

The Dawn of the Location-Enabled Web

by [Alissa Cooper](#) [1]
June 19, 2009

There's been a lot of buzz over the last few days about the new [iPhone 3.0 software](#) [2] that was released this week. You might have seen reviews of a [new service offered as part of the update called Find my iPhone](#) [3], which shows you your iPhone's location on an online map should you misplace it. But while Find my iPhone may be getting all of the location buzz, the new iPhone software includes another feature which, I think, will ultimately prove to be much more significant for location - and for location privacy. With the release of the new software, the latest version of the Safari web browser running on the iPhone will be location-enabled. This means that any Web site can ask Safari for the user's location, and Safari can provide it by using the location positioning technologies built into the phone (including GPS, among others). Apple has implemented a simple interface (based on a draft of a [W3C standard](#) [4] that Web sites can use to request location.

Location-savvy users will realize that Safari isn't the first browser to make the location-enabled leap. Google has been providing this capability in Google Chrome, the Android browser and Google Gears for months; the current beta version of Firefox is location-enabled; and Opera has released a location-enabled version of its browser. Even before the browsers jumped into the game, Web sites have for years been using reverse-IP address lookups to obtain the approximate locations (think city-level precision) of Web users. But with 40 million iPhone users, Apple's foray into geolocation marks the true beginning of an era when pinpointing many Internet users on a map - with the precision of a few meters, not a few miles - goes from complicated and onerous to simple and fast. This won't work for all users, but 40 million is a pretty significant start. What does this mean for privacy, you ask?

It's CDT's belief that location information should only be used on individual Internet users' own terms. Individuals should get to decide with whom they share their location, what that information is used for, whether or not it gets shared, and how long it's retained. Location-enabled technologies - including Web browsers - should be designed with privacy in mind from the beginning and with built-in user controls to allow individuals to manage their location data as it's collected. CDT has been working for years to incorporate some of these concepts into technical standards, [originally in the IETF's Geopriv working group](#) [5] and more recently within the [W3C Geolocation working group](#) [6], which created the draft standard that Apple, Google, Mozilla and Opera are all using. Unfortunately, we've met a lot of resistance at the W3C (more on that in a subsequent post), and we see a lot of room for improvement with the companies' initial efforts at providing user control. Take the iPhone Safari implementation, for example. In some ways, it's highly protective of users. Each Web site that wants to use your location has to first get your permission not once, but twice. And those permissions are reset every 24 hours. As far as consent goes, this is a really strong baseline. But in terms of providing more granular control and transparency, the iPhone is lacking.

There's no way to see which sites (or applications, for that matter) you've shared your location with. If you visit a site and decline to provide your location to it, the site may prompt you to provide your location on every visit. Wouldn't it be nice to have a whitelist of sites that you trust to have your location, or a blacklist of sites you don't trust? (Incidentally, the IETF's Geopriv work has a built-in whitelisting capability.) That way, you could avoid the 24-hour permission renewal described above when you want to, and you wouldn't be badgered into consenting by accident when you don't want to. This kind of granularity would also help with permission revocation. Right now, to revoke even a single site's permission, your only choice is to revoke all sites' permissions. Even accomplishing that is, in my opinion, a counterintuitive process: you need to go into your general settings, find the tab marked "Reset" (sort of a scary name), and select "Reset Location Warnings." Granted, the 24-hour permission relapse means that, today, there probably won't be many sites to revoke permissions from. But if the permission model ever changes, the revocation model needs to change too. Some of the other browsers' controls are more granular, but as a group they have a long way to go. Of course, the argument on the other side is that mobile devices have limited screen space and

functionality, which makes creating meaningful transparency and controls difficult. If the iPhone doesn't offer granular controls for cookies (which it doesn't), then why should it offer granular controls over location? What's missing in this calculus is recognition of the potential sensitivity of location information.

A mobile phone can reveal the fact that a person was at a particular medical clinic at a particular time, for example. The ubiquity of location information may also increase the risks of stalking and domestic violence if perpetrators are able to use (or abuse) location-based services to gain access to location information about their victims. Location information can also be highly identifiable, even when it isn't directly associated with other personal information. In my household, there's only one person who spends her daytime hours at CDT and her nighttime hours in my apartment. After a day or two of collecting just those two data points from my phone, it would become pretty obvious whom those data points describe. Furthermore, location information is and will continue to be of particular interest to governments and law enforcers around the world.

In the U.S., standards for government access to location information held by companies are unclear at best and far too low at worst (see our [Digital Search & Seizure report](#) [7] for more detail). The laws that dictate what government agents must do to obtain location data simply have not kept pace with technological evolution. So given the privacy interests at stake and the relative lack of protection in the law, we would expect location controls to be better than other kinds of technological controls on the Web, to offer users more choices about what happens to their data and to be especially transparent about when location data is being passed around. It doesn't appear that every one of our expectations will be met here at the dawn of the location-enabled Web. But as location comes to pervade the Web experience - which it will, given the simple interface offered by the browser vendors and myriad uses of location information - we'll be taking a closer look at how current user controls work, how they could be improved, and how standards, policy, and law can contribute to protecting location privacy on the Web.

- [safari](#)
- [software](#)
- [upgrade](#)
-
- [privacy](#)
- [location-based](#)
- [browser](#)
- [CDT](#)
- [iphone](#)
- [Apple](#)

Copyright © 2013 by the 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/alissa-cooper/dawn-location-enabled-web>

Links:

- [1] <https://cdt.org/personnel/alissa-cooper>
- [2] <http://www.apple.com/iphone/softwareupdate/>
- [3] <http://www.apple.com/mobileme/whats-new/>
- [4] <http://dev.w3.org/geo/api/spec-source.html>
- [5] <http://cdt.org/publications/20070100ieee.pdf>
- [6] <http://www.w3.org/2008/geolocation/>
- [7] <http://www.cdt.org/publications/digital-search-and-seizure.pdf>