Journal of Technology Law & Policy

Volume XIII – Spring 2013

ISSN 1087-6995 (print)

DOI 10.5195/tlp.2013.121

http://tlp.law.pitt.edu

First Amendment Concerns in Governmental Acquisition and Analysis of Mobile Device Location Data

Gerald J. Votava III

First Amendment Concerns in Governmental Acquisition and Analysis of Mobile Device Location Data

Gerald J. Votava III[*]

> *I would rather be exposed to the inconveniences attending too much liberty, than those attending too small a degree of it.*
>
> Thomas Jefferson[1]

INTRODUCTION

Mobile cellular telephones have been widely adopted in the United States, and they are essentially a ubiquitous item carried by all citizens, similar to a person's house keys and wallet.[2] These mobile devices are in near constant communication with nearby cellular radio towers and related infrastructure and are required by Federal Regulations to include location-identifying technology for the use of 9-1-1 services.[3] These systems, while providing clear benefits to the public, also provide governmental authorities an unprecedented ability to identify, monitor, collect, and analyze the location and movements of all people within the range of a cellular radio tower.[4]

Over the past generation, the United States has shifted to a form of governance dependent on the collection, collation, and analysis of information about its people.[5] These information gathering activities are intended to enhance

[*] Gerald J. Votava III is a J.D. Candidate at the University of Pittsburgh School of Law, 2014; B.E.E. in Electrical Engineering from the Villanova University.

[1] Letter from Thomas Jefferson to Archibald Stuart in Philadelphia (Dec. 23, 1791), *in* 22 THE PAPERS OF THOMAS JEFFERSON 436 (Charles T. Cullen ed., 1986).

[2] *See infra* Part I.A and associated footnotes.

[3] *See infra* Part I.B and associated footnotes.

[4] *See infra* Part I.C and associated footnotes.

[5] Jack M. Balkin, *The Constitution in the National Surveillance State*, *in* THE CONSTITUTION IN 2020, at 198 (Jack M. Balkin & Reva B. Siegel eds., 2009).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

national security, prevent crime, and deliver social services.[6] This new form of governance is the National Surveillance State.[7]

This pervasive and unchecked surveillance threatens Americans' rights of freedom of expression and freedom of association.[8] Datasets of the locations and movements of individuals obtained via mobile device location data[9] can be combined to elicit patterns of association.[10] Writing in concurrence in the landmark GPS case, *United States v. Jones*,[11] Justice Sotomayor said, "[a]wareness that the Government may be watching *chills associational and expressive freedoms*. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[12]

I. MOBILE DEVICE LOCATION DATA: ORIGINS AND USES

A. Current Technology

Mobile cellular devices are now very prevalent in the United States, and are carried by most citizens every day. These devices include traditional cellular telephones known as feature phones, advanced cellular telephones known as smartphones, and tablet and notebook computers with cellular radios included in the device. As of 2012, there were approximately 259 million people over the age of 14 in the United States.[13] Telecommunications industry analyst data indicates that approximately 235 million people in that population utilize a mobile device,[14] equating to a penetration rate of over 90%. The data further indicates that roughly half of mobile device users have adopted advanced smartphones, including Apple

[6] *Id.* at 199.

[7] *Id.* at 198.

[8] *See infra* Part II.A and associated footnotes.

[9] This article addresses mobile device location data as opposed to cell-site location records (CSLR), because CSLR is one component of location data, which also includes other services such as GPS and aGPS data created by mobile devices.

[10] *See infra* Part I.C and associated footnotes.

[11] United States v. Jones, 132 S. Ct. 945 (2012).

[12] *Id.* at 956 (Sotomayor, J., concurring) (emphasis added).

[13] CIA WORLD FACTBOOK (Feb. 12, 2013), https://www.cia.gov/library/publications/the-world-factbook/geos/us.html.

[14] Henry Blodget, *Actually, The US Smartphone Revolution Has Entered The Late Innings*, BUSINESS INSIDER (Sept. 13, 2012), http://www.businessinsider.com/us-smartphone-market-2012-9#ixzz2Mjqum3PI (citing ComScore data of mobile device usage).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

iPhone and Google Android devices.[15] All mobile devices, including feature phones and smartphones, are capable of creating and transmitting various forms of data to identify the location of the device.

