

The Location-Enabled Web Debate Hits Capitol Hill

February 24, 2010

CDT's John Morris [testified this morning](#) [1] 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. Joining John as witnesses were Professor Lorrie Cranor of Carnegie Mellon University, Michael Altschul of CTIA – The Wireless Association, Jerry King of location-based application provider uLocate, Terry Bernard of the location aggregator Useful Networks, and Ann Collier of the advocacy group ConnectSafely.org.

Location privacy is a timely issue here at the dawn of the [location-enabled Web](#) [2]: 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.

The hearing started out with a bang when Chairman Bobby Rush (Subcommittee on Commerce, Trade, and Consumer Protection) emphatically stated that "with the information learned from today's hearing we will have now learned enough to take the next step...it is my intent that the next hearing [on this topic] be a legislative hearing." Mr. Rush promised that we will be seeing a draft of a "comprehensive privacy bill" soon.

The Congressman's choice of the term "comprehensive" caught people's attention and in a later exchange with CDT's John Morris, Chairman Rick Boucher (Subcommittee on Communications, Technology, and the Internet) elaborated on Mr. Rush's opening remarks. Mr. Boucher asked witnesses whether the time has come for Congress to pass a statute that governs the privacy rights associated with presently un-protected types of location-based information. John answered with a resounding "yes" but added a qualification. "We would hope," he said, "[these protections] would be in the context of a larger privacy bill instead of a sectoral bill focused solely on location." To which the congressman responded, "I couldn't have provided a better answer myself. I expect you will see this issue emerge as part of a larger legislative item."

Although the other witnesses were split in their responses to Mr. Boucher's question (Professor Cranor, Mr. King and Ms. Coulier felt there should be general privacy or location privacy legislation, while Mr. Altschul and Mr. Bernard disagreed), one general consensus did seem to emerge out of the hearing. In both the opening statements from the representatives and the commentary provided by the witnesses, there was agreement that the current regulatory environment surrounding the use of location-based information is woefully outdated.

As CDT wrote in [testimony](#) [3] submitted ahead of the hearing:

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 work without the involvement or even knowledge of a telecommunications company ... many smart phones can take advantage of [both] types of location determination technologies.

...From the user perspective, the number of possible uses for location data is 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.

And 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.

The witnesses may have differed in their recommendations for bringing the laws governing location privacy into the 21st century, but the hearing demonstrated that some progress has been made in this space. After all, as the saying goes, the first step is recognizing you have a problem.

- [privacy](#)
- [locpriv](#)
- [privacy](#)
- [social media](#)
-
- [testimony](#)
- [location-enabled web](#)
- [hearing](#)
- [Congress](#)
- [capitol hill](#)
- [data](#)
- [geolocation](#)
- [geopriv](#)
- [applications](#)

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://cdt.org/blogs/erica-newland/location-enabled-web-debate-hits-capitol-hill>

Links:

[1] 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

[2] <http://www.cdt.org/policy/dawn-location-enabled-web-0>

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