Computer & Communications Industry Association
1972-2012: 40 YEARS OF TECH ADVOCACY

Before the

Subcommittee on Crime, Terrorism, and Homeland Security
U.S. House of Representatives Committee on the Judiciary

Regarding

Geolocation Privacy and Surveillance Act
May 17, 2012

Testimony of Edward J. Black
President & CEO
Computer & Communications Industry Association (CCIA)

Mr. Chairman, Ranking Member, and Members of the Subcommittee:

Thank you for the invitation to testify before you today on the important issue of geolocation privacy. CCIA is an international non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. In particular, we have a number of members involved in the mobile industry. Our members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue.[1]

Our industry occupies a unique position in the global marketplace. More than any other industry, it connects and empowers users. It helps educate, entertain, and erase distance. It serves as a powerful force for good in the global marketplace. At the same time, information generated by communication services can be misused by governments. In addition to posing a grave threat to civil liberties, this misuse will impair adoption and growth of ICT services. Thus, our constitutional values and our economic interests align, and point inexorably to the conclusion that a judicial warrant, founded upon probable cause, must accompany any law enforcement demands for private individuals' location information.

[1] For a complete listing of CCIA members see http://www.ccianet.org/members.

My testimony makes five points: First, geolocation privacy is a civil liberties imperative. The privacy concerns and Constitutional beliefs of the nation strongly support warrant protection for location information. Where a person is located in relation to society – their interactions, their associations, their sense of being a free citizen – this information is the very essence of personhood. To cede to government the unchecked power to track you wherever you are is to lay the cornerstone of the surveillance state. As the D.C. Circuit noted in its opinion in *United States v. Maynard*, location data reveals information about a person that would shock the average American, and it can do it for numerous surveillance targets, from the comfort of an air conditioned office. There can be no question that, as the court in *Maynard* decided, Americans have a reasonable expectation of privacy in their whereabouts.[2] The law should close the loophole in ECPA that was inadvertently created by new geolocation technology. Otherwise the intent of the original law as well as this reasonable expectation of privacy in one's whereabouts will be undermined.

Second, there is also an important business interest in location privacy. Mobile telephony and mobile Internet access are some of the fastest growing sectors in our national economy. Mobile penetration itself has grown at an incredible rate, and smartphones in particular continue to grab new users all the time. Mobile technology promises to improve lives in many ways and geolocation-aware devices and apps in particular offer a renaissance for users.

Third, many constituencies, from low-income and minority users, to many professionals, increasingly depend on mobile technology. For many, mobile devices are either the only means of accessing the Internet, or an indispensable tool in the workplace.

Finally, decreasing the trust that people have in the devices they use will have a meaningful impact on how those people interact in society and in business in the future. Trust is the most essential question when looking at the uptake of a new technology, particularly where data is concerned. This is why the GPS Act as introduced by Representatives Goodlatte and Chaffetz is so vital. Today, many users are aware that their smartphones have the capability to track their movements and, thanks to press surrounding the U.S. v. Jones case from last year, know that, at least for the time being,

[2] *United States v. Maynard*, 615 F.3d 544, 563-64 (DC Cir. 2010).

cell-site location data may not have the protection of a warrant. That knowledge impedes trust, and the GPS Act would send a clear signal that geolocation information collected through the use of cell phones will be respected and protected against government intrusion at the highest level.

I. Civil liberties of Americans demand the protection of location data.

Basic Fourth Amendment considerations call for the protection of location data just as we protect the content of letters and files within the home. The prevailing test for protection under the Constitution leads to the conclusion that the movement of people over time is information that the average American views as private data. To the extent that the courts have not embraced that rationale, Congress can and should step in to preserve location privacy rights.

The question of Fourth Amendment privacy rights in location information was raised most recently in a case that arose in Washington, DC. Police placed a GPS tracking device on the car of a suspected drug dealer without following proper warrant procedures, and the data gathered was challenged at trial.[3] The DC Circuit Court of Appeals issued a thoughtful opinion that came to the conclusion that people have a reasonable expectation of privacy in the collected history of their location information.[4] It can reveal intimate information about a person, including religion, political affiliation, health issues, and a host of other private details.[5] CCIA wholly agrees with this analysis.

The Supreme Court took a much narrower view when they heard the case, however. While they upheld the ruling, the majority opinion's theory was focused on the trespass that occurred when police placed the GPS receiver on the suspect's car.[6] This ruling certainly answered the question before the court, but left many other questions unanswered. It was not decided, for example, whether cell-site location information is similarly protected.

These questions are all the more unsettling because the government may misuse its powers in the name of preventing crime. The framers knew this reality well, and it is

[3] *Id.* at 549.
[4] *Id.* at 563-64.
[5] *Id.* at 562.
[6] *United States v. Jones*, 565 U.S. ___, slip op. at 4 (2012).

the genesis of the Fourth Amendment. Congress also appreciated the concern when it passed the Electronic Communications Privacy Act in 1986. It is now past time to clarify ECPA standards in response to new technology in several areas and geolocation information is one of them. CCIA agrees with the DC Circuit that the Fourth Amendment properly read protects all location data, but people's civil liberties need not wait on the courts. Congress has the ability to make sure that fundamental rights are not trampled on by a well-meaning but overreaching law enforcement, and the GPS Act would go a long way toward achieving that goal.

