prescriptive regulatory standards on telecommunications services, for example, leaves these services subject to outdated marketing restrictions that go far beyond protections needed to safeguard consumer privacy. Yet at the same time, those rules have no applicability to mobile applications and other services that are growing rapidly and, in some cases, raising privacy and security issues.²⁶ For example, the FCC’s privacy rules apply to traditional mobile voice services and “interconnected” VoIP services. But they do not apply to the growing host of one-way VoIP and other online voice, messaging and video-conferencing services that are offered as mobile applications. This category of unregulated services includes popular applications such as Skype, Google Voice and Apple’s Face Time. There is no rational basis for a regulatory regime that subjects comparable and competitive services to drastically different sets of privacy rules.

²⁴ Obama Editorial, *supra* n. 23.

²⁵ Blueprint, *supra* n. 1, at 39.

²⁶ *See, e.g.*, NTIA Mobile Notice, *supra* n. 3.

B. The Commission Should Encourage Participation in NTIA and FTC Processes.

Because of the need for a uniform, consistent approach applicable to *all* of the participants in the wireless ecosystem, the Federal Trade Commission (as the Blueprint expressly recognized) is particularly well-suited to spearhead development and enforcement of federal consumer privacy policy (along with state attorneys general who provide complementary enforcement at the state level).²⁷ And, in fact, the FTC has substantially increased its oversight of mobile privacy issues in recent years (as discussed more below), with state attorneys general following suit.²⁸ Federal FTC and state attorney general enforcement provides a solid baseline level of protection throughout the industry “that effectively protect[s] consumer data privacy within a flexible and evolving approach to changing technologies and markets.”²⁹ In contrast, the Commission’s scope of authority is far too limited to implement a consistent policy for the mobile ecosystem as a whole. Section 222 applies by its express terms only to telecommunications carriers. It does not apply to information service providers or other non-carrier entities, nor does it apply to telecommunications carriers when they are not acting in their capacity as such. It is further limited to certain types of customer information received by telecommunications carriers, as described in the statutory definition of customer proprietary

²⁷ Blueprint, *supra* n. 1, at 29 (explaining the scope of the FTC’s “significant enforcement and policy expertise...on consumer data privacy issues” and noting active state attorney general participation in enforcement of data privacy issues).

²⁸ For example, California Attorney General Kamala D. Harris recently announced that Facebook has become the seventh company to sign the state’s Joint Statement of Principles regarding privacy protections for mobile apps. Amazon, Apple, Hewlett-Packard, Microsoft, and Research in Motion have also signed the agreement. See Press Release, State of California, Department of Justice, Office of the Attorney General, *Attorney General Kamala D. Harris Announces Expansion of California’s Consumer Privacy Protections to Social Apps as Facebook Signs App Agreement* (June 22, 2012), <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer>. Moreover, the new President of the National Association of Attorneys General, Maryland Attorney General Doug Gansler, has announced “Privacy in the Digital Age,” as his year-long presidential initiative for NAAG. See News Release, Nat’l Assoc. of Attorneys General (June 22, 2012), <http://www.naag.org/new-naag-president-is-maryland-attorney-general.php>.

²⁹ Blueprint, *supra* n. 1, at 29.

network information.³⁰ It would thus not be in the public interest for the Commission to develop a new set of balkanized regulations or declaratory rulings for the small percentage of data stored on mobile devices that falls within the Commission’s purview.

That does not mean that the Commission should have no meaningful role in the development of a comprehensive framework for privacy issues involving wireless services and information stored on wireless devices. To the contrary, the Commission can and should use its expertise to support the FTC, the NTIA, and industry stakeholders in their development of a privacy and security framework that applies equally to each service and service provider in the mobile marketplace.

2. The Role of the FTC.

The FTC is well-positioned to be responsible for mobile privacy issues. The FTC has been very active in the mobile sphere, both through guidance and enforcement actions, and it has taken numerous steps to raise consumer awareness and to encourage proactive industry involvement in addressing emerging mobile issues. As the FTC stated in testimony last year to the U.S. Senate, Committee on the Judiciary, Subcommittee for Privacy, Technology and the Law, “[f]or more than a decade, the [FTC] has explored mobile and wireless issues” under its authority to enforce the FTC Act.³¹ For example, the FTC has held a number of workshops on mobile issues, including a workshop to discuss the privacy implications of mobile computing,³² a

³⁰ See 47 U.S.C. § 222(c) & (h)(1). See also *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1229 n.1 (10th Cir. 1999) (Section 222 “recognizes three types of customer information: (1) CPNI; (2) aggregate customer information; and (3) subscriber list information”); *In the Matter of Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, 4 n. 7 (FCC Apr. 2, 2007), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf (setting forth “three general categories of customer information to which different privacy protections and carrier obligations apply pursuant to section 222”).