1. Cell-site Location Records

All cellular mobile devices connect to a telecommunications network via cellular radio towers constructed by private service providers.[16] These towers contain up to three antennae, and keep records of the mobile devices that connect to them, including the specific sector that they are connecting from.[17] These records are often referred to as cell-site location records (CSLR). The accuracy is limited to the distance between the recording cell radio tower and any nearby towers to which the mobile device can connect.[18] Although this data is fairly general, it can be used to track a person's movement. In addition to the passive collection of CSLR data, that data can be aggregated and analyzed to triangulate the user's position.

2. Global Positioning Systems

The Global Positioning System (GPS) uses a network of 27 satellites to permit client devices to triangulate their position with a relatively high degree of accuracy.[19] Devices with a greater number of GPS sensors or higher quality sensors are able to obtain better accuracy, but these devices are more expensive and require more power to operate.[20] In mobile devices, traditional GPS systems have been augmented by assisted-GPS (aGPS).[21] With aGPS, the mobile device continues to receive signals from GPS satellites, but it can also contact ground-based servers via a terrestrial telecommunication network, providing an even greater accuracy of the location data.[22] The aGPS service reduces the time needed to acquire a location data point and assists with accuracy indoors, where signals from GPS satellites are more difficult to obtain.[23] aGPS has many benefits for mobile device users.

---

[15] *Id.*

[16] *Cell Phone Location Tracking by Government: How It's Done*, GRITS FOR BREAKFAST (Mar. 4, 2013), http://gritsforbreakfast.blogspot.com/2013/03/cell-phone-location-tracking-by.html.

[17] *Id.*

[18] *Id.*

[19] S. Kamakshi, *What is A-GPS? How Does it Work?*, TECH2 (Mar. 18, 2010), http://tech2.in.com/features/all/what-is-agps-how-does-it-work/115142.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

However by definition, the device also contacts third party networks, which can record locational data.[24]

B. Services That Utilize Mobile Device Location Data

There are numerous systems within a mobile device, which utilize mobile device location data. Often, these services are difficult or prohibited from disabling. As a result, whenever a user powers on their device, locational data is being recorded, and in some cases, shared with third parties.

1. E911 Systems

As cellular phones became the communication tool of choice for many Americans, they began to use those devices to initiate 9-1-1 emergency response calls. Traditionally, wireline telephone service provided 9-1-1 operators with specific location data in the case that the caller was unable or unwilling to provide that information. The Federal Communications Commission (FCC) created regulations that compel mobile devices and the networks to which they connect, to provide data regarding the location of the device in order to assist in emergency response operations.[25] Notably, by January 18, 2013, 67% of all calls placed from handsets should be locatable to within 50 meters,[26] with further increases in accuracy required after that date. Compliance with these regulations is typically accomplished through the inclusion of GPS or aGPS technology within the mobile device, leaving consumers with no methods to opt out of this service.

2. Use by Cellular Telecommunications Companies

Telecommunications companies actively collect and utilize mobile location data.[27] The data is utilized in a variety of ways. It can be used to understand how each company's customers use the provided services so that the company can then take any necessary actions to strengthen and improve those services.[28] Furthermore, mobile device location data is aggregated and used for marketing and advertising activities.[29]

---

[24] *Id.*

[25] 47 C.F.R. § 20.18 (2012); *911 Wireless Services*, FCC, http://www.fcc.gov/guides/wireless-911-services (last visited Apr. 11, 2013).

[26] 47 C.F.R. § 20.18(h)(2)(i) (2012).

[27] Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html.

[28] *Id.*

[29] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

3. Use by Third Party Application Developers

Modern mobile devices are often layered with an ecosystem of software applications created by third parties other than the device manufacturer or the telecommunications company. These applications expand the utility of the mobile device by allowing users to customize the features of the phone. Many of these applications acquire mobile device location data, and at times, transmit that data to third party servers to deliver additional service.[30]

For example, some companies[31] use mobile device location data to interpret, via algorithm, traffic flow in order to reroute other users of the application to their destination more efficiently.[32] A second example involves a task as common as an internet search made from a mobile device. In an effort to improve its services and increase the value of user data used in connection with its advertising activities, Google, an internet search company,[33] routinely gathers location data from users interacting with its search products.[34] These locational details are retained as business records in connection with the company's advertising businesses.[35] Finally, even mobile applications designed to connect us with our elected officials sometimes collect mobile device location data.[36]

C. Obtainment of Location Data by Government Agents

In the wake of *Jones*, government agents have increasingly used mobile device location data to identify the locations of investigation targets, and this has created a shift in governmental policy towards the warrantless acquisition of cell

---

[30] *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html; *What They Know—Mobile*, WALL ST. J., http://blogs.wsj.com/wtk-mobile/ (last visited Apr. 11, 2013).

