Testimony of

Sally Greenberg

Executive Director

National Consumers League

Hearing on S. 2171

The Location Privacy Protection Act of 2014

Before the

United States Senate

Committee on the Judiciary

Subcommittee on Privacy, Technology and the Law

June 4, 2014

Introduction

Good afternoon Chairman Franken, Ranking Member Flake and members of the subcommittee. My name is Sally Greenberg and I am the Executive Director of the National Consumers League (NCL).[1] Founded in 1899, NCL is the nation's pioneering consumer organization. Our non-profit mission is to advocate on behalf of consumers and workers in the United States and abroad. I appreciate this opportunity to appear before the subcommittee to speak in support of S. 2171 and I applaud you for considering this critically important consumer privacy protection bill.

The Right to Privacy is a Bedrock Principle of American Democracy

Supreme Court Justice Louis Brandeis – who served as NCL's general counsel – noted in a landmark 1928 decision that the right to privacy is "the most comprehensive of rights, and the right most valued by civilized men."[2] We could not agree more. NCL believes that privacy is a cornerstone of consumer protection and a fundamental human right.

According to a *Consumer Reports* poll from 2012, most consumers are "very concerned" about Internet firms selling information about them without their

---

[1] The National Consumers League, founded in 1899, is America's pioneer consumer organization. Our non-profit mission is to protect and promote social and economic justice for consumers and workers in the United States and abroad. For more information, visit www.nclnet.org.

[2] *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, L., dissenting). Online: http://www.law.cornell.edu/supremecourt/text/277/438#writing-USSC_CR_0277_0438_ZD

permission. The poll found that 71% of consumers were very concerned about online data collection, while 65% were worried about the way smartphone apps could access their personal contacts, photos, location and other data without their permission.[3] A *Los Angeles Times* poll showed similar results; 82% of Californians were very or somewhat concerned about Internet and smartphone firms collecting their information.[4]

As new technologies, products, and services are introduced into the marketplace, their ability to gather information and share data broadly without sufficient privacy rules and protections in place is of great concern. This is why NCL supports S. 2171, the Location Privacy Protection Act of 2014**,** which will put in place a privacy protection regime that is adapted to today's mobile data ecosystem.

This bill proposes a modest approach to protecting consumer privacy and includes exceptions for parental rights, national security, law enforcement or other discrete circumstances. We support affirmative consumer consent prior to the collection of location information and disclosure about the purpose of such collection and the uses of that information. Consumers must have control over whether and how their location information is used, particularly if it is to be used for purposes other than those for which it was originally obtained. We also believe

[3] Sarno, David. "Consumer Reports, Times polls find broad data privacy concerns," *The Los Angeles Times.* April 3, 2012. Online: http://articles.latimes.com/2012/apr/03/business/la-fi-tn-consumer-reports-privacy-20120403

[4] *Id.*

that consumers should have a private right of action to obtain redress when breaches of their privacy occur.

Privacy Breaches Threaten Trust in Location-Based Services

The ubiquity of smartphones, tablets and other mobile devices has dramatically changed the way consumers interact with the digital world. There is no question that consumers love the convenience and functionality of the array of apps and other mobile technologies available to them today. Thanks to the widespread use of location data, enabled by technologies such as GPS, consumers can now navigate to their favorite coffee shops, discover the closest sushi restaurant and be more easily located by emergency response providers. This technology has clearly provided immense consumer benefits.

The wide adoption of location-aware devices has also spawned a growing industry. In May 2011, only 35% of American adults owned smartphones. Today, 58% of adults own them.[5] Marketers are increasingly cashing in on the treasure trove of location data that the proliferation of such devices has created. According to one study, the $3.9 billion currently spent on "geo-targeted" mobile advertising tailored to a user's precise location is likely to grow to $9.1 billion by 2017.[6]

---

[5] Smith, Aaron. *Smartphone Ownership 2013*. June 5, 2013. Online: http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/

[6] BIA/Kelsey. "BIA/Kelsey Forecasts U.S. Mobile Local Ad Revenue to Reach $9.1 Billion in 2017," Press Release. April 4, 2013. Online: http://www.biakelsey.com/Company/Press-Releases/130404-U.S.-Mobile-Local-Ad-Revenues-to-Reach-$9.1-Billion-in-2017.asp

As the collection and use of location data has become an integral part of the mobile ecosystem, so too has consumer concern over the use – and misuse – of these data. Consumers place special value on their location data. They are less comfortable sharing this information with people they don't know and they want more control over it.[7] This should not be surprising. Unlike location data gained from a non-mobile device, such as a desktop computer, data from mobile devices is inherently personal and can be used to learn and possibly disclose information that in many cases consumers would rather be kept private. Supreme Court Justice Sotomayor underscored the sensitivity of location data in her concurring opinion in *U.S. v. Jones* when, quoting from an earlier New York case, she wrote:

> *"Disclosed in [GPS] data... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal*

[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.

defense attorney, the by-the- hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[8]

While reputable businesses may recognize and respect the sensitivity of location data, the rules that govern use of these data are largely voluntary. In addition, there are significant loopholes and confusion regarding the applicability of current laws to sensitive location data. We need only look to the recent past to find incidences where businesses have failed to follow industry best practices. For example:

- In August 2011, it was reported that Windows 7 smartphones were sending their users' location to Microsoft when the camera app was on. This data sharing happened even when users denied consent to do so.[9]

- In December 2013, the makers of the Brightest Flashlight Android app settled a FTC enforcement action alleging that, contrary to their privacy

[8] UNITED STATES v. JONES () 615 F. 3d 544. Online: http://www.law.cornell.edu/supremecourt/text/10-1259

[9] Levine, Dan. "Lawsuit says Microsoft tracks customers without consent," *Reuters*. August 31, 2011. Online: http://www.reuters.com/article/2011/08/31/us-microsoft-lawsuit-idUSTRE77U6BT20110831

policy, the makers of the app disclosed users' precise location and unique device identifier to third parties, including advertising networks.[10]

- We learned in February of this year that the dating app Tinder allowed any user of the app to identify another user's location to within 100 feet, not the nearest mile as the app promised. This was the second time in less than a year that this app was found to be broadcasting sensitive location data.[11]

- Just last month, the FTC settled charges against Snapchat, Inc. – makers of a popular photo-sharing app – that the company collected and transmitted location of information from users of its Android app despite claims in its privacy policy that it did not track this information.[12]

These are just a few recent examples of companies failing adhere to their own stated privacy policies and play fair with consumers' location data.

---

[10] Federal Trade Commission. "Android Flashlight App Developer Settles FTC Charges It Deceived Consumers," Press Release. December 5, 2013. Online: http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived

[11] Summers, Nick. "New Tinder Security Flaw Exposed Users' Exact Location for Months," *BloombergBusinessweek*. February 19, 2014. Online: http://www.businessweek.com/articles/2014-02-19/new-tinder-security-flaw-exposed-users-exact-locations-for-months

[12] Federal Trade Commission. "Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False," Press Release. May 8, 2014. Online: http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

Investigations by the *Wall Street Journal*,[13] the U.S. Government Accountability Office[14] and the Federal Trade Commission[15] have all found that the collection and sharing of consumers' location data is widespread and often occurs without their consent.

Current Laws Have Failed to Keep Pace With the Rapid Evolution of Location-Based Services

The consensus among consumer privacy advocates and government officials is that there is no adequate legal framework protecting consumers' most sensitive data, including location data, in the current and ever-evolving mobile ecosystem. No federal law requires companies to obtain consumers' permission before sharing location data collected from users' mobile devices. Absent such legislation, consumers are left to rely for their protection on self-regulation by mobile phone

---

[13] Thurm, Scott and Kane, Yukari Iwatani. "Your Apps Are Watching You," *The Wall Street Journal*. December 17, 2010. Online: http://online.wsj.com/news/articles/SB10001424052748704694004576020083703574602?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB10001424052748704694004576020083703574602.html

[14] *See e.g.*, U.S. Government Accountability Office. *Mobile Location Data: Additional Federal Actions Could Help Protect Consumer Privacy*, pg. 19. September 2012. Online: http://www.gao.gov/assets/650/648044.pdf

[15] Federal Trade Commission. "FTC's Second Kids' App Report Finds Little Progress in Addressing Privacy Concerns Surrounding Mobile Applications for Children," Press Release. December 10, 2012. Online: http://www.ftc.gov/news-events/press-releases/2012/12/ftcs-second-kids-app-report-finds-little-progress-addressing

providers and app developers, as well as outdated and vague laws that may or may not apply to location data collected via mobile devices.

For example, the Electronic Communications Privacy Act (ECPA) prevents companies that collect location information from a smartphone (e.g. mobile operating system providers, application developers, and wireless carriers) from sharing that information with the government without consumer consent. However, under ECPA there is virtually no legal restriction on businesses' ability to share location data obtained from mobile devices with other, non-governmental, third parties.[16]

Similarly, the Telecommunications Act of 1996 and the Cable Communications Policy Act of 1984 prohibit telecommunications providers from disclosing customer proprietary network information (CPNI), including "location—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."[17] Except in certain narrow instances (such as in emergency contexts), the CPNI rules provide privacy

[16] *See, e.g.* Statement of Jason Weinstein, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice before the Subcommittee on Privacy, Technology and the Law of the Committee on the Judiciary, United States Senate. May 10, 2011. ("It [ECPA] places a great deal of restrictions on the ability of providers to share that information with the Government, but virtually no legal restriction on providers' ability to share that with other third parties.") Online: http://www.gpo.gov/fdsys/pkg/CHRG-112shrg86775/html/CHRG-112shrg86775.htm

[17] 47 U.S.C. § 222.

protections for location information transmitted by a consumer's mobile device in the course of a telephone call. However, if that same device were to then be used to transmit location data via the wireless carrier's mobile broadband network (such as via a mapping app), the privacy of that data would *not* be protected the CPNI rules do not apply to location data collection independent of the telecommunications carrier's network.

Finally, the Federal Trade Commission (FTC) has been seen as the default privacy regulator for most consumer data under the FTC Act's prohibition on unfair and deceptive trade practices.[18] Indeed, the FTC has brought numerous enforcement actions against companies that have failed to live up to their privacy policies with regards to the collection and sharing of location data (e.g. Snapchat, Brightest Flashlight). However, under current law, if companies affirmatively state in their privacy policies that they will collect and share their users' location data without consent with any third party they wish, they are free to do so and the FTC has little power to stop them. As long as a company is not violating its own privacy policy, the FTC or state Attorneys General would likely have no grounds to bring a case. Given the sensitivity of location data, the limited resources of state and federal enforcement agencies and the lack of a comprehensive privacy framework, we need the affirmative rules governing the sharing of location data that S. 2171 provides.

[18] 18 U.S.C. § 1030

Industry Self-Regulation Has Failed to Adequately Protect Consumers' Location Data

Absent a clear legal framework regarding location privacy, businesses have relied on a variety of often voluntary and inconsistently applied company policies and industry best practices.

For example, Apple contractually requires that app developers using its app store obtain users' consent before collecting or disclosing location information to third parties and provide disclosure regarding the use of location-based data.[19] Google requires users to provide opt-in consent before location information can be collected by its Android operating system during the initial set-up process for a smartphone or other mobile device.[20] However, Google does not control the use of location data by third-party applications using a device running the Android operating system.[21]

---

[19] Letter from Bruce Sewell to The Honorable Edward J. Markey and the Honorable Joe Barton. Pg. 10. July 12, 2010. Online: http://www.wired.com/images_blogs/gadgetlab/2011/04/applemarkeybarton7-12-10.pdf#page=10

[20] *See, e.g.* Testimony of Alan Davidson, Director of Public Policy, Google Inc. Before the U.S. Senate Committee on Commerce, Science and Transportation Subcommittee on Consumer Protection, Product Safety, and Insurance. Pg. 5. May 19, 2011. Online: https://docs.google.com/a/nclnet.org/file/d/0BwxyRPFduTN2ZTJjYzA4YjItZTc0Ni00ZjQ3LTk1YTYtZDFiMzkwMGY1NTYx/edit?hl=en

[21] *Ibid*. Pg. 7.

Similarly, a GAO study of in-car location based services found that despite recommended practices, location data disclosures were often broadly worded and inconsistently described the purposes for sharing de-identified location data. In addition, the GAO study noted that the in-car services had inconsistent policies or failed to follow industry best practices with regards to location data retention, data deletion and accountability disclosure.[22]

Multi-stakeholder agreements, such as the National Telecommunications and Information Administration's (NTIA) short form notice code of conduct to promote transparency in mobile applications[23] and Future of Privacy Forum's Mobile Location Analytics Code of Conduct[24] may provide a forum for industry self-regulation in the area. However, the voluntary nature of multi-stakeholder agreements and industry best practices limits their value in protecting consumers in the rapidly growing mobile data ecosystem.

---

[22] United States Government Accountability Office. *In-Car Location-Based Services: Companies Are Taking Steps to Protect Privacy, but Some Risks May Not Be Clear to Consumers* (GAO-14-81). Pg. 12-20. December 2013. Online: http://www.gao.gov/assets/660/659509.pdf

[23] National Telecommunications & Information Administration. *Short Form Notice Code of Conduct To Promote Transparency in Mobile App Practices*. Redline Draft. July 15, 2013. Online: http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf

[24] Future of Privacy Forum. "Future of Privacy Forum Partners with The Wireless Registry to Create Central Location Analytics Opt-out Service," Press Release. February 18, 2014. Online: http://www.futureofprivacy.org/wp-content/uploads/FINAL-PRESS-RELEASE.pdf

The Location Privacy Protection Act of 2014 Is a Critically Important Consumer Protection Measure For Meeting the Privacy Challenges of Today's Rapidly Evolving Mobile Data Ecosystem

While NCL supports a comprehensive legal framework to protect the privacy of *all* consumer data, absent Congressional action to create such a framework, steps should be taken to protect especially sensitive types of information such as location data. Such action is appropriate and would be consistent with other areas in which Congress has recognized the sensitivity of certain types of consumer data such as health care (the Health Insurance Portability and Accountability Act's Privacy Rule[25]), financial services (the Gramm-Leach-Bliley Act's Financial Privacy Rule[26]), children's data (Children's Online Privacy Protection Act[27]) and videotape rental and sales records (Video Privacy Protection Act[28]).

As consumer surveys demonstrate, consumers are worried about the use of their location data and want greater understanding of and control over what they share with businesses in the mobile data ecosystem. It is also apparent that the combination of current law and industry best practices has failed to meet this need. Congressional action is clearly necessary to address the gaps in the law that make it impossible to provide robust consumer protections for sensitive location data.

---

[25] 45 C.F.R. Parts 160 and 164, Subparts A, C, and E

[26] 15 U.S.C. §§ 6801–6809

[27] 15 U.S.C. §§ 6501–6506

[28] 18 U.S.C. § 2710

This pro-consumer and pro-privacy bill would help to restore consumer trust in location-based services and ensure that the many benefits of this technology continue to flow to consumers and the economy. The need for this bill has been amply demonstrated via recommendations from the GAO, FTC and consumer and privacy advocates.

In particular, we believe that the bill's opt-in provisions will give consumer the information they need to make an informed decision regarding the use (or not) of location-based services on their mobile devices. Requiring up-to-date disclosures of how location data are being used, coupled with an opportunity to opt-out at a later date, gives consumers needed and ongoing control over their data.

By prohibiting so-called "stalking apps," the law will appropriately outlaw a class of inherently deceptive and predatory applications that compromise the personal safety of some of our most vulnerable citizens. No federal law currently prohibits the operation of such apps, which are designed to run secretly without the user's knowledge.

This bill would not, as some have argued, create an undue burden on innovators.[29] Indeed, if that were a real threat, NCL would not support this effort.

[29] Josten, R. Bruce. "Letter Opposing S.1223, the 'Location Privacy Protection Act of 2011,' and Substitute Amendment," U.S. Chamber of Commerce. December 4, 2012. Online:

Fortunately, the LPPA simply closes loopholes in existing law and levels the playing field to ensure that all mobile device applications and services play by a standard set of consumer protection rules. Responsible application service providers such as Apple and Google already require or at least strongly recommend that mobile applications respect the sensitivity of consumers' location data. This bill would simply give those best practices the force of law, creating a strong incentive for application developers and others to use location data responsibly. The bill also gives the FTC discretion to craft rules that preserve the benefits of location-based services and avoid redundant notifications to consumers.

Protections such as those embodied in S. 2171 would be of little use without effective enforcement mechanisms. We therefore support the bill's provisions establishing clear enforcement authority for the Department of Justice. S. 2171 is in line with similar consumer protection laws such as ECPA. In addition, we strongly believe that the creation of a private right of action is imperative. Given the limited resources of federal enforcement agencies, an appropriately defined private right gives an extra layer of protection to consumers. The granting of a private right of action will not, as some have argued, squelch innovation.[30] For example, the Stored

---

https://www.uschamber.com/letter/letter-opposing-s1223-%E2%80%9Clocation-privacy-protection-act-2011%E2%80%9D-and-substitute-amendment

[30] *See, e.g.* U.S. Chamber of Commerce. "Letter Opposing S. 1223, the 'Location Privacy Protection Act of 2011,' and Substitute Amendment," December 4, 2012. Online: https://www.uschamber.com/letter/letter-opposing-s1223-%E2%80%9Clocation-privacy-protection-act-2011%E2%80%9D-and-substitute-amendment

Communications Act[31] and the Video Privacy Protection Act[32] both have had uncapped private rights of action (as opposed to the $2 million cap for willful violations proposed in S. 2171). While these laws were in place the Internet economy and online video services such as YouTube and Netflix have flourished.

Conclusion

In closing, I would like to reiterate NCL's strong support for S 2171. In today's ever-changing digital economy, consumers expect and deserve that the privacy of sensitive data such as their location information will be protected. Absent such protections, consumers may indeed become less trusting in location-based services, which would be hugely harmful to innovation and the broader economy.

Mr. Chairman, Mr. Ranking Member and members of the subcommittee, on behalf of the National Consumers League and America's consumers, I applaud your leadership in convening this hearing and your invitation to testify on this important issue. I look forward to answering any questions you may have.

Thank you.

[31] 18 U.S.C. Chapter 121 §§ 2701–2712

[32] 18 U.S.C. § 2710