³¹ FTC Statement, *supra* n. 16, at 3 (summarizing the FTC’s activity on mobile privacy issues over the past decade).

³² FTC Transcript of Roundtable Record, *Exploring Privacy: A Roundtable Series: Panel 4, “Privacy Implication of Mobile Computing*, at 238 (Jan. 28, 2010), http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.Pdf.

workshop on consumer protection issues concerning mobile payments,³³ and a workshop on advertising and privacy disclosures in mobile environments.³⁴ Among other enforcement actions on mobile privacy issues, the FTC settled charges with mobile application developers that violated the FTC’s children’s privacy rule by collecting and disclosing children’s personal information without prior parental consent,³⁵ and that advertised apps with misleading online endorsements and disclosures.³⁶ In response to “an explosion in children’s use of mobile devices,” the FTC proposed a new rule under the Children’s Online Privacy Protection Act, 15 U.S.C. § 6501, *et seq.*, that is designed to prevent mobile apps from capturing children’s personal information without parental consent.³⁷ The FTC released a report on the inadequacy of privacy disclosures in mobile apps for children, which exposed the fact that neither mobile app stores nor mobile app developers are explaining to consumers what data are being collected and how.³⁸

And there is more to come. The FTC’s comprehensive privacy report, issued in March of this year, stated: “Over the course of the next year, [FTC] staff will promote the framework’s implementation by focusing its policymaking efforts on five main actions items”—including “[m]obile.”³⁹ Recognizing the FTC’s expertise in this area, the Blueprint identified FTC enforcement as the appropriate failsafe for ensuring compliance with voluntary codes of

³³ FTC Press Release, *FTC Announces Agenda, Panelists for Mobile Payments Workshop* (Apr. 12, 2012), <http://www.ftc.gov/opa/2012/04/mobilepayments.shtm>.

³⁴ FTC Press Release, *FTC Announces Final Agenda and Panelists for Workshop about Advertising and Privacy Disclosures in Online and Mobile Media* (May 28, 2012), http://ftc.gov/opa/2012/05/dotcomdiscl_ma.shtm.

³⁵ Consent Order, *United States v. W3 Innovations, LLC*, No. CV11-03958 (N.D. Cal. filed Aug. 12, 2011).

³⁶ FTC Press Release, *Public Relations Firm to Settle Charges that It Advertised Clients’ Gaming Apps Through Misleading Online Endorsements* (Aug. 26, 2010), <http://ftc.gov/opa/2010/08/reverb.shtm>. (describing consent order in *In the Matter of Reverb Communications, Inc.*, FTC File No. 092 3199).

³⁷ See 76 Fed. Reg. 59804, 59812 (Sept. 27, 2011).

³⁸ FTC Staff Report, *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing* (Feb. 2012), available at http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf.

³⁹ FTC Report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, at v (Mar. 2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>.

conduct.⁴⁰ The FTC has announced its readiness to accept this mantle, telling Congress that it is “committed to protecting consumers’ privacy in the mobile sphere[,] by bringing enforcement where appropriate and by working with industry and consumer groups to develop workable solutions that protect consumers while allowing innovation in this growing marketplace.”⁴¹

In short, the President’s Blueprint identifies the right path. Flexible industry standards articulated in voluntary codes of conduct will promote the best privacy and security practices as well as the best environment for continued innovation.⁴² Companies will continue to find it in their direct economic interest to promote transparency in order to foster consumer understanding of and comfort with innovation, and such transparency will give consumers confidence in new technologies. As the Commission recently acknowledged in the cybersecurity context, voluntary efforts by AT&T and industry members can be effective to “better secure their communications networks and protect consumers and business.”⁴³ Any enforcement action that might be warranted can be handled by the FTC.