[31] *See* WAZE, http://www.waze.com/ (last visited Apr. 12, 2013) (Waze is a mapping and traffic application that relies on location received from users to provide traffic estimates to other users of the application.).

[32] Saurabh Amin et al., *Using GPS Mobile Phones As Traffic Sensors: A Field Experiment*, 15TH WORLD CONGRESS ON INTELLIGENT TRANSPORTATION SYSTEMS (Nov. 16, 2008), *available at* http://bayen.eecs.berkeley.edu/sites/default/files/conferences/its08.pdf.

[33] *See About Google*, GOOGLE, https://www.google.com/intl/en/about/ (last visited Mar. 28, 2013) (corporate website).

[34] Jeremy Hull, *What Else Are You Telling Google When You Hit the Search Button?*, CLICKZ (Mar. 14, 2013), http://www.clickz.com/clickz/column/2254624/what-else-are-you-telling-google-when-you-hit-the-search-button.

[35] *Id.*

[36] John E. Dunn, *Obama and Romney election apps suck up personal data, research finds*, NETWORKWORLD (Aug. 12, 2012), http://www.networkworld.com/news/2012/082112-obama-and-romney-election-apps-261806.html.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

phone data.[37] The data is often sought as a "business record," belonging to cellular telecommunications companies or third party application developers, such as Google and Microsoft.[38]

Elected leaders have also attempted to shed light on this issue. Rep. Edward Markley[39] found that "in 2011, federal, state and local law enforcement agencies made more than 1.3 million requests of wireless carriers for the cell phone records of consumers."[40] The investigation further revealed that agencies often requested "'cell tower dumps' in which carriers provide all the phones numbers of cell users that connect with a tower during a discreet period of time, including information on innocent people."[41]

Advocacy groups, such as the American Civil Liberties Union (ACLU), have also investigated the collection and use of mobile device location data. Their review of over 250 law enforcement agencies revealed that only 13 had not used mobile device location data.[42] The investigation noted that some agencies pervasively seek and use the data.[43]

Further, some government agents have begun to use the StingRay platform, which acts as a cellular radio tower in order to stimulate nearby mobile devices to identify their locations through triangulation.[44] With this device, "government investigators and private individuals can locate, interfere with, and even intercept communications from cell phones and other wireless devices."[45] This activity

---

[37] David Kravets, *After Car-Tracking Smackdown*, WIRED (Mar. 31, 2012), http://www.wired.com/threatlevel/2012/03/feds-move-to-cell-site-data/.

[38] *Google Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US/ (last visited Mar. 29, 2013); Brad Smith, *Microsoft Releases 2012 Law Enforcement Requests Report*, THE OFFICIAL MICROSOFT BLOG (Mar. 21, 2013), http://blogs.technet.com/b/microsoft_blog/archive/2013/03/21/microsoft-releases-2012-law-enforcement-requests-report.aspx.

[39] Democratic Representative from Massachusetts.

[40] *Markey: Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers*, ED MARKEY (July 9, 2012), http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers.

[41] *Id.*

[42] *Cell Phone Location Tracking Public Records Request*, AMERICAN CIVIL LIBERTIES UNION (Mar. 25, 2013), http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request.

[43] *Id.*

[44] *EPIC v. FBI—Stingray/Cell Site Simulator*, EPIC, http://epic.org/foia/fbi/stingray/ (last visited Apr. 12, 2013).

[45] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

clearly goes beyond the seemingly innocuous practice of accessing business records.

Finally, a significant concern with the sweeping collection of locational data is the government's ability to analyze that information to determine an individual's membership in groups.[46] Algorithms can be used to determine individuals' ad-hoc and semi-permanent social groups based on the examination of locational trends of groups of individuals.[47] If government agents embrace this type of activity, it would very likely be considered an unconstitutional violation of the individual's freedom of expressive association.[48]

