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 **John B. Morris, Jr.**
General Counsel, and Director of CDT's Internet Standards,
Technology & Policy Project
Center for Democracy & Technology

before the House Committee on Energy and Commerce,
Subcommittee on Commerce, Trade, and Consumer Protection and
Subcommittee on Communications, Technology, and the Internet

THE PRIVACY IMPLICATIONS OF COMMERCIAL LOCATION-BASED SERVICES

February 24, 2010

Chairman Rush, Chairman Boucher, and Members of the Subcommittees:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Subcommittees' leadership and foresight in examining the burgeoning area of commercial location-based services, and we appreciate the opportunity to address the privacy implications of what is one of the fastest growing areas of online innovation. As a note of introduction, I am an attorney and serve as CDT's General Counsel, but I also have a technical background, and I direct CDT's Internet Standards, Technology & Policy Project. This Project seeks to address the fact that the work of technical standards bodies such as the Internet Engineering Task Force (IETF) often has important impact on civil liberties and other policy concerns. In particular, I have been involved for the past nine years with the IETF's efforts to address and protect the privacy of location information, and I am a co-author of four IETF standards documents addressing location privacy.[1]

The Promise and Risks of Location-Aware Technologies

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.

---

[1] RFC 3693, "Geopriv Requirements" (with J. Cuellar, D. Mulligan, J. Peterson, J. Polk) (Internet Engineering Task Force 2004) (defining requirements for technical protocol to protect privacy of location information transmitted over the Internet); RFC 3694, "Threat Analysis of the Geopriv Protocol" (with M. Danley, D. Mulligan, J. Peterson) (Internet Engineering Task Force 2004) (analyzing risks and threats to privacy of location information on the Internet); RFC 4745, "Common Policy: A Document Format for Expressing Privacy Preferences" (with H. Schulzrinne, H. Tschofenig, J. Cuellar, J. Polk, J. Rosenberg) (Internet Engineering Task Force 2007) (defining protocol format for expression of privacy preferences concerning location information); RFC 5606, "Implications of 'retransmission-allowed' for SIP Location Conveyance" (with J. Peterson, T. Hardie) (Internet Engineering Task Force 2009).

The availability of location information paves the way for exciting new applications, ranging from uses that support essential services to those that address less weighty needs. For example, firefighters in Washington, D.C., use a customized version of Google Earth that displays the real-time location of fire trucks in the city. In its first year of use, this software has reportedly saved the city $3 million.[2] At the same time, millions of users rely on location technology to guide them to the closest coffee shop or to help them navigate through unfamiliar neighborhoods.

But the easy availability of location information also raises several different kinds of privacy concerns. The idea of "Big Brother" always watching the citizenry has long been a concern for many in this country. Ubiquitous availability of individualized location information on a mass scale is ripe for abuse. Location services can reveal very private information and even put users at physical risk. 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.

Location data comes in a variety of forms and these forms vary in sensitivity. Web analytics programs, which analyze a Web site's traffic, have long leveraged the fact that IP addresses can be roughly correlated to metropolitan areas to calculate the approximate locations from which Web site visitors access individual sites. But as technology has developed, it has become possible to determine the near-exact location of most mobile device users. While this capability has existed for some years within cellular networks, it is only recently that the explosion of location-based technologies and applications has begun, with every new device locatable in multiple ways and an ocean of applications developers incorporating location-based features into their products. With the popularity of iPhones, Blackberries, and the myriad other smartphones on the market, hundreds of millions of users are all now easily locatable, as are many users of laptops, as Mozilla's Firefox – the second-most popular Web browser[3] – has also recently become location-enabled.[4]

The collection and use of fixed device location (such as home or business addresses) has obvious privacy implications. However, especially troubling privacy concerns arise from the collection of "mobile location data," which identifies the whereabouts of an individual or his or her device in real or near-real time.[5] In this testimony, we focus on the risks raised by the increasing collection and use of mobile location data.

---

[2] *See* CNBC, *CNBC Original: Inside the Mind of Google* (Dec. 3, 2009), http://www.cnbc.com/id/33831099/.

[3] As of January 2010, Firefox had over 250 million users. *See* Erick Schonfeld, *Where Did Internet Explorer's Browser Share Go?,* TechCrunch.com (Feb. 2, 2010), http://techcrunch.com/2010/02/02/internet-explorer-browser-share/.