III. AT&T HAS INDUSTRY LEADING POLICIES AND PROGRAMS TO SAFEGUARD CUSTOMER PRIVACY AND TO PROTECT CUSTOMER DATA.

As the mobile wireless ecosystem has continued to evolve rapidly to provide customers with an increasing array of innovative services, transparency and security are values essential to ensuring that customers understand which data may be collected, how that data might be used, and how it is secured, so that customers can make informed choices about devices, services, and

⁴⁰ Blueprint, *supra* n.1, at 29.

⁴¹ FTC Statement, *supra* n. 16, at 12.

⁴² Blueprint, *supra* n. 1, at 2, 5, 24, 31.

⁴³ FCC News Release, *CSRIC Adopts Recs. To Minimize Three Major Cyber Threats*, (Mar. 22, 2012), <http://www.fcc.gov/document/csric-adopts-recs-minimize-three-major-cyber-threats> (“Chairman Genachowski applauds voluntary commitments by nation’s largest Internet Service Providers, including AT&T, CenturyLink, Comcast, Cox, Sprint, Time Warner Cable, T-Mobile and Verizon”).

applications.⁴⁴ AT&T believes that the better a customer understands a service, the more likely it is that the customer will benefit from and seek out that service. For these reasons, AT&T has worked diligently to develop and adopt among the most transparent and robust privacy and security policies and procedures in the industry. These policies and procedures apply to all AT&T services and data, including to the Carrier IQ (“CIQ”) data AT&T uses to improve its network for the benefit of all users.

As the mobile services offered by AT&T, device-makers, and applications developers have expanded and evolved to use customer data to provide advanced location-based services, AT&T has responded by developing and revising its privacy and security practices and policies and making those policies transparent to customers.

A. AT&T’s Privacy Policies and Practices.

During the past several years, AT&T has devoted considerable resources towards developing industry-leading policies and practices to protect customer privacy. In 2009, AT&T adopted an updated, consolidated and streamlined privacy policy applicable to all of AT&T’s business units and services. Among other things, the AT&T Privacy Policy is designed to describe in an easy-to-understand manner, and in a single, easy-to-find place, the information AT&T collects, how that information is collected, and how it is used.⁴⁵

In November of 2010, AT&T posted an update to its Privacy Policy that significantly expanded its Frequently Asked Question (“FAQ”) section devoted to location information. The updated policy, which became effective in March of 2011, provides additional information

⁴⁴ Cf. LBS Report, *supra* n. 17, at 19 (“One of the most important aspects of companies’ approaches to privacy is that they provide transparent notice to consumers regarding the company’s privacy practices, informing the consumer as to what the company is doing with the personal information it collects.”).

⁴⁵ See AT&T Privacy Policy, <http://www.att.com/gen/privacy-policy?pid=2506>.

describing location information, how it is collected, how AT&T uses it, how AT&T's location-based services function, where and how they may be obtained, and how they work.⁴⁶

AT&T's approach to protecting our customers' privacy rests upon four pillars: transparency, consumer control, privacy protection and consumer value. Consistent with its Privacy Policy, AT&T protects the privacy and security of customers' personal information through encryption and other security safeguards described in subsection B below. AT&T does not sell its customers' personal information, and disclosure to non-A&T entities is limited to special circumstances described in the Privacy Policy, such as responding to 911 calls and other emergencies, complying with legal process, to assist in identity verification and fraud prevention, to enforce AT&T's rights, to obtain payment for products and services described on customer billing statements, etc. AT&T ensures both control and transparency in its privacy practices by clearly explaining its practices in the Privacy Policy and FAQs and by providing customers with prompt notice of changes to the Policy.

While AT&T does not exercise control over third-party policies or practices, it endeavors to encourage privacy best practices by third-party applications.⁴⁷ Accordingly, all third-party applications on AT&T's AppCenter go through a content review process that, among other things, determines whether the application collects customer information. If so, the application will be rejected if there is no associated privacy policy, or if the privacy policy in place does not specifically disclose: (1) what customer information is collected and how it will be used; (2) the identity of the party collecting the information; (3) whether the customer information is shared

⁴⁶ See AT&T Privacy Policy FAQs, <http://www.att.com/gen/privacy-policy?pid=13692>.