II. FIRST AMENDMENT: FREEDOM OF EXPRESSION AND ASSOCIATION

A. Freedoms Defined

The First Amendment,[49] and its protection of speech, religion, expression, and association, is one of the critical cornerstones of American culture and democracy. There are four central principles behind these freedoms. First, open discussion has been recognized as an essential component of self-governance. The ability to directly criticize government officers and policies is within "the central meaning of the First Amendment."[50] Second, truth can be discovered through the clash of ideas. Justice Oliver Wendell Holmes described this tension as a "marketplace of ideas," each competing through the power of thought.[51] Third, the First Amendment protects and fosters individuality and personal autonomy, and sees expression as intrinsically important. "The First Amendment serves not only the needs of the polity but also those of the human spirit—a spirit that demands self-expression."[52] Finally, the three prior principles can be combined with a fourth principle of promoting tolerance. This principle "involves a special act of carving out one area of social interaction for extraordinary self-restraint, the purpose of

[46] Steve Mardenfeld et al., *GDC: Group Discovery using Co-location Traces*, IEEE INTERNATIONAL CONFERENCE ON PRIVACY, SECURITY, RISK AND TRUST (2010), *available at* http://cs.njit.edu/~borcea/papers/sca-socialcom10.pdf.

[47] *Id.*

[48] *See infra* Part II.A.1 and associated footnotes.

[49] U.S. CONST. amend. I.

[50] New York Times v. Sullivan, 376 U.S. 254, 273 (1964).

[51] Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting).

[52] Procuiner v. Martinez, 416 U.S. 396, 427 (1974) (Marshall, J., concurring).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

which is to develop and demonstrate a social capacity to control feelings evoked by a host of social encounters."[53]

1. Freedom of Association

The freedom of association is a constitutional right that ensures the inviolability and integrity of groups against unjustified government intrusion. The right is not explicitly enumerated in the Constitution, but it has repeatedly been upheld as a right protected by the First Amendment. The Supreme Court first articulated the right in *NAACP v. Alabama*[54] as the right to privacy in one's associations. The Court held that the NAACP could not be required to disclose the identities of its members to state agents.

The Court in *NAACP* defined association as foundational to First Amendment rights:

> Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly. It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable part of the . . . freedom of speech.[55]

The Court also emphasized the need for privacy in association:

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [affirmative governmental action in other cases.] This court has recognized the vital relationship between freedom of association and freedom of privacy.[56]

---

[53] LEE BOLLINGER, THE TOLERANT SOCIETY: FREEDOM OF SPEECH AND EXTREMIST SPEECH IN AMERICA 9–10 (1986).

[54] NAACP v. Alabama, 357 U.S. 449 (1958).

[55] *Id.* at 460.

[56] *Id.* at 462.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

Revelation of identity or association with a group "may induce members to withdraw . . . and dissuade others from joining [a group] because of fear of exposure of their beliefs . . . and of the consequences of this exposure."[57] These consequences are particularly pronounced when certain groups embrace beliefs that are not popular with the majority.[58] The government's conduct is "subject to the closest scrutiny" due to the seriousness of the harm.[59]

In this case, NAACP members sought to prevent future releases of membership information because their members had previously been subjected to economic reprisals and physical threats from private individuals when their identities were divulged.[60] The government claimed a need for the list in order to determine whether the organization was conducting intrastate business in violation of the Alabama Foreign Corporation Act.[61] In evaluating the link between the statute and the list, the Court held such justification too insubstantial to require disclosure.[62]

The Court has bifurcated the right of association into two broad categories:[63] intimate association[64]—the right to associate to pursue private relationships, and expressive association[65]—the right to associate to engage in protected First Amendment expression.

2. Chilling Effects

There is a strong possibility that overreaching relational surveillance will chill free expression and association. The First Amendment's protection of freedom of association provides a proper framework for regulating relational surveillance.[66] Citizens are discouraged from exercising their constitutionally protected rights

---

[57] *Id.* at 463.

[58] *Id.* at 462.

[59] *Id.* at 461.

[60] *NAACP*, 357 U.S. at 462.

[61] *Id.* at 451.

[62] *Id.* at 464.

[63] Roberts v. U.S. Jaycees, 468 U.S. 609 (1984).

[64] *Id.* at 619–20.

[65] *Id.* at 618.

