Before the

FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	)	
	)	
Helping Consumers Harness the Potential Of Location-Based Services	)	WT Docket No. 11-84
	)	
	)	
	)	

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

Leslie Harris
Justin Brookman
Erica Newland

Center for Democracy & Technology
1634 I Street, N.W., Suite 1100
Washington, DC 20006
(202) 637-9800

July 8, 2011

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Helping Consumers Harness the Potential	)	WT Docket No. 11-84.
Of Location-Based Services	)	
	)	
	)	

The Center for Democracy & Technology ("CDT") respectfully submits these comments in response to the Commission's Privacy Public Notice regarding privacy concerns and expectations associated with the use of location-based services. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation and freedom on the decentralized Internet.

We applaud the Commission's leadership in examining the privacy issues presented by location-enabled mobile devices and appreciate the opportunity to address the lack of legal protection facing of what is one of the fastest growing areas of technological innovation.

1. The Promise and Peril of Location-Enabled Mobile Devices

Mobile phones and tablets have exploded in popularity in recent years, and all evidence indicates that this trend will continue. Smartphone sales are expected to eclipse those of desktop and laptop computers combined in the next two years.[1] However, as the Commission is well aware, mobile devices store and transmit a particularly personal set of data. These devices typically allow third parties to access personal information such as contact lists, pictures, browsing history, and identifying information more readily than in traditional internet web browsing. The devices also use and transmit information about a consumer's precise geolocation information as consumers travel from place to place.

At the same time, consumers have less control over their information on mobile devices than through traditional web browsing. While third parties, like ad networks, usually must use "cookies" to track users on the web, they often get access to unique — and unchangeable —device identifiers in the mobile space. While cookies can be deleted by savvy users, device identifiers are permanent, meaning data shared about your device can always be correlated with that device. As is the case with most consumer data, information generated by mobile devices is for the most part not protected by current law and may be collected and shared without users' knowledge or consent.

Consumers interact with their mobile devices by running applications, or "apps" (i.e., programs designed to run on mobile devices). The mobile apps ecosystem is robust and offers an ever-increasing range of functionality from games, music, maps, instant messaging, email, metro schedules, and more. Mobile apps may be preinstalled on the

[1] Cecilia Kang, *Smartphone sales to pass computers in 2012: Morgan Stanley analyst Meeker*, THE WASHINGTON POST, November 11, 2010, http://voices.washingtonpost.com/posttech/2010/11/smartphone_sales_to_pass_compu.html.

device by the manufacturer or distributor, or users can download and install the programs themselves from their operating system's "apps store" (like iTunes or the Android Market), or a third-party store (like Amazon). App developers range from large, multinational corporations to individuals coding in their parents' basements. Generally speaking, we have seen a vibrant and creative app market develop for mobile devices. Unfortunately, it can be hard to know what information these apps have access to and with whom they are sharing it.

Recent studies of this flourishing apps data ecosystem have unearthed troubling findings. A recent survey indicated that of the top 340 free apps, only 19% contained a privacy policy *at all*.[2] Last December, the Wall Street Journal investigated the behavior of the 101 most popular mobile apps, finding that more than half transmitted the user's unique device ID to third parties without the user's consent.[3] Forty-seven apps transmitted the phone's location.[4] One popular music app, Pandora, sent user age, gender, location and phone identifier to various ad networks.[5] In sum, a small phone can leak a big amount of data.

Once an app has access to a user's data, there are usually no rules governing its disclosure, and no controls available to consumers to regain control of it. For the most part, once a party has access to consumer data, that data is effectively "in the wild." It may be retained long after the moment of collection, and often long after the original service has been provided. App developers, advertisers, ad networks and platforms, analytics companies, and any number of other downstream players can share, sell, or unpredictably use data far into the future. Even insurance companies are eying data mined from online services for new predictive models.[6] In short, today's mobile environment provides a gateway into an opaque and largely unregulated market for personal data.