⁴⁷ AT&T does not assume any responsibility for third-party products, which are subject solely to the privacy policy of the third party. AT&T attempts to foster privacy and security with the guidelines described here, but does not act as the guarantor of the privacy or security of any third-party product or service. For general third party applications that are provided by the Android Marketplace, Apple's iTunes App store, independent app stores such as Amazon, or any other platform or entities app repository, AT&T has no participation in any assessment process. These distribution methods are solely controlled and owned by those entities.

with third parties; (4) the use of any tracking technology; and (5) the security measures in place to protect that information. Similarly, in order to utilize AT&T's application program interface ("API"), third-party developers are contractually required to provide and prominently display a privacy policy outlining their uses of customer information and the protections for that information.

B. AT&T's Security Policies and Practices.

AT&T applies to its mobile services the same robust security measures AT&T applies to all of its services. Specifically, as part of its comprehensive information security program, AT&T maintains administrative, technical, and physical safeguards to secure customer data, to prevent unauthorized access to or disclosure of that information, and to ensure customer data is used only for the purposes for which it was collected.

All AT&T employees are subject to the AT&T Code of Business Conduct, which requires all employees to follow the legal requirements and company policies related to the privacy of communications and the security and privacy of customer records, or face disciplinary action (up to and including dismissal). AT&T personnel receive regular training, including annual privacy training, to reinforce the company's standards of confidentiality and security, and to ensure compliance with AT&T's policies on the security and privacy and customer personal information.

Our security policies provide for security controls based on industry standards and best practices, including encryption of information classified as Sensitive Personal Information ("SPI"). With regard to location information, we define SPI to include the longitude and latitude coordinates of a mobile device in combination with customer name or a unique identifier derived from that device, such as the MSISDN (Mobile Station Integrated Services Digital Network Number). AT&T has established a comprehensive program to identify occurrences of SPI in our

corporate databases and encrypt that data according to our security policies. That program is expected to be substantially complete by the end of 2012, with some carryover to work into 2013. This illustrates AT&T's approach to security: consistently robust security, with thoughtful efforts to improve.

Encryption is only one element of AT&T's comprehensive security program. For example, AT&T minimizes access to customer personal information in several other ways, including by limiting access to AT&T data and AT&T systems to authorized personnel who require access to perform authorized functions; requiring user authentication to access sensitive data maintained in AT&T's computer systems; and by requiring caller/online authentication before providing account information. In addition to these electronic access controls, AT&T maintains technical controls, which securely maintain and protect AT&T's information storage and associated infrastructure.

Our security procedures extend not only to storage and processing of customer information, but also to retention and secure destruction of customer information. As stated in the AT&T Privacy Policy, we retain the personal information of our customers and users "as long as needed for business, tax or legal purposes, after which we destroy it by making it unreadable or undecipherable."⁴⁸

In addition, AT&T partners with mobile device original equipment manufacturers ("OEMs") and operating system platform providers to facilitate compliance with AT&T's product standards, which include certain baseline device security measures. These security measures guard against unauthorized access to devices via known vulnerabilities, such as by surreptitious Bluetooth access; protection of information from indiscriminate access, such as

⁴⁸ See AT&T Privacy Policy FAQ, *Questions About Data Protection and Security*, <http://www.att.com/gen/privacy-policy?pid=2506>.

arbitrary third party applications; unauthorized or inappropriate use of the network by the device; and installation or execution of unauthorized or inappropriate software on devices as delivered to AT&T.

AT&T provides guidance to OEMs for minimizing many known risks. For example, devices should obtain user permission before accessing wireless (non-cellular) connections to others' devices through methods like Wi-Fi, Bluetooth®, IrDA, etc.; devices should not host files which can be read from or written to by any third party application; and devices should not host applications which unjustifiably run as the system or “root” user. To bolster the security of data transmission of AT&T devices, OEMs should ensure that Wi-Fi capable devices support Wi-Fi encryption methods (e.g., WEP and WPA).

AT&T also provides consumers with education materials about mobile security. For example, on the “AT&T Tech Channel,” customers can navigate to the “AT&T ThreatTraq” for information about latest security news and trends,⁴⁹ or to “Security Tips” for practical tips for enterprise and home security.⁵⁰ AT&T publishes “Wi-Fi Security Tips” that explain important precautions to customers about using public Wi-Fi connections.⁵¹ AT&T Wireless Support offers specific mobile security guidance.⁵²

In addition, on one of AT&T's main consumer-facing portals, “AT&T Smart Controls,” AT&T provides customers with clear methods for preserving parental control and safeguarding personal information on mobile devices.⁵³ Features available on this website pertain to stolen

⁴⁹ AT&T, *Tech Channel: AT&T ThreatTraq*, <http://techchannel.att.com/showpage.cfm?Cyber-Threat-Report>.

