

CDT Testifies on Location Privacy

March 2, 2010

Tags: Array

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

- 1) [CDT Testifies on Location Privacy](#)
- 2) [Location Information is Poorly Protected in the Commercial Context](#)
- 3) [Statutory Protection of Location Information is Woefully Outdated](#)
- 4) [Existing Legal Standards for Access to and Protection of Location Information Are Woefully Inadequate](#)

1) CDT Testifies on Location Privacy

CDT's John Morris recently testified in a Congressional hearing on "The Collection and Use of Location Information for Commercial Purposes." Held by the House Energy and Commerce Committee's Subcommittee on Commerce, Trade, and Consumer Protection and Subcommittee on Communications, Technology, and the Internet, the hearing featured testimony from business, consumer, and academic representatives on how Congress can best address the privacy risks raised by the increasingly ubiquitous availability of highly accurate, individualized location information.

The widespread consumer adoption of increasingly high-powered mobile devices has already spawned the Internet's next generation of location-based services and applications. As the accuracy of location data has improved and the expense of calculating and obtaining it has declined, location has become an increasingly common part of the online experience, and location-based services are an increasingly important market for U.S. companies.

Weak privacy protections put users at risk in two important ways. First, data collected about users may be retained long after the moment of data collection, and may be shared, sold, or put to unpredictable uses far in the future. The second type of risk derives from services that share consumer location with acquaintances or with the public at large. While these technologies offer exciting new opportunities for Internet users, products built with defaults that do not protect privacy may place the uninformed user in dangerous situations.

Ensuring that location information is subject to neither commercial nor government misuse – but is instead transmitted and accessed in a privacy-protective way – is essential to the long-term success of location-based applications and services. Beyond the risks to individuals' privacy, the present lack of privacy protection also creates market risks for the very companies seeking to capitalize on location services.

In CDT's testimony, we spelled out two specific measures needed to protect the privacy of location information that would benefit from Congressional action:

- First, the disclosure of precise location information in a commercial context must only be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose location only to trusted parties. As Congress contemplates enacting baseline consumer privacy legislation, such a requirement should be part of a broader framework governing sensitive user data.
- Second, the standards for government access to location information must be amended to make clear that a probable cause warrant is required for the government to obtain location information.

[Testimony of John Morris](#) [1] (February 2010)

"[The Collection and Use of Location Information for Commercial Purposes](#) [2]" - Hearing information and testimonies

CDT Policy Post, [The Dawn of the Location-Enabled Web](#) [3] (July 2009)

[The founders of Pleaserobme.com on location awareness](#) [4] (February 2010)

2) Location Information is Poorly Protected in the Commercial Context

In the past, telecommunications carriers served as gatekeepers of location information – data about a cell phone user’s location was primarily calculated within a carrier’s network using the signals sent by the phone to the carrier’s service antennas. Laws to protect users’ location information were accordingly focused on the role of the carrier and offered a baseline of protection for how the carrier could share and use that information.

But today the location of mobile devices can be determined through a range of technologies. Some of these technologies require the participation of an underlying wireless carrier, while others (such as WiFi positioning) work without the involvement or even knowledge of a telecommunications company – many smart phones can take advantage of both types of location determination technologies.

Consider the example of Yelp, a service used to find and rate businesses located near the user (allowing someone to find out “how good is that dry cleaner that I drive by every day?”). A consumer who uses the Yelp application on the location-enabled Apple iPod Touch provides her location information to Yelp entirely independently from any cell carrier – the iPod Touch is not a cellular device, and only has WiFi connectivity.

The amount of location data that is sent independently from any cellular carrier is very significant and rapidly growing. As of July 2009, 3300 location-based applications were offered through application stores for mobile devices. And in May 2009, Skyhook Wireless, the company that provides WiFi positioning for Apple products, AOL, and others, was receiving 250 million location requests every day.

The number of possible uses for location data is also ever-growing and the number of companies handling location information is continuously expanding as well: Web sites, application developers, location providers like Google and Skyhook Wireless, handset vendors, operating system vendors, advertisers, advertising networks, and analytics companies may also have access to precise, sensitive information about where users are located.

It is clear that the existing statutes, which extend protections only to certain types of location information held by telecommunications carriers, are woefully outdated and insufficient.

[Location Technologies Primer at TechCrunch](#) [5] (June 4, 2008)

3) Statutory Protection of Location Information is Woefully Outdated

Technology has bypassed statutes intended to protect location privacy in the commercial context. Foremost among these statutes are the Consumer Proprietary Network Information (CPNI) rules, protecting “customer proprietary network information,” including location.

Starting with the Telecommunications Act of 1996 and continuing with subsequent amendments, Congress has prohibited a telecommunications carrier from disclosing 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.” With this minimal standard, Congress prohibited carriers from releasing location information on a solely

discretionary basis.

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

- First, the CPNI rules do not apply to the most innovative and burgeoning types of location technologies, applications, and services. The CPNI rules do not cover any of the technologies that determine location independent of carriers. The WiFi-only iPod Touch example described above starkly illustrates the limits of the CPNI rules, but even when an iPhone or Android user installs a location-based application, the location data transmitted by the resulting service is largely invisible to the telecommunications carrier over which the service is provided. The CPNI rules simply do not reach the location transaction.
- Second, 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. 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.

Even the Electronic Communications Privacy Act (ECPA), which may offer some privacy protections through its coverage of location-based services who receive location data from a user, process it, and deliver value-added results to the user, may be rendered unresponsive to user privacy concerns by a caveat in the law and uncertainty about its scope. At the very least, consumers are left with the kind of ambiguity that provides little foundation for user confidence.

In other words, under the current regulatory scheme, once sensitive location information falls into the hands of any one of these non-carrier companies, it lives outside of any regulatory authority other than the FTC's general and tough-to-enforce Section 5 (unfairness and deception) jurisdiction.

[Statement of Commissioner Copps](#) [6], Wireless Broadband Order (March 2007)

[Digital search and seizure report](#) [7]

4) Existing Legal Standards for Access to and Protection of Location Information Are Woefully Inadequate

Users want and demand a level of privacy around their location with respect to commercial entities – but they also seek locational privacy vis-à-vis the government.

A lack of clear rules about law enforcement access to location information held by service providers has left location technology without sound legal footing. 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. 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. Finally, the Electronic Communications Privacy Act (ECPA), while it sets a 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 used to generate the location information.

Uncertainty about the privacy afforded to location information could restrain consumer adoption of location-based services. Internet users deserve clarity and simplicity in the law governing law enforcement access to location information.

[CDT blog post on the privacy battle over law enforcement access to cell phone tracking data](#) [8]
(February 2010)

-
- [location privacy](#)
- [location](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://www.cdt.org/policy/cdt-testifies-location-privacy>

Links:

[1] <http://www.cdt.org/files/pdfs/CDT-MorrisLocationTestimony.pdf>

[2] http://energycommerce.house.gov/index.php?option=com_content&view=article&id=1906:the-collection-and-use-of-location-information-for-commercial-purposes&catid=129:subcommittee-on-commerce-trade-and-consumer-protection&Itemid=70

[3] <http://www.cdt.org/policy/dawn-location-enabled-web>

[4] <http://www.cdt.org/blogs/cdt/over-sharing-and-location-awareness>

[5] <http://techcrunch.com/2008/06/04/location-technologies-primer/>

[6] http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-30A3.pdf

[7] <http://www.cdt.org/publications/digital-search-and-seizure.pdf>

[8] <http://www.cdt.org/blogs/brock-meeks/privacy-battle-over-cell-phone-tracking-data-hits-appeals-court>