II. Economic considerations demand protecting location data.

A. Mobile technology is revolutionizing our economy.

Over the past decade mobile technologies have proven to be one of the most transformative of the information age. Their effects have been felt in everything from local emergency response to the fall of dictatorships.[7] Studies have linked mobile penetration to growth in GDP, particularly noting the network effects that increase GDP growth when penetration grows above 25%.[8]

The economic benefits of mobile access are hard to argue with. The mobile industry accounted for $195.5 billion in contribution to GDP and 3.8 million jobs in 2011 alone.[9] These numbers don't take into account the monetary benefits to mobile users who are better able to find what they're looking for, conduct business when traveling, and who gain numerous other advantages.

Nor do these studies address the non-monetary impact of mobile technologies. There are plenty of non-quantifiable, yet nonetheless important, benefits to mobile users. From family members quickly and easily able to let everyone know about a birth in the family, to checking the lyrics of that song you've had stuck in your head all day, all the way to being able to meet up with friends at the State Fair, mobile phones enable a host of desirable effects.

---

[7] Jamila Boughelaf, *Mobile phones, social media, and the Arab Spring*, April 2011. Tim Large, *Cell phones and radios help save lives after Haiti earthquake*, Reuters, Jan. 25, 2010.
[8] Kathuria *et al*., 2009.
[9] Press Release, Wireless Industry A Catalyst For U.S. Economic Growth, Supporting 3.8 Million Jobs And Adding $195.5 Billion To GDP In 2011, *at* http://www.prnewswire.com/news-releases/wireless-industry-a-catalyst-for-us-economic-growth-supporting-38-million-jobs-and-adding-1955-billion-to-gdp-in-2011-149649095.html

In the past few years, the effects of the mobile revolution have been compounded by the rise of smartphones, giving access to computational power that only would have been available in a desktop computer just few years ago, in a form factor that fits in a pocket. Access to the Internet at the push of a button has changed how we communicate but also how we work, shop, travel, and play. This market has shown its power, shipping 144.9 million smartphones in the first quarter of 2012, and proving to be a bright spot in an otherwise somber economic outlook.[10]

In addition to being a booming business of its own, mobile and smartphones enable other businesses. The marketplace for smartphone apps has exploded in the past few years, for example. The small applications that run on smartphones can be useful, such as maps or educational tools, or amusements to kill time, such as music players, games, and social networking. In any case, they are often simpler to program than their equivalents on computers, and an industry of small businesses and independent developers has risen to create this new marketplace.

B. Geolocation is an important piece of this marketplace.

One particularly appealing piece of the smartphone market is the potential for geolocation-enabled apps. Through a number of different means, including the use of global positioning satellites (GPS) and cell-site location information, smartphones are able to determine their own location with considerable accuracy.

The device's ability to know its own precise location enables a wide variety of exciting services. Turn-by-turn directions are an obvious usage, but the possibilities go far beyond that. Apps can provide reviews of and coupons for nearby establishments, let you know when friends are nearby, and more. Despite their usefulness, however, only 6% of Americans use geolocation aware apps, and 70% of users are completely unaware that they exist.[11]

---

[10] IDC Press Release, *Worldwide Smartphone Market Continues to Soar, Carrying Samsung Into the Top Position in Total Mobile Phone and Smartphone Shipments, According to IDC*, May 1, 2012, *at* http://www.idc.com/getdoc.jsp?containerId=prUS23455612

[11] Liz Gannes, *Checking in From the Cutting Edge: Only Six Percent Use Geolocation Apps*, Dec. 6, 2011, http://allthingsd.com/20111206/checking-in-from-the-cutting-edge-only-6-percent-use-geolocation-apps/

Users also often express uncertainty, however, regarding the privacy of their geolocation information when asked about location-aware apps.[12] Location privacy is of the utmost importance, because of the depth of details about a person that can revealed. A trace of a person's comings and goings over the course of a week can show not just where they work and sleep, but also religious preferences, doctor visits, political affiliations, and many other pieces of personal information.[13]

The potential for abuse that comes with this information means that the trust of the user is of the utmost importance if this market is to grow and reach its fullest potential. CCIA believes that companies must treat geolocation information with the highest respect when it is gathered from users. Companies, however, can only control their own data practices. The same problems of trust in the platform arise when it is the government demanding information. This is why it is so important to this nascent marketplace that Congress pass a law requiring a warrant based on probable cause before law enforcement may demand location information about a person.