[4] *See Location-Aware Browsing,* http://www.mozilla.com/en-US/firefox/geolocation/ (last visited Feb. 21, 2010); *Mozilla Advances the Web with Firefox 3.5* (June 30, 2009), http://www.mozilla.com/en-US/press/mozilla-2009-06-30.html.

[5] In 2009, CDT worked with companies and other advocacy organizations in our Internet Privacy Working Group (IPWG) to establish a workable and specific vocabulary to describe how data is stored and used online. This definition for "mobile location data" originates in the set of definitions that was released through that collaboration. *See* Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), http://www.cdt.org/privacy/20090128threshold.pdf.

Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may describe both what a person is doing and where he or she is doing it. It can reveal visits to potentially sensitive destinations, like medical clinics, courts, political rallies, and union meetings. The ubiquity of location information has also increased the risks of stalking and domestic violence as perpetrators are able to use (or abuse) location-based services to gain access to location information about their victims.[6] And, as an increasing number of minors carry location-capable cell phones and devices, location privacy will become a child safety matter as well.

Beyond the risks to individuals' privacy, the lack of privacy protection also creates market risks for the very companies seeking to capitalize on location services. As my fellow witness, Professor Lorrie Cranor, can explain in far greater detail, research shows that people value their location privacy, are less comfortable sharing their location with strangers than with acquaintances, and want granular control over their location information.[7] At the end of the day, location-based services stand to be more successful if there is a framework of privacy giving users confidence that their information will be protected.

The sensitivity of location information clearly puts it at high risk for misuse by companies and governments alike. As location information begins to pervade the Web experience, standards, policy, and law must develop in ways that contribute to the protection of location privacy. CDT believes that Congress can help to protect location privacy in two ways:

- 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.

- The standards for government and law enforcement access to location information must be amended to make clear that a probable cause warrant is required for the government to obtain location information.

---

[6] *See, e.g.,* "Tracing a Stalker," Dateline NBC (June 16, 2007), http://www.msnbc.msn.com/id/19253352/; "Albert Belle pleads guilty to stalking ex-girlfriend," Associated Press (July 26, 2006), http://sports.espn.go.com/mlb/news/story?id= 2530911&campaign=rss&source=ESPNHeadlines.

[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.

Understanding Location-Aware Technologies

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. Although there are a number of variations, the most significant location determination technologies can be grouped into the following six categories[8]:

Carrier-controlled or -involved location technologies:

1. Cell tower-based calculations: Among the oldest forms of mobile location determination are calculations based on the location of cell towers and the signals received by the carrier at one or more towers. In its simplest form, if two or three cell towers can detect a mobile device at the same time, the carrier can triangulate from the towers to determine the approximate location of the phone. Carriers can, if needed, make calculations based on the strength and direction of a phone's signal as received at a single tower. This type of location determination does not require special hardware or computing power in the handset. The precision of this technique is relatively low, on the order of hundreds or thousands of meters, and is dependent upon the density of cell towers in the vicinity of the handset.

2. GPS: By receiving signals from the Global Positioning System (GPS) satellites, a handset can determine its own location, and can transmit it to the carrier. GPS produces higher precision locations (on the order of meters or tens of meters). In the context of emergency calls, mobile handsets in the U.S. are designed to transmit GPS information (if it is available) whenever a 911 call is placed (and handsets can be configured to transmit GPS data to the carrier when other telephone calls are placed). In this context, one part of the handset (the cellular voice circuitry) requests the location from the GPS chip in the handset, and passes the location on to the cellular carriers. One drawback of GPS-based positioning is that it can take 30 seconds or more (sometimes much more) for the GPS chip to make an initial location determination.

3. A-GPS: To address the potential slowness of GPS positioning, "Assisted-GPS" technology was developed, combining both of the above two location technologies. Using a number of methods, GPS data is combined with cell-tower based information to significantly speed up the initial location determination while taking advantage of the higher precision of GPS.