Location data is of particular concern. In recent years, the accuracy of location data has improved while the expense of calculating and obtaining it has declined. As a result, location-based services are an integral part of users' experiences and an increasingly important market for U.S. companies. Consumers like the convenience and relevance of location based services. Location data can be used guide you to the closest coffee shop or help you navigate an unfamiliar neighborhood. Your location can be leveraged to connect you with coupons or deals in your immediate vicinity. And new, innovative, and useful services are introduced daily.

People generally carry their mobile devices wherever they go, making it possible for location data be collected everywhere, at any time, and potentially without prompting. Understandably, many find the use of location data without clear transparency and control troubling. Research shows that people value their location privacy, are less

---

[2] Mark Hachman, *Most Mobile Apps Lack Privacy Policies: Study*, PC MAGAZINE, April 27, 2011, http://www.pcmag.com/article2/0,2817,2384363,00.asp.
[3] Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
[4] *Id.*
[5] *Id.*
[6] Leslie Scism and Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, THE WALL STREET JOURNAL, November 19, 2010, http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

comfortable sharing their location with strangers than with acquaintances, and want granular control over their location information.[7] Indeed, location data is especially sensitive information that can be used to decipher revealing facts or put people at physical risk. Location information could disclose visits to sensitive destinations, like medical clinics, courts and political rallies. Access to location can also be used in stalking and domestic violence.[8] Finally, as an increasing number of minors carry location-capable cell phones and devices, location privacy may become a child safety matter as well.

There are also questions and concerns about the collection, usage, and storage of data by mobile platform providers such as Apple and Google. Because in many instances, these companies are the ones actually calculating your location (based on comparing the WiFi access points in range of your device with known databases), they may receive extremely detailed information about consumer activity, considerably more so than traditional computer operating systems. Although these companies typically assert that data they receive from consumers is anonymized and used merely to build out their databases of access points, these limitations are self-imposed. Furthermore, these platforms may store detailed location and other customer information on the phone itself, which could then be accessed by government officials, potentially without a warrant, malicious hackers, or merely the person who finds your lost phone at Starbucks.[9]

2. Existing Legal Protections for Mobile Device Information are Outdated, Inapplicable, or Unclear

A number of measures currently exist to protect electronic communications, including location information. Unfortunately, technology has far outpaced these protections in both the commercial and government contexts. An update is long overdue.

Following is a summary of relevant laws and rules and an analysis of their application to today's location-enabled mobile devices.

A. The Telecommunications Act of 1996 and Cable Communications Policy Act of 1984 (CPNI Rules)

Through the Telecommunications Act of 1996, with subsequent amendments, Congress has prohibited a telecommunications carrier from disclosing customer proprietary network information (CPNI), including "information that relates to the . . . location . . . [of] any customer of a telecommunications carrier . . . that is made available to the carrier by

---

[7] *See, e.g.,* Janice Y. Tsai, Patrick Kelley, Paul Drielsma, Lorrie Cranor, Jason Hong, Norman Sadeh, *Who's viewed you?: the impact of feedback in a mobile location-sharing application*, Conference on Human Factors in Computing Systems: Proceedings of the 27th international conference on human factors in computing systems (2009), http://www.cs.cmu.edu/~sadeh/Publications/Privacy/CHI2009.pdf; Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge, Location Disclosure to Social Relations: Why, When, & What People Want to Share, CHI '05: Proceedings of the SIGCHI conference on human factors in computing systems (2005), www.placelab.org/publications/pubs/chi05- locDisSocRel-proceedings.pdf.

[8] *See, e.g.,* Rob Stafford, *Tracing a Stalker*, Dateline NBC, June 16, 2007, http://www.msnbc.msn.com/id/19253352/.

[9] *See* Alexis Madrigal, *What Does Your Phone Know About You? More Than You Think*, THE ATLANTIC, April 25, 2011, http://www.theatlantic.com/technology/archive/2011/04/what-does-your-phone-know-about-you-more-than-you-think/237786/.

the customer solely by virtue of the carrier-customer relationship" — except in emergency contexts or "as required by law or with the approval of the customer."[10]

Fifteen years ago, these privacy rules were a groundbreaking development. At the time, telecommunications carriers served as the primary gatekeepers for location information. Information about a cell phone user's location was calculated within a carrier's network using signals sent by the phone to the carrier's service antennas. But the rules have been left behind as the ecosystem has expanded beyond voice (traditionally the purview of telecommunications carriers) to data service (which is often not the purview of telecommunications carriers).

In light of modern location technology, there are at least two major gaps in privacy protections created by the CPNI statute and resulting Federal Communications Commission (FCC) rules:

1. The CPNI rules do not apply to new types of location technologies, applications, and services. More specifically, the CPNI rules do not cover methodologies that are independent of telecommunications carriers covered by the law (e.g., WiFi database lookups, cell tower database lookups, or unassisted GPS lookups). Thus, when an iPhone or Android user installs a location-based application, the location data transmitted by the resulting service is very likely completely unregulated under the CPNI rules.

2. Even, when a telecommunications carrier is involved in providing a location-based service, it may not be covered by the CPNI rules because the FCC has classified wireless broadband as information services rather than telecommunications services. In light of the Wireless Broadband Order, it appears quite possible that even carrier-provided location based services that run over the wireless data network are not protected by the CPNI rules.[11] Although Congress and then the FCC did extend CPNI rules to cover IP-enabled "interconnected" VoIP services,[12] that protection still only extends to voice service regulated under Title II. At best, the application of CPNI rules to carrier-provided location-based data services is a murky question; at worst, the CPNI rules provide no protection whatsoever.

Practically speaking, this creates some striking confusion. A consumer using a mobile phone today can be protected by the CPNI rules one moment and unprotected the next. For example, a user might place a phone call using the traditional Commercial Mobile Radio Service (CMRS). In this case, they could feel secure that the CPNI rules required their carrier to protection their information. After the call, they use an Internet-based app or location service that uses precise geolocation location data. Here, the user is likely unprotected.

As we discuss in more detail below, while many of the gaps in privacy protection for location information that are created by the CPNI rules are best filled by Congressional

---

[10] 47 U.S.C. § 222.

[11] *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*,
Declaratory Ruling, WT Docket No. 07-53, FCC 07-30, 2 (rel. Mar. 23, 2007).

[12] *See* 47 C.F.R. § 64.2001, *et seq.*

legislation, the FCC privacy report should emphasize the existence of these gaps and highlight to Congress the importance of the mobile privacy protection.

B. The Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act was passed in 1986 primarily to address the issue of government access (about which, see below). However, it also contains important limitations on how companies may voluntarily share with other companies customer communications. Most notably, the law prohibits certain companies from sharing the content of customer communications or records without their consent.[13] In theory, this might prohibit mobile operating systems or applications from sharing consumer data without permission. Unfortunately, ECPA, while a very important and forward-looking statute at the time it was passed, was not written with the mobile apps ecosystem in mind. As applied to the current mobile environment, ECPA as a limitation on inter-business sharing of consumer data is, at best, vague and uneven.

When discussing the kinds of mobile applications and services at issue here today, it is not even clear which parties are currently covered by ECPA. ECPA's coverage of stored communications extends only to two categories of services — electronic communications services (ECSs) and remote computing services (RCSs). An ECS is a service that permits users to send or receive communications information (defined in part as "signs, signals, writing, images, sounds, data, or intelligence of any nature")[14] to a third party or parties, like an email service or a private bulletin board such as a restricted Facebook wall. Some apps and location-based services are ECSs, some are not, and some fall into a grey area. For example, a service that allows users to share their location with a specific group of friends or associates is likely an ECS, with the "data or intelligence" communicated to friends being the combination of the user's identity and her location data. However, an app that allows a user to share his location with a restaurant chain solely to allow it to return the location of the nearest restaurant is likely not an ECS, because it does not provide a way to communicate with third parties. The statute ultimately requires highly fact-dependent analysis on the ECS question.

Remote computing services are, if anything, even murkier. An RCS includes any service that provides to the public computer storage or processing. The limited case law developed around this definition has not clarified its boundaries. Courts have held that websites enabling certain commercial transactions are not RCSs, but have suggested that remote processing of user-collected or -generated data is likely to be covered. Almost any app that collects user location or personal data and sends it to a remote server for further processing could, theoretically, fall under the ambit of this provision. However, it is important to note that mobile operating systems — the entities that often generate consumer location information in the first place — likely do not qualify as either ECSs or RCSs, and thus ECPA offers no protections at all as to those companies.

Of course, even if an app were to fall under the ECPA's ambit, there would still be open questions about whether customer data constituted the "content" of a communication subject to protection. If a consumer affirmatively sent a location request to an app maker to ask for a nearby bar or restaurant, ECPA could arguably restrict the transfer of that information to third parties because the consumer's location was the content of a customer-initiated communication. If on the other hand, the app accessed the user's

[13] 18 U.S.C. §§ 2702(a).
[14] 18 U.S.C. §§ 2510(12).

location in the background merely in order to send to a third party to serve relevant advertising, such request probably would not be governed. Such a reading of the statute would however lead to the perverse result that a consumer's information is afforded greater protections when she affirmatively shares sensitive data, as opposed to when her data is shared without her knowledge or consent.

D. Federal Trade Commission Act and State Attorneys General

Absent any affirmative legal requirements provided by sector-specific privacy laws (such as those governing health or financial data), the default privacy rule for most consumer data is set by the FTC Act's prohibition on unfair and deceptive trade practices.[15] Under this authority, the FTC has established some general precedents about what constitutes a deceptive or unfair privacy practice online, such as recent settlements against companies who offered deceptive and ineffective opt-out solutions, and against Google for sharing personal data with other Google customers in violation of previous representations as part of the Buzz product. While these cases are important, they also demonstrate that the FTC is generally limited under current law to bringing enforcement actions against companies that make affirmative misstatements about their own privacy practices. In the absence of a baseline federal privacy law that gives the FTC the tools it needs and establishes it as the lead law enforcement agency for privacy matters, consumer protections in the location privacy space will continue to fall short.

State Attorneys General also have consumer protection mandates that allow them to pursue service providers that engage in unfair or deceptive trade practices. To date, however, perhaps due to the inherent limitations in their authority, relatively little attention has been paid at the state level to consumer privacy concerns.

As the FCC evaluates its role in protecting the privacy of consumer location information, it must be careful not to compromise the FTC's authority to address online privacy issues. Importantly, the common-carrier exception to FTC authority applies to providers of telecommunications services only "to the extent that [they are] engaged in providing telecommunications service."[16] Any non-telecommunications service offered by Internet access service providers, such as e-mail, web-hosting, web apps, content aggregation, and others, remain under FTC oversight.

In the long run, developing a more unified privacy regime, rather than the current patchwork of agency jurisdictions and statutory provisions, is a project that warrants effort and attention, and we recommend that the FCC urge Congress to implement uniform privacy protections. In the meantime, the FCC and FTC should continue after this joint workshop to work together and coordinate sensible policy responses and recommendations in the absence of consistent location privacy protections.

---

[15] The FTC Act, 15 U.S.C. §§ 41 *et seq*.

[16] See Broadband Connectivity Competition Policy, FTC Staff Report, n.159 and accompanying text (2007) (quoting 47 USC § 153(44)), available at http://www.ftc.gov/reports/broadband/v070000report.pdf.

3. Recommendations for the privacy report

Precise location data is created, collected, and used by a wide variety of technologies.[17] Crafting protections for location data is therefore a complex task. CDT believes that the FCC can contribute the most to this process by emphasizing the following in its privacy report:

- The Commission should document the complexity of the current ecosystem as it relates to location-based services and the collection of precise location information. The Commission should explain the wide range of technologies and services involved in the creation of location data, its collection, and its use.
- Commission should closely examine the privacy issues raised by the location information (and other information) collected, retained, shared, and used by common carrier telecommunications services.
- The Commission should highlight that crafting protections for the privacy of mobile location data is important to the future of communications in this country and throughout the world and is important to the growth of the information economy.[18]
- The Commission should emphasize that the existing CPNI rules leave many technologies and use cases unaddressed. As a result, protections for most consumer-generated precise location data are weak or non-existent.
- The Commission should emphasize that in most cases, precise geolocation data should only be collected and/or shared with the informed, affirmative consent of the person whose information is being collected and/or shared.
- The Commission should affirm that its authority over the generation, collection, and use of location data is, however, limited. As we discussed above, the Commission's authority is appropriately over those entities over which the FTC does not have authority, namely common carrier telecommunications services. Indeed, the Commission must avoid significantly compromising the FTC's authority to address online privacy issues. Importantly, the common-carrier exception to FTC authority applies to providers of telecommunications services only "to the extent that [they are] engaged in providing telecommunications service."[19] Thus, the Commission should clearly state that its authority does not include entities such as mobile applications that collect location information, operating systems that request location information, and services operated by companies such as Google and Skyhook wireless that calculate users' location information. The FTC appropriately has (admittedly limited) authority over such entities and should be provided with greater authority to protect consumer privacy over these types of entities. Indeed, the FTC has a long record of working

[17] Testimony of John B. Morris, Jr., General Counsel for the Center for Democracy and Technology, before the House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Communications, Technology, and the Internet on "The Privacy Implications of Commercial Location-Based Services" (Feb. 24, 2010) *available at* http://www.cdt.org/files/pdfs/CDT-MorrisLocationTestimony.pdf.

[18] Department of Commerce (Internet Policy Task Force), Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (Dec. 16, 2010) *available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.

[19] See Broadband Connectivity Competition Policy, FTC Staff Report, n.159 and accompanying text (2007) (quoting 47 USC § 153(44)), available at http://www.ftc.gov/reports/broadband/v070000report.pdf.

to protect consumer privacy at the application layer and is currently actively engaging in this space.[20]

- To this end, the Commission should continue to work closely with the FTC to promote the development of greater protections for consumer location-based information.
- The Commission should call for a baseline consumer privacy law, one that includes provisions that create protections for location-based data.

4. Need for Baseline Consumer Privacy Legislation

Given that the default rule for most consumer data — including sensitive location data — is merely that companies cannot make affirmative misstatements about the use of that data, CDT strongly supports the enactment of a uniform set of baseline rules for personal information collected both online and offline. Location data is not the only type of information governed by a confusing patchwork of laws and rules that leave much data unprotected. Indeed, most consumer data is only weakly protected by existing laws and regulations. A new privacy law should therefore not merely cover location-based information but rather set a baseline for the conditions under which consumer data of all types can be collected and used. We urge the FCC, in its privacy report, to call for such a law.

The Fair Information Practices (FIPPs) should be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. The most recent formulation of the FIPPs by the Department of Homeland Security offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation.[21] Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

For particularly sensitive data, such as health information, financial information, information about religion or sexuality, and — most relevant here — precise geolocation data, a legislative framework should provide for enhanced application of the Fair Information Practice Principles, including for affirmative opt-in consent for the collection

[20] Federal Trade Commission (Bureau of Consumer Protection), A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, 57-63 (Dec. 1, 2010) available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[21] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

and/or transfer of such information. Consumers understandably have greater concerns about the use and storage of such information, and the law should err against presuming a consumer's assent to share such information with others.

Furthermore, the laws governing government access to consumer data should be modernized to require a warrant to access sensitive location information.

4. Conclusion

CDT would like to thank the Commission for investigating this important set of issues. The FCC has an important role to play in promoting the privacy of mobile location information, and CDT looks forward to working with the Commission as it pursues these issues further.

For more information, contact Justin Brookman, justin@cdt.org, (202) 637-9800.