III. Several constituencies depend heavily upon mobile technologies.

The issues surrounding trust in location information are exacerbated by the fact that for many minorities, low-income individuals, rural populations, and professionals, smartphones may be the primary (and in some cases only) means of accessing the Internet and the great possibilities and opportunities that exist online. Unfortunately, these groups are also precisely the ones with the least trust of government. The possibility is very real that knowledge of the ease with which the government can obtain location information is deterring some of these groups from accessing the Internet via smartphones.

Broadband access in the United States is expensive and slow as compared to the rest of the world.[14] In many rural areas, in fact, landline broadband Internet is still not available at any price.[15] For those who cannot afford or access landline broadband,

[12] Louise Barkuus and Anind Day, *Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns*, July 2003.
[13] *United States v. Maynard*, 615 F.3d 544, 562 (DC Cir. 2010).
[14] Saul Hansell, *The Broadband Gap: Why is Theirs Faster?*, N.Y. Times, Mar. 10, 2009.
[15] FCC, High-Speed Services for Internet Access: Status as of December 31, 2008 (2010), *at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-296239A1.pdf

smartphones have become the only available means of reaching the Internet. While it is excellent that smartphones provide this service to those who would otherwise not have a means of Internet access, this limitation also presents problems with government surveillance.

The problem arises because those very groups that benefit in this way from smartphones have long standing reasons to be suspicious of government surveillance. These anxieties, valid or not, will affect the uptake of smartphones. This effect is likely to particularly affect potential smartphone users because the idea that a phone can carry geolocation information is much more obvious in a *smart*phone (as opposed to a feature phone, which can be located by cell-site data just as easily, but which is not transparent about the fact). It is likely that the perception of a lack of privacy against government intrusion affects the trust that potential smartphone users will place in the platform. If they perceive that the device will make it easier for the police to track their movements, they will forego using the device. Unfortunately, in many cases that also means they they will forego access to the Internet entirely, along with the economic and social benefits that come with access.

For many professionals, including members of Congress and their staff, a mobile device is necessity of life. In many other cases as well, the modern technology-enabled workplace demands its use. Thus, even those who might forfeit the empowering technology of mobile communications to escape an umbrella of perpetual surveillance cannot do so because of the demands of their job.

IV. Trust is fundamental for growth and the current law undermines it.

The situations described above hold true across the nation. As businesses across the Internet industry know, the trust of users is essential when collecting information from them, and geolocation information is no different. New geolocation services have the challenge of convincing potential users that they will treat information about their location with respect. In short, they must convince the users to trust them.

There are many things that companies can do to enhance that trust. Among other practices, they can and should be transparent with their users about the information they gather and how it will be used, give those users as much control as possible over whether

and when the information is collected, and protect the information once it is in their hands. It is vital for the health of their business to make this effort, and it is industry best practice.

The one thing a company that collects location data cannot promise, however, is that they will protect that information against warrantless snooping by the government. The current state of Fourth Amendment law gives warrant protection against location information collected through a physical trespass (i.e., placing a device on a suspect's car), but not through cell-site information or information collected directly from a device's GPS receiver.[16] There is therefore quite a bit of uncertainty amongst companies about what the law is for each type of data, and what promises they can make to their users.

That uncertainty itself hampers innovation and the expansion of businesses. Any company seeking start-up funding for a business plan that involves location information faces an uphill battle trying to overcome the stigma of legal uncertainty in a related area. The same is true when trying to form business partnerships or trying to sell a business that has achieved some success.

The same uncertainty has an even more important effect on user trust. Users who are nervous about the privacy of their information will be turned off by finding out that the company collecting that data either cannot say for certain when they will have to turn it over to law enforcement or will affirmatively do so even when the government does not have a warrant.

V. The GPS Act can solve these problems.

The bill proposed by Representatives Goodlatte and Chaffetz would solve these problems by applying a uniform standard for government demands of location data. By making that standard a warrant, it gives assurances to all users that their location information will be protected at the highest level under the law. This simple change would eliminate the uncertainty that exists in the location services industry and increase the trust that users place in the companies in that industry.

[16] *United States v. Jones*, 565 U.S. ___, slip op. at 11 (2012).

The GPS Act is a straightforward piece of legislation. While the Electronic Communications Privacy Act is itself complex and in need of reform in a broader sense, this bill would make some simple additions that ensure that the government must show a judge probable cause before it may demand either the present or past location of a suspect. This bill does not render this information completely off limits to government. Law enforcement would simply need to obtain a warrant, just as it must do to access many other types of evidentiary personal information under the law and the Constitution.

The bill is also balanced. It recognizes that there are circumstances in which obtaining a warrant may be too time consuming or inappropriate. Exceptions are provided for cases of emergency, the consent of the user, and instances of foreign intelligence gathering. In this way the proposal does not attempt to put law enforcement in a straitjacket that prohibits the government from doing its job.

We believe that the changes made by the GPS Act are vital both for the privacy and civil liberties of Americans and for the positive effects it would have on an exciting and booming sector of our economy. I thank you for the opportunity to testify today, and I look forward to answering your questions.