Location technologies independent of carriers:

4. WiFi database lookup: The location of WiFi-capable devices (including nearly all laptops and smartphones) can be determined using a database to identify WiFi access points in the vicinity of the particular device. Both Google and Skyhook have developed databases of WiFi access points and their

[8] For a more detailed explanation of the various leading location determination technologies, see "Location Technologies Primer," TechCrunch (June 4, 2008), http://techcrunch.com/2008/06/04/location-technologies-primer/.

locations. When an application (such as Web browser or location-aware application) needs the location of the device, it sends a query to (for example) a Google database, and Google returns the location based on nearby WiFi access points. This lookup process takes place without the involvement or even knowledge of any cellular carrier used by the device (and indeed, by using this approach, devices that have *no* cellular capabilities can be located).

5. Cell tower database lookup: This approach is similar to a WiFi database lookup, except that the lookup is to a database of cellular tower locations. As with its WiFi access point database, Google has amassed a database of the locations of cell towers. When a device is accessing the Internet over a cellular data network, it can send a query to Google containing the cell tower ID that the device is connected to, and Google is able to return an approximate location. As with WiFi database lookups, this approach does *not* need the involvement of any carrier, even though locations are determined based on the locations of the carrier's cell towers.[9]

6. GPS: Finally, applications (including Web browsers such as Firefox and Apple's Safari) running on a mobile device can receive location information directly from a GPS chip in the device, *without* any involvement or knowledge of a carrier. The GPS information can in turn be sent to anyone on the Internet through the mobile data connection. And, because mobile Web browsers can connect to any Web site on the Internet, *any* Web page can include code that requests the user's location from the device.

Many smart phones can take advantage of all six of these location determination technologies,[10] and most new wireless devices – including cell phones, smart phones, e-book readers, laptops, netbooks, and even the new iPad – have at least one of these capabilities (and usually two or more). Moreover, as GPS and WiFi capabilities have been built into an increasing number of these devices, location information has become increasingly accurate.[11]

---

[9] For a discussion of how Google is able to automatically determine the location of cell towers, see "Google enables Location-aware Applications for 3rd Party Developers" (June 6, 2008), http://googlemobile.blogspot.com/2008/06/google-enables-location-aware.html.

[10] It is important to note that these six arrangements describe only how a device location can be determined, not how that location is used or later transmitted. The carrier-independent technologies result in the device knowing its own location. That location may then be used locally by applications on the device (such as Web browsers of mobile apps) or sent to a Web site or remote server. In the latter case, for handsets connected to a cellular network, the location may be transmitted as content over a cellular data connection. But this does not mean that the carrier is involved in locating the device, or that the carrier is even aware that the content contains the device's location. The positioning of the device and the transmission of its location to effectuate a particular application or service on the device can be entirely separate processes.

[11] One small study of the accuracy of these location-determining technologies on the 3G iPhone (the first mobile device to successfully integrate all of the primary location technologies) found that cellular network positioning yielded a median error of 600 meters, WiFi positioning yielded a median error of 74 meters, and GPS yielded a median error of 8 meters. *See* Paul A Zandbergen, *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi, and Cellular Positioning,* Transactions in GIS, Volume 13, Issue s1 (July 2009), http://gisandscience.com/2009/07/15/accuracy-of-iphone-locations-a-comparison-of-assisted-gps-wifi-and-cellular-positioning/.

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 (as described as "cell tower-based calculations" above). As discussed more fully below, 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 location information is now collected by a much broader spectrum of companies.

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?").[12] 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.[13]

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.[14] 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*.[15]

Moreover, the range of companies that potentially have access to location data is not limited to telecommunications carriers, location providers like Skyhook Wireless, application developers, or Web sites. 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: handset vendors, operating system vendors, advertisers, advertising networks, and analytics companies may also have access to precise, sensitive information about where users are located.

Existing Legal Standards For Access to and Protection of Location Information Are Woefully Inadequate

Although Congress has in the past sought to protect electronic communications, including location information, the technology has far outpaced the statutory protections, both regarding use of location in the commercial context, as well as protection of location from unwarranted government access. Clear privacy rules for location are a pre-requisite to the growth and success of new location-based services.

Although the focus of this hearing is on *commercial* use of location information, it is important to look at the inadequacy of legal protection in both the commercial and governmental contexts. 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

---

[12] *See* Yelp, Inc. *Yelp: Version 4.0.0* (iPhone application), http://itunes.apple.com/us/app/yelp/id284910350?mt=8 (last visited Feb. 21, 2010).

[13] *See iPod Touch: Features*, http://www.apple.com/ipodtouch/features/ (last visited Feb. 21, 2010).