[66] Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

while under broad sweeping state inquiries.[67] Even when the chilling effect is an unintended consequence of the government's conduct, strict scrutiny review of the conduct is necessary.[68]

In *Clark v. Library of Congress*,[69] a government employee brought an action against his employer for conducting full-fledged investigations into his political activities with the Young Socialists Alliance.[70] The court found that the investigation chilled the plaintiff's right to freely associate,[71] and found that there was no legitimate or compelling justification for the investigations.[72]

Zweibon v. Mitchell[73] discussed the problem of continuous surveillance by government agents. In this case, the Federal Bureau of Investigation subjected the Jewish Defense League to numerous wiretaps on their telephones without prior judicial approval.[74] The court determined that a warrant was necessary for such surveillance.[75] According to the court, judicial review was necessary to protect First Amendment rights of expression and association from the chilling effects of unsupervised and unlimited executive power to institute electronic surveillance.[76]

3. Overbreadth

A law is unconstitutionally overbroad if it regulates substantially more expression than the Constitution allows to be regulated.[77] A law is deemed to be unconstitutionally overbroad when a person to whom the law can be constitutionally applied can argue that it would be unconstitutional as applied to others.[78] Where the overbreadth is substantial and real, it is unconstitutional.[79] The

---

[67] Baird v. State Bar of Ariz., 401 U.S. 1, 6 (1971) (holding the State Bar Association's bar of an applicant solely for membership in certain political organizations was barred by the First Amendment).

[68] Elrod v. Burns, 427 U.S. 347, 362 (1976).

[69] Clark v. Library of Cong., 750 F.2d 89 (D.C. Cir. 1984).

[70] *Id.* at 91–92.

[71] *Id.* at 91.

[72] *Id.* at 99.

[73] Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975).

[74] *Id.* at 605.

[75] *Id.* at 614.

[76] *Id.* at 634–35.

[77] Gooding v. Wilson, 405 U.S. 518, 520–21 (1978).

[78] *Id.* at 522.

[79] Houston v. Hill, 482 U.S. 451, 458 (1987).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

Court said in *NAACP v. Button*[80] that "[b]road prophylactic rules in the area of free expression are suspect. . . . Precision of regulation must be the touchstone in an area so closely touching our most precious freedoms."[81]

The function of the overbreadth doctrine "attenuates as the otherwise unprotected behavior that forbids the State to sanction moves from 'pure speech' towards conduct and that conduct—even if expressive—falls within the scope of otherwise criminal laws that reflect legitimate state interests in maintaining comprehensive controls over harmful constitutionally unprotected conduct."[82] Moreover, when a law is shown to punish a significant portion of protected expression compared to the statute's legitimate sweep, all enforcement of the law is invalidated unless the courts have narrowed its application.[83] Finally, as a plaintiff needs only to show "the threat of enforcement of an overbroad law may deter or 'chill' [protected expression]"[84] to challenge a law based on a claim of overbreadth; the traditional requirements for standing do not need to be met.[85]

B. Justiciability of Intelligence Gathering

Laird v. Tatum[86] is the leading Supreme Court case discussing political intelligence gathering. The suit was brought for declaratory judgment that Army's surveillance of 'lawful and peaceful civilian political activity' was unconstitutional and requested an injunction forbidding such surveillance.[87] However, the Court held that the plaintiffs failed to present a justiciable controversy by alleging that the mere existence and operation of the Army's intelligence-gathering and distributing system constituted a 'chilling' effect on their First Amendment rights.[88] The Court noted that the plaintiffs identified no specific evidence of unlawful surveillance activities against them but indicated that the government's principal sources of information were news media and publications in general circulation.[89]

---

[80] NAACP v. Button, 371 U.S. 415, 438 (1963).

[81] *Id*.

[82] Broadrick v. Oklahoma, 413 U.S. 601, 614 (1973).

[83] *See* Faustin v. City & Cnty. of Denver, Colo., 423 F.3d 1192 (10th Cir. 2005).

[84] Virginia v. Hicks, 539 U.S. 113, 119 (2003).

[85] *Broadrick*, 413 U.S. at 612.

[86] Laird v. Tatum, 408 U.S. 1 (1972).

[87] *Id.* at 2.

[88] *Id.* at 9.

[89] *Id.* at 6.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

However, *Laird*, while appearing to be "on-point," is in-fact factually dissimilar to the issues presented in this article. In that case, the Army deployed a large number of forces to read material that was substantially public in nature.[90] In fact, most of the reviewed material was acquired from newspaper articles.[91] With mobile devices, the acquisition and analysis of data is both automatic, requiring no human assets, and has not been publically published.

Given that the Supreme Court has not spoken beyond *Laird*, issues of standing will continue to present significant obstacles in cases alleging injury from surveillance. First, plaintiffs will need to show actual chilling effects due to surveillance.[92] Second, plaintiffