KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

Before the Senate Judiciary Committee
Subcommittee on Privacy, Technology, and the Law

Hearing on
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy"

May 10, 2011

Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Chairman'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.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. I will briefly note the particular privacy issues presented by mobile services, and then describe the inadequacy of existing law to protect consumers. CDT strongly believes that legislation based on the full range of Fair Information Practice Principles (FIPPs) should be enacted to address the privacy challenges faced in the mobile space.

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, 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 consumer's precise geolocation information as consumers travel from place to place.

[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.

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 — unique 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 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 users' 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 data leaves the phone, it 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-

---

[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.

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 and are less 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]

Mobile devices and the services they enable provide consumers with great benefit. But it is imperative that Congress provide a clear policy framework to protect users' privacy and trust. CDT strongly supports privacy legislation that implements the full range of Fair Information Practice Principles (FIPPs) across all consumer data and provides enhanced protections for sensitive information, such as precise geolocation, including enhanced, affirmative opt-in consent.

Unfortunately, today's legal protections fall far short.

---

[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/.

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

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

Following is a summary of relevant laws 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 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] In short, Congress issued a minimal standard that prohibited carriers from releasing location and other customer information on a solely discretionary basis.

Fifteen years ago, these privacy rules were a groundbreaking development. At the time, telecommunications carriers served as the primary gatekeepers for location information. Data 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. These traditional protections have been left behind as we move from voice (traditionally the purview of telecommunications carriers) to data (which is often not the prevue of telecommunications carriers).

In light of modern location technology, there are at least two major shortcomings of the CPNI statute and resulting Federal Communications Commission (FCC) rules:

1. The CPNI rules simply 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 locations). 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 removed wireless broadband service from Title II of the Communications Act (to which the CPNI rules apply) and deregulated it. When the Commission issued its Wireless Broadband Order,[11] Commissioner Copps explained the fractured effect of the Order on the protection of location information under the CPNI rules.[12]

[10] 47 U.S.C. § 222.

[11] *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*,

Thus, modern mobile devices leverage location services that are largely invisible to the telecommunications provider and thus very likely outside the scope of the law. Although Congress and then the FCC did extend CPNI rules to cover IP-enabled "interconnected" VoIP services,[13] 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 location data rendered apart from the telecommunications carrier. Here, the user is likely unprotected.

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.[14] 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")[15] 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.

Declaratory Ruling, WT Docket No. 07-53, FCC 07-30, 2 (rel. Mar. 23, 2007).

[12] *Id* at ¶ 2 (carriers offering Title I services "appear[] to be entirely free, under our present rules, to sell off aspects of the customer[s'] call or location information to the highest bidder.").

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

[14] 18 U.S.C. §§ 2702(a).

[15] 18 U.S.C. §§ 2510(12).

Remote computing services are, if anything, even more murky. 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 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.

Though the issue is not the focus of the present hearing, it is important to note that legislation to clarify the standards for government access to that information should also remain a Congressional priority. While the Communications Assistance for Law Enforcement Act (CALEA) indicates what the standard for law enforcement access to location information *is not,* no statute indicates what the standard for law enforcement access *is.* CALEA provides that a pen register or trap and trace order[16] cannot be used to obtain location information, but that statute is silent on what the standard should be.[17] There is a federal statute on tracking devices, but it does not specify the standard that law enforcement must meet in order to place such a device.[18] Most importantly, the Electronic Communications Privacy Act (ECPA),[19] which sets up the sliding scale of authority for governmental access to information relating to communications (ranging from mere subpoena to warrant), does not specify what standard applies to location information.

This has resulted in a mish-mash of confused decisions while courts struggle to find and apply a legal standard. It has led to sometimes arbitrary distinctions based on whether location information is sought in real time or from storage, the degree of precision in the location information sought, the period(s) during which location information is sought, and the technology

[16] A pen register/trap and trace order permits law enforcement to obtain transactional, non-content information about wire and electronic communications in real time, including numbers dialed on a cellular telephone and telephone numbers of calls coming into a cell phone. *See* 18 U.S.C. §§ 3121-3127.

[17] 47 U.S.C. § 1002(a)(2).

[18] 18 U.S.C. § 3117.

[19] 18 U.S.C. §§ 2510 *et seq.*

used to generate the location information. Some courts[20] have adopted a "hybrid theory" advanced by the Department of Justice, holding that location information is accessible to government *in real time* if it meets the standard for *stored* transactional information in Section 2703(d) of the Stored Communications Act.[21] Other courts have required a higher level of proof – probable cause – for law enforcement access to this prospective location information.[22] As one federal magistrate judge recently testified in front of the House Judiciary Committee, there is no comprehensible standard for magistrate judges to apply when the government requests access to cell site location data – just an incoherent array of competing court decisions.[23]

As the first few circuit court decisions to address governmental requests for location information of all types have started to come down, it is becoming clear that the courts have constitutional concerns with these requests. In August, the D.C. Circuit held that putting a device in place to engage in extended GPS tracking without a warrant violates the Fourth Amendment.[24] In September, the Third Circuit held that magistrate judges faced with a request from the government for cell site location information have discretion under ECPA to insist upon a showing of probable cause, in part because of the potential sensitivity of the information.[25] Both the confusion in the lower courts and the consternation in the appeals courts demonstrate that Congressional attention to these statutes is sorely needed.

Congress enacted ECPA in 1986 to foster new communications technologies by giving users confidence that their privacy would be respected. ECPA helped further the growth of the Internet and proved monumentally important to the U.S. economy. Now, technology is again leaping ahead, but the law is not keeping up. CDT — through its Digital Due Process coalition — has convened technology and communications companies, privacy advocates and academics to create four principles for reforming ECPA for the next quarter-century. One of those principles is that location information should only be accessed through the use of a warrant[26] and we believe Congress should enact legislation that imposes a warrant requirement. Though the larger ECPA reform effort is and should remain independent of the issues being discussed here today, CDT believes setting easily-understood privacy-protective standards for government access to location data is a critical component of ensuring the privacy of American citizens and the success of American technology service providers.

---

[20] *See, e.g., In re Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

[21] The SCA, part of the Electronic Communications Privacy Act, is codified at 18 U.S.C. §§ 2701 *et seq.*

[22] *See, e.g.*, *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F. Supp. 2d 747 (S.D.Tex. 2005).

[23] *See Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the H. Comm. on Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties*, 111th Cong. (June 24, 2010) (statement of Stephen Wm. Smith, United States Magistrate Judge).

[24] *U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

[25] *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010).

[26] For more information on the Digital Due Process coalition and its principles, see Digital Due Process at http://www.digitaldueprocess.org.

C. The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) is a criminal statute that prohibits intentional trespass into and theft from protected computer systems.[27] It criminalizes, in relevant part, one who "intentionally accesses a computer without authorization or exceeds authorized access . . . information from any protected computer."[28] In short, it's a law to prosecute malicious hackers.

The CFAA is a law design to combat egregious computer crimes and cannot, and should not, be a primary tool in protecting consumers' mobile privacy from data sharing for marketing or related purposes. In the past, there have been failed attempts to stretch the CFAA to cover contractual terms of service.[29] CDT has warned that these attempts come with troubling encroachments on civil liberties and freedom of speech.[30] Criminal sanctions for certain computer crimes might well deter bad actors and provide appropriate tools in extreme circumstances. However, it is a blunt instrument not designed to address mobile privacy challenges arising from commercial activity.

The mobile market is nascent and innovating quickly. Many mobile app developers are individuals or small startup companies. They might be amateur programmers, working with various prefabricated pieces of code and advertising solutions. They may or may not have expertise in privacy or relevant law. Criminal sanctions, including jail time, would be heavy-handed and would likely chill the innovation we see today.

D. Federal Trade Commission Act and State Attorneys General

Absent any affirmative legal requirements provided by sectoral 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.[31] 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.

---

[27] 18 U.S.C. § 1030.

[28] 18 U.S.C. § 1030(a)(2)(C).

[29] *See generally*, US v. Drew, Electronic Frontier Foundation, *available at* https://www.eff.org/cases/united-states-v-drew (last visited May 6, 2011).

[30] *Id.*

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

3. The Need for Congressional Action

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. Modern data flows often involve the collection and use of data derived and combined from both online and offline sources, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well. The mobile device space implicates many different kinds of data in a complicated ecosystem. Cramming more notices onto small screens is alone insufficient. We need a data privacy law that incentivizes and requires companies to provide clear and conspicuous notice to consumers about the use of their information and provides for meaningful control of that information. Moreover, companies should collect only as much personal information as necessary, be clear about with whom they're sharing information, and expunge information after it is no longer needed.

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.[32] 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 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, as noted above, the laws governing government access to consumer data should be modernized to require a warrant to access sensitive location information.

[32] 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.

4. Conclusion

CDT would like to thank the Subcommittee again for holding this important hearing. We believe that Congress has a critical role to play in ensuring the privacy of consumers in the growing market of mobile devices and services. CDT looks forward to working with the Members of the Subcommittee as they pursue these issues further.

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