⁵⁰ AT&T, *Tech Channel: Security Tips*, <http://techchannel.att.com/showpage.cfm?Security-Tips>.

⁵¹ AT&T, *Smart Controls: Wi-Fi Security Tips*, <http://www.att.com/gen/general?pid=6504>.

⁵² AT&T, *Wireless Support: Solutions for Security* <http://www.att.com/esupport/main.jsp?cv=820&ct=800007&view=all&pv=2> (addressing mobile issues).

⁵³ AT&T, *Smart Controls*, <http://www.att.net/smartcontrols>.

mobile phone safety and tools designed to curb the desire to text and drive. The AT&T Smart Controls website includes links to several third-party organizations that offer information about, among other things, mobile security. The AT&T Mobile Safety website provides a variety of tools and information for parents on children's use of mobile technology.⁵⁴

C. AT&T's Application of Its Privacy and Security Practices to CIQ.

The Notice specifically asks about the privacy and security practices related to Carrier IQ data. CIQ is software that is installed on certain devices and also embedded in AT&T's Mark The Spot ("MTS") application software. AT&T uses CIQ solely to collect device-side technical data for network management and service improvement purposes. These data have been invaluable to AT&T in improving its network and the services it offers to its customers.

For example, when a customer's voice call or data session fails to connect or is dropped, the data recorded by AT&T's network may not contain sufficient information to permit AT&T to determine the reason for the problem. Indeed, when a device fails to connect at all, the network will not even know of the failure. The CIQ software in the device records the location, time, network events, and various technical data that AT&T technicians can then analyze to determine the cause of the failure and ultimately to fix the problem. AT&T has used this data, for example, to identify where network expansion and upgrades are most needed.

The CIQ data also records information indicating when the device has been forced to fall back to a slower data connection (*e.g.*, from 3G service to 2G service), or when the device initiates roaming on another carrier's network. These technical data likewise permit AT&T to identify holes in its existing network that are not otherwise detected by AT&T's network

⁵⁴ AT&T, *Mobile Safety*, <http://www.att.com/gen/press-room?pid=1748>.

engineering tools. In addition, CIQ allows AT&T to identify when a particular brand and model device is incurring a disproportionate number of problems relative to other devices.

AT&T's collection of location and other technical data from the device is transparent to customers. AT&T's Wireless Customer Agreement and the MTS End User Licensing Agreement ("EULA") both expressly state that AT&T collects network, performance, and usage information from our network and customer devices, and that AT&T uses that information to maintain and improve our network and their wireless experience.⁵⁵ And AT&T's Privacy Policy describes how AT&T protects such information. AT&T does not share CIQ data with third parties, with the exception that AT&T has shared limited data with the CIQ software vendor, as AT&T's service provider, as necessary to troubleshoot problems and test the software and platform performance.⁵⁶

AT&T also applies its robust security measures to the CIQ data. The CIQ archive file on the device stores data in a compressed and encoded format. The CIQ data in the archive file will automatically be deleted from the device when a different SIM card is used, a Factory Reset is invoked, or there is a re-flashing of the firmware on the device. The CIQ data in the archive file

⁵⁵ AT&T, *Wireless Customer Agreement*, <http://www.wireless.att.com/learn/articles-resources/wireless-terms.jsp>; AT&T, *Mark the Spot End User License Agreement*, Exh. A to Letter from AT&T to Sen. Al Franken (Dec. 14, 2011), <http://apps.fcc.gov/ecfs/document/view?id=7021920018>.

⁵⁶ It is important to recognize that collection of CIQ data, in addition to allowing AT&T to protect and manage its network, serves a collective good, enabling AT&T to provide a better network for *all* customers. Whereas collection of location data from a single individual who opts into LBS benefits that specific individual (*i.e.*, the individual who opts in to LBS can use an LBS-based app, etc.), collection of CIQ data from a large number of persons benefits all network users. Users of LBS choose LBS for an obvious reason: they derive immediate, individual benefit from the service. In contrast, network users given the opportunity to decline collection of CIQ data may choose to free-ride, because their specific participation in CIQ data collection is not directly tied to the positive network experience that is, in fact, enabled by CIQ data collection. Because AT&T uses CIQ data to improve the physical provisioning of its services to its customers, this data falls within the exception in the Act permitting a carrier to use or disclose CPNI "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." *See* 47 U.S.C. § 222(c)(1); *see also id.* § 222(d)(1). Use of such data is also authorized "to protect the rights or property of the carrier." *Id.* § 222(d)(2); *see also* Notice at 3 (acknowledging that the data is used for "network diagnostics or improving customer care").