[14] *See* Skyhook Wireless, *Location Aware App Report: From the Apple, Blackberry, Android, Nokia and Palm App Stores* (July 2009), http://www.locationrevolution.com/stats/skyhookjulyreport.pdf.

[15] *See* Jenna Wortham, *Cellphone Locator System Needs No Satellite,* New York Times (May 31, 2009), http://www.nytimes.com/2009/06/01/technology/start-ups/01locate.html.

government. Thus, to promote and facilitate innovation and market acceptance of location-based services in the *commercial* context, it is important that Congress also act to protect location information in the law enforcement investigative context as well. Thus, before discussing the legal standards governing commercial use of location, we briefly address the inadequacies in the government context.

The Electronic Communications Privacy Act Should be Updated to Protect Location Information from Inappropriate Disclosure to 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.* 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] Finally, the Electronic Communications Privacy Act (ECPA),[19] 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. 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] But a plurality of courts have required a higher level of proof – probable cause – for law enforcement access to this prospective location information.[22] Just this month, the federal court of appeals in Philadelphia heard oral argument on the question of what

---

[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.*

[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).

standard should apply to stored location data, the first but probably not the last case to present that issue at the appellate level.[23]

Uncertainty about the privacy afforded to location information could restrain consumer adoption of location-based services. 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 the Digital Privacy and Surveillance Working Group – has convened technology and communications companies, privacy advocates and academics in an effort to arrive at consensus proposals to update ECPA. We plan to unveil those proposals in the coming weeks, including one that, if adopted, would bring clarity and simplicity to the law governing law enforcement access to location information.

Statutory Protection of Location Information in the Commercial Context is Also Inadequate

Just as technology has bypassed ECPA and other statutes on government access to information, technology has also bypassed statutes intended to protect location privacy in the commercial context. Foremost among these statutes are the CPNI rules, protecting "customer proprietary network information," including location. Although the CPNI rules continue to provide important protections, they are less and less relevant, and taken together, they and other laws do not provide sufficient protection for location information.

CPNI Rules

Starting with the Telecommunications Act of 1996, 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."[24] 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 simply 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 "location technologies independent of carriers" described above as technologies 4 through 6, because there is no telecommunications carrier involved in the location determination or location-based service. The WiFi-only iPod Touch example described above starkly

[23] *See* Brock Meeks, "Privacy Battle Over Cell Phone Tracking Data Hits Appeals Court," Center for Democracy & Technology (Feb. 12. 2010), http://www.cdt.org/blogs/brock-meeks/privacy-battle-over-cell-phone-tracking-data-hits-appeals-court.

[24] 47 U.S.C. § 222.

illustrates the limits of the CPNI rules, but even when location data is transmitted over a cellular network, the carrier is increasingly not directly involved in the location transaction. 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. When the Commission issued its Wireless Broadband Order,[25] Commissioner Copps explained the effect of the Order on the protection of location information under the CPNI rules:

  > [C]onsider a cutting-edge device like Apple's much-anticipated iPhone, which allows a user to communicate via IP-based Wi-Fi technology as well as traditional CMRS [Commercial Mobile Radio Service] service. Under our precedent, a consumer who uses the CMRS features of the device to place a phone call can be secure in the knowledge that our Title II CPNI rules require the carrier to protect his or her call and location information. But what about when that very same consumer uses that very same device just moments later to send an email via Wi-Fi, to call up a map of his or her location via a browser, or even to place a VoIP call to another Internet user? Because *those* services—which the customer can be excused for thinking of as functionally identical to the CMRS call—are now classified as Title I information services, the carrier appears to be entirely free, under our present rules, to sell off aspects of the customer's call or location information to the highest bidder.[26]

  In light of the Wireless Broadband Order, as Commissioner Copps explained, it appears quite possible that even carrier-provided location based services that run over the wireless *data* network are not protected by the CPNI rules. Although Congress and then the FCC did extend CPNI rules to cover IP-enabled "interconnected" VoIP services,[27] 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.

When first enacted almost 15 years ago, the CPNI rules were groundbreaking, and provided important protections for the primary wireless service used by Americans at

---

[25] *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*, Declaratory Ruling, WT Docket No. 07-53, FCC 07-30, 2, ¶ 2 (rel. Mar. 23, 2007), http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-30A1.pdf ("Wireless Broadband Order").

