

## Should all sensitive data be treated the same?

February 26, 2010

There was a discussion over on [ReadWriteWeb](#) [1] yesterday about whether location information should be given the same privacy protections as medical data. The blog post made reference to the [recent testimony](#) [2] of CDT General Counsel John Morris on location privacy but challenged his assertion that “[protecting location information] will require location be treated as sensitive data, like medical data. You'll need to do more than just post a disclosure statement.”

While we are happy to see a spirited debate about the privacy concerns raised by location information, it is important to keep in mind that treating both location information and medical information “as sensitive data” does not translate into a prescription for the exact same protections for these two very different data types. Location information is sensitive but it is sensitive in different ways than medical data; location information deserves special protections, but different protections than medical data does.

The ubiquity of location information presents three classes of privacy risk to users: company misuse or abuse of data, government misuse or abuse of data, and unintentional over-sharing by the user. Categorizing location information under the umbrella of sensitive data places appropriate emphasis on the risks inherent in creating and storing records of visits to courts, political rallies, union meetings, and medical clinics. Under current legal standards, for example, location information is often treated as transactional data, like email “to/from” information, and it is unclear [what protections it is afforded](#) [3] when law enforcement comes a-knocking. While standards have been articulated for law enforcement access to a few categories of sensitive information, like medical data (though these standards remain insufficient), there are not similarly clear standards for access to location data.

Moreover, claims that location sharing is opt-in only are often misleading at best and deceptive at worst. Users may opt in to sharing their location for the purpose of finding the nearest drycleaner, but they are hardly opting in to the sharing of their information with location providers, the application’s business partners, advertisers, and the police. And giving notice of all this widespread sharing of location information in paragraph 27 of a privacy policy is wholly inadequate. Meanwhile, many photo sharing and social networking applications fail to offer a real opt in to location sharing: the location of the person posting is often made public by default.

But no matter how we classify location information, as John said in his testimony, what the American public really needs is comprehensive privacy legislation that provides a baseline of protection for all personal information and extra protection for sensitive information: “We would hope,” John said at the hearing, “[protections for location information] would be in the context of a larger privacy bill instead of a sectoral bill focused solely on location.”

- [readwriteweb](#)
- [testimony](#)
- 
- [privacy](#)
- [privacy](#)
- [location-enabled web](#)
- [locational data](#)
- [commercial data](#)



## Should all sensitive data be treated the same?

Published on Center for Democracy & Technology (<https://cdt.org>)

---

as you make no substantive changes and clearly give us credit. [Details](#).

**Source URL:** <https://cdt.org/blogs/erica-newland/should-all-sensitive-data-be-treated-same>

### Links:

[1] <http://www.nytimes.com/external/readwriteweb/2010/02/25/25readwriteweb-location-data-sensitive-like-medical-inform-75294.html>

[2] <http://www.cdt.org/blogs/erica-newland/location-enabled-web-debate-hits-capitol-hill>

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