is uploaded daily in encrypted format to AT&T servers located inside AT&T's secure firewalls, and is not retained in the archive file on the device. These AT&T servers are uniquely provisioned for CIQ data and adhere to AT&T's security policy and requirements that include, among other things, authentication, access controls, security settings, and administrative procedures. The servers are monitored for performance, reliability and unauthorized intrusion. Only properly authorized, authenticated, and approved AT&T employees, CIQ personnel, and contractors acting on behalf of AT&T have access to the data on this server. Our AT&T Labs Operations personnel meet daily to review security, compliance, performance and availability of the CIQ data, and the AT&T Network organization meets weekly to address program status and conduct device testing and certification procedures.

CIQ data is erased so that it is no longer retrievable from the AT&T CIQ servers 60 days after being uploaded from the device, subject to any legal holds that may apply. Personal information is encrypted before CIQ data is sent to downstream systems, which have a 90 day retention period. Data in those systems may be decoded by authorized personnel for certain, specified purposes such as data validation or customer care. After 90 days the encrypted data is eliminated so that CIQ data is only available in the aggregate.

IV. SAFEGUARDING THE PRIVACY AND SECURITY OF CONSUMER INFORMATION REQUIRES THE ACTIVE INVOLVEMENT OF ALL RELEVANT INDUSTRY PARTICIPANTS IN THE MOBILE MARKET.

As discussed above, the mobile marketplace is made up of a variety of players, including wireless carriers, browsers, device manufacturers, operating system providers, platform providers, and application developers.⁵⁷ No segment of the mobile marketplace is the single touch point for consumer interaction, nor is any segment the single collector of consumer data.

⁵⁷ LBS Report, *supra* n. 17, at 13, 27.

To the contrary, consumers have a variety of business relationships with many market participants.

Given the complexity of this mobile ecosystem, collaboration is essential to developing a consistent approach to privacy and security. The trend is positive. Increasingly, market participants are developing tools to work together to provide consumers with clear notice of privacy and security practices throughout the mobile marketplace. AT&T is leading the way by incorporating privacy protections and education into our Apps Developer Program, and by encouraging participation in industry self-regulatory programs. If all key segments of the mobile marketplace participate in these efforts, the mobile marketplace can become a locus of consistently robust privacy and security practices where consumers have real choices about their data. For this reason, we applaud the NTIA's efforts to develop a multi-stakeholder process to create voluntary codes of conduct that will allow consumers to understand and act on their privacy and security interests and foster continued innovation.

A. AT&T Incorporates Privacy Protections and Education into Our Apps Developer Program.

AT&T collaborates with other participants in the mobile marketplace to encourage robust privacy and security practices throughout the mobile ecosystem. This is particularly evident in the Apps Developer Program. AT&T's program consists of an Online Portal and the AT&T Foundry, an open and collaborative community supported by a network of technology companies. Through this program, AT&T provides information and links to the Future of Privacy Forum ("FPF") website, ApplicationPrivacy.org, where apps developers can find tools to develop consumer-friendly privacy practices. The site includes information about emerging standards, best practices, privacy guidelines, platform and application store requirements, as well

as information regarding relevant laws and regulatory guidance so that app developers can address privacy issues throughout the development process.

B. AT&T Participates in Various Industry Efforts to Develop Privacy Principles and Guidelines.

Ultimately, the most productive approach to ensuring robust privacy and security standards is voluntary compliance with broadly accepted industry guidelines. AT&T participates in a number of organizations designed to enhance security standards and best practices for mobile devices, including the Global System for Mobile Communications Association (“GSMA”), the Network Safety Information Exchange (“NSIE”), the Communications Security, Reliability and Interoperability Council (“CSRIC”), the CTIA, and the Messaging Anti-Abuse Working Group (“MAAWG”).