[26] Statement of Commissioner Copps, Wireless Broadband Order, at 1, http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-30A3.pdf.

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

that time – voice. Now that our society is moving away from voice and to data, and our online interactions provide a far more robust window into our personal lives, the protections offered by the CPNI rules have been left behind.

Federal Trade Commission Act and State Attorneys General

Under its authorizing statute,[28] the Federal Trade Commission is empowered to challenge unfair and deceptive trade practices. Under this broad authority, the FTC has established some general precedents about what constitutes a deceptive or unfair privacy practice online – deviating from a stated privacy policy or failing to secure personal information are two examples. More specific authority has also been granted to the agency to deal with particular privacy issues, including spam, credit reporting, financial privacy, children's privacy, and telemarketing.

The FTC has a strong track record of pursuing bad actors engaged in egregiously deceptive or unfair practices – the agency's efforts in the spyware area provide good examples. However, the FTC has been hesitant to use its unfairness jurisdiction to address questionable privacy practices, and it lacks several important tools – including rulemaking authority and civil penalty authority – that are necessary for the agency to successfully protect consumers from privacy threats, including those related to location privacy. 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 do not live up to their privacy policies or that engage in other unfair or deceptive trade practices. To date, however, little attention has been paid at the state level to location privacy concerns.

ECPA

ECPA covers entities providing "remote computing services," defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." This definition may cover providers of location-based services, who receive location data from a user, process it, and deliver value-added results to the user. In the absence of consent, remote computing services are prohibited from divulging the contents of communications they receive, but only if the communications are maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computing processing." That caveat, uncertainty about the scope of the definition of "remote computing service," and the ease with which subscriber consent can be obtained as part of terms of service, render ECPA unresponsive to user privacy concerns or, at the very least, leave consumers with the kind of ambiguity that provides little foundation for user confidence.

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

The Privacy Practices of Companies Collecting Location are Uneven at Best and Inadequate at Worst

In the face of inadequate statutory protection for location information, it is perhaps not surprising that the privacy practices of companies collecting location, and the granularity of controls they offer, range widely in terms of the level of protection that they provide. CTIA–The Wireless Association has, commendably, issued best practices to govern the provision of location-based services,[29] and CTIA has indicated that it is committed to maintaining its guidelines as technology evolves. However, the primary adherents to those self-regulatory guidelines are wireless carriers – which, as noted above, are far from alone in offering the newest location-based services, and are already bound by the CPNI rules.

Because of the sensitivity of location information, the users of location-based services deserve a robust set of protections to help manage the associated privacy risks. The list of possible protections is long: providing clear notice of when location information is being collected, offering robust user choice about when location can be collected, providing access to stored data (for example, showing maps of where the user has been), providing the ability to broadcast "fake" location, sending reminders to users that their location is being shared, applying de-identification techniques,[30] encrypting location information in transit and storage, and many others. Some providers of location-based services, such as Loopt (which provides location-based social networking) have fully integrated these kinds of protections into their products.[31] Others have included strong consent mechanisms, but failed to incorporate more comprehensive user control tools.[32] Still others have failed to incorporate even the most basic of protections – privacy policies.

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 often long after the original location service has been provided. Whether the location information is stored by location providers like Skyhook Wireless and Google, by the developers of applications downloaded to the device, by location-aware Web sites, or by advertisers and analytics companies, this data 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.

---

[29] CTIA-The Wireless Association, "Best Practices and Guidelines for Location-Based Services," http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf.

[30] For example, when Google maps began collecting traffic data from location-enabled cell phones, it took steps to delete the starting and ending points of users' journeys. *See* Tom Krazit, *Google Maps adds traffic data from your cell phone* (Aug. 25, 2009), http://news.cnet.com/8301-30684_3-10317223-265.html.

[31] *See* Loopt, *Loopt: Privacy & Security*, http://www.loopt.com/about/privacy-security (last visited Feb. 22, 2010).

[32] *See* Alissa Cooper, *The Dawn of the Location-Enabled Web*, Center for Democracy & Technology (July 6, 2009), http://www.cdt.org/policy/dawn-location-enabled-web-0.

Unfortunately, many location-based products and services have not adequately addressed these risks:

- Many companies that offer applications for mobile devices collect real-time location data from their customers but offer no assurances for how that data will be protected: often their privacy policies fail to detail how location data will be used, shared, or sold. For example, the privacy policy for Foursquare, a location-based social networking service in which users "check-in" at their present locations and share these locations with friends through Facebook and Twitter, does not specifically describe how the location information Foursquare receives will be used, shared, or protected – in fact, it does not even mention the word "location," and the policy itself is not accessible before or during the application sign-up process.[33] Many other location-based services lack privacy policies all together.[34] Privacy policies alone offer little in the way of privacy protection, but their existence represents an important – and necessary – step toward promoting accountability: without a privacy policy, it is exceptionally difficult to even begin to evaluate a company's practices vis-à-vis user privacy.

- Services that publish user locations to friends or to the world vary considerably with respect to the privacy controls they offer. Two different products offered by Google illustrate this variation well. Google Latitude, released in February 2009, is a location-aware application that allows a user's cell phone location to be overlaid on Google Maps and shared with friends. Latitude was designed with privacy in mind. A user's location information is shared on an opt-in basis and only with friends the user has designated, location logs are by default deleted, and users who have enabled location-sharing receive periodic emails reminding them that the service is turned on.[35] In contrast, Google's Buzz for Mobile, released just a few weeks ago (one year after Latitude), has proven to be a privacy disaster. Buzz serves as a Gmail-integrated feed to which users can post thoughts, articles, photos, and similar updates. If the user has location services enabled on his or her mobile device, then every comment the user makes via Buzz Mobile by default includes his or her current location. If a user hasn't taken steps to make a Buzz private then the comment is tossed into the public "buzzstream," allowing anyone, anywhere in the world to track where the user is at any given time.[36] One could use Buzz to check out who is hanging out at the corner bar, attending a protest rally or visiting a particular medical facility. A new Web site, pleaserobme.com, was posted to highlight the risks inherent in making

---

[33] *See* Foursquare Labs, Inc., *Foursquare Labs, Inc. Privacy Policy* (Nov. 13, 2009), http://foursquare.com/legal/privacy.

[34] *See* Nick Doty, *Who's Using the W3C Geolocation API?* http://npdoty.name/location/services (last visited Feb. 21, 2010).

[35] *See e.g., Google Latitude, http://www.google.com/latitude/intro.html* (last visited Feb. 21, 2010); Ryan Singel, *Google Latitude to Cops: 'I Don't Remember,'* Wired (March 5, 2009), http://www.wired.com/epicenter/2009/03/googles-latitud/; Robin Wauters, *Google Warns Latitude Users That They Might Be Sharing Their Location*, TechCrunch (Feb. 18, 2010), http://techcrunch.com/2010/02/18/google-warns-latitude-users-that-they-might-be-sharing-their-location/.

[36] *See* Leslie Harris, *Buzz or Bust,* The Huffington Post (Feb. 17, 2010), http://www.huffingtonpost.com/leslie-harris/buzz-or-bust_b_466133.html.

such public announcements about location. The Web site provides a live feed of posts by Twitter and other users who have publicly announced that they are somewhere other than at home.[37]

As CDT has noted in its recent submission to the FTC on privacy, notice, choice and security comprise an incomplete framework for privacy protection. Privacy in the 21st century must be grounded in the full set of Fair Information Practice principles, including individual access, data minimization, and accountability. In the absence of this comprehensive framework,[38] many questions remain around the uses of location data and whether customers are being tracked against their will, whether location data is being protected throughout its lifecycle, and whether the entities that handle location data are giving sensitive location data the respect it deserves in terms of minimizing data collection and data uses and maximizing transparency, security,[39] and user control and consent.[40]

Given the privacy interests at stake, we would expect location controls to be better than other kinds of technological controls on the Web.[41] Unfortunately, the market has clearly not provided the protections users need for their location data.

Technical Standards Could Help Protect Location Privacy, but the Mobile Applications Industry Has Been Reluctant to Adopt Such Standards

CDT has worked since 2001 within the Internet Engineering Task Force (IETF) – the leading technical standards setting body for the Internet – on the development of a location privacy standard named "Geopriv."[42] One goal of Geopriv was to change the

---

[37] *See* Barry Borsboom, Boy van Amstel, and Frank Groeneveld, *Please Rob Me*, www.pleaserobme.com (last Visited Feb. 21, 2010).

[38] Center for Democracy & Technology, Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable (Nov. 2009), http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf

[39] Firefox has taken an important step toward protecting the security of location information. It establishes an SSL connection with its location provider, Google, in order to protect the location data being exchanged between the browser and the location provider. *See Location-Aware Browsing,* http://www.mozilla.com/en-US/firefox/geolocation/ (last visited Feb. 21, 2010).

[40] Important but often overlooked aspects of user control include: giving users the ability to obscure location or present a location other than their actual one - just as annonymization tools allow PC users to blur who or where they are, applications and devices should allow users to obscure their location; and allowing users to generate a whitelist of trusted sites that can always obtain the user's location and a blacklist of untrusted sites that cannot ever access it.

[41] Location-enabled browsers have so far offered pretty strong baselines for consent to location sharing. On the iPhone, for example, each Web site that wants to use location has to first obtain the user's permission not once, but twice. Those permissions are reset every 24 hours. However, the privacy controls offered by the iPhone still lack granularity. *See* Alissa Cooper, *The Dawn of the Location-Enabled Web*, Center for Democracy & Technology (July 6, 2009), http://www.cdt.org/policy/dawn-location-enabled-web-0.

[42] *See* Geopriv Working Group Charter, http://www.ietf.org/html.charters/geoprivcharter.html. For more information about this standard, see John Morris and Jon Peterson, "Who's Watching You Now?," IEEE Security and Privacy Magazine, Vol. 5, Issue 1 (January/February 2007), http://www.cdt.org/publications/20070100ieee.pdf; Alissa Cooper and John Morris, "Binding Privacy Rules to Location on the Web," Proceedings of the 2nd International Workshop on Location and the Web, LOCWEB '09 (Boston, Mass., Apr. 04, 2009), http://www.cdt.org/privacy/LocWebFinal.pdf.

historic reliance on privacy policies set by service providers, and to allow users to specify the rules that would govern use and retention of location information about them.

Unfortunately, in a 2008 effort spearheaded by the leading browser vendors (including Opera, Mozilla, and Apple), a different standards body rejected the IETF approach and instead opted to continue to leave it up to individual service providers to issue privacy policies governing location. This other body, the World Wide Web Consortium (W3C), has far more influence over "applications layer" services (including most location services) than does the IETF. When W3C declined to follow the standards set by the IETF, it instead developed its own location standard that urges developers to respect privacy, but includes no technical steps that would help force developers to do so.[43] The W3C process is on going, and CDT is working to improve the W3C standard, but it is very unlikely that the W3C will change course to adopt the more privacy-protected approach created by the IETF.

Although the W3C standard does have good language urging developers to protect privacy, the experience in the marketplace ranges widely. A researcher at the University of California at Berkeley, Nick Doty, has sought to identify Web sites that are implementing the W3C location standard. Of the sites he has been able to identify, about one-third of them have *no privacy policy whatsoever*, and many of the rest are silent in their privacy policies about the handling of location information.[44]

This standards development issue is *not* one that Congress should directly seek to address – technical development is best left in the hands of industry and standards bodies, not governments. However, the failure of the W3C member companies to take strong action to protect location privacy highlights the kinds of privacy gaps that result from allowing the marketplace to wholly dictate how privacy protections (or lack thereof) will evolve. The appropriate response from Congress should be to pass baseline privacy legislation that specially protects sensitive information such as location. If the United States adopts strong requirements to protect location privacy, the technology community will respond with standards and products that meet the legal requirements.

The Role of Congress

CDT believes that there are at least three specific measures needed to protect the privacy of location information, the first two of which 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.

[43] *See* W3C Geolocation Working Group Overview, http://www.w3.org/2008/geolocation/.

[44] *See* Nick Doty, Who's Using the W3C Geolocation API?, http://npdoty.name/location/services (last visited Feb. 21, 2010).

- 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.
- Third, location-based services and applications should follow technical standards that give users clear control over the use of their location information and that require the transmittal of privacy rules with the location information itself.

Conclusion

CDT would like to thank the Subcommittees again for holding this important and forward-looking hearing. We believe that Congress has a critical role to play in ensuring that privacy of location information is protected as location-based services increasingly become ubiquitous. CDT looks forward to working with the Members of both Subcommittees as they pursue these issues further.

For more information, contact John Morris, jmorris@cdt.org, or Alissa Cooper, acooper@cdt.org, or at (202) 637-9800.