Where a mobile privacy or security issue has been of particular importance, AT&T has participated in targeted industry working groups to develop industry guidelines. For example, AT&T participated in the development of the CTIA Best Practices and Guidelines for Location-Based Services. It participated in discussions with the Center for Democracy and Technology and the Future of Privacy Forum regarding the development of broader industry guidelines on privacy protections for location-based services.⁵⁸ In addition, AT&T is participating in the development of the Digital Advertising Alliance and Mobile Marketing Association (“MMA”) self-regulatory principles for online behavioral advertising (“OBA”) in the mobile environment. AT&T’s privacy group and technical experts are also participating in the World Wide Web Consortium (“WC3”) working group on Do Not Track solutions for mobile browsing.

⁵⁸ See Future of Privacy Forum Website, *Best Practices for Mobile Application Developers*, <http://www.futureofprivacy.org/best-practices-for-mobile-app-developers/>.

AT&T has been an industry leader in developing industry best practices for online behavioral advertising. AT&T implemented the Future of Privacy Forum icon (indicating compliance with self-regulatory principles and making available opt-out of cookies for targeted advertising) even before the DAA opt-out icon for cookies was established. Web pages on our domain www.att.com that collect data for targeted advertising include the DAA icon, and to the extent that AT&T uses behavioral advertising elsewhere, it always makes the DAA opt-out available. AT&T contracted with TRUSTe, which also provides the compliance seal for the AT&T Privacy Policy, to monitor AT&T ads for DAA compliance.

AT&T also participates in a variety of industry bodies and public-private partnerships that address data security issues, and has been urging particular focus on data security in the mobile environment. These partnerships include the National Security Telecommunications Advisory Committee (“NSTAC”), USSS Cyber Crimes Task Force, FBI’s InfraGard®, Computer Emergency Response Team/Coordination Center (“CERT/CC”), the Internet Engineering Task Force (“IETF”), the WC3, the Forum of Incident Response and Security Teams (“FIRST”), Communications - Information Sharing and Analysis Center (“Communications-ISAC”), and ATIS - Network Reliability Steering Committee (“NRSC”). There is increasingly widespread recognition of the importance of mobile security, and these groups are beginning to build the framework to address these important issues.

CONCLUSION

We applaud the FCC's efforts to reassure customers of AT&T, and like-minded companies, of the telecommunication industry's commitment to consumer privacy and security. We believe that it is essential to recognize, however, that this industry is no longer hermetically sealed from other sectors. As the use of mobile devices and data services has skyrocketed, other players—device manufacturers, browsers, search engines, advertising networks, social networks, operating system providers, platform providers, application store developers, and application developers, etc., none of whom is regulated by the FCC—have assumed highly prominent places in consumer interactions, and may collect significant amounts of consumer information. As the White House's Privacy Blueprint notes, balanced, thoughtful engagement with all stakeholders is necessary to preserve and enhance consumer privacy and security and to promote innovation by all players in the mobile marketplace.

The Commission should take particular note that even as it embarks upon this collection of information regarding mobile privacy and security, multi-stakeholder groups already are working to develop voluntary codes of conduct on the very same subject matter. We encourage the Commission to recognize how fast the mobile industry is changing, and how many different players are relevant. The Commission should be sensitive to avoid tilting the playing field for or against any particular participant in the marketplace. The FCC should also recognize that legitimate industry members like AT&T have a track record of committing to meaningful, voluntary efforts to improve communications security—and will continue to do so.

Applying the letter and spirit of President Obama's regulatory Executive Orders counsels in favor of emphasizing flexibility, harmonization and innovation. Burdensome, outdated and overlapping regulations are neither necessary nor consistent with protecting consumers' important interests. Instead, industry-led efforts, coordinated under the White House's

Blueprint, will be most effective to protect privacy and security. In particular, AT&T supports efforts by all stakeholders to promote meaningful transparency and direct communication with their customers regarding their privacy and security policies. This will allow competition in the marketplace to be most effective in addressing the important issues of interest to the Commission in this inquiry.

Respectfully submitted,

/s/

David L. Lawson
Alan Charles Raul
Edward R. McNicholas
Elisa K. Jillson
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
(202) 736-8000

James J.R. Talbot
Gary L. Phillips
Peggy Garber
AT&T Inc.
1120 20th Street, N.W.
Washington, D.C. 20036
(202) 457-2055

Kelly Murray
AT&T Services Inc.
208 S. Akard Street
Dallas, TX 75202
(214) 757-8042

Counsel for AT&T Inc.

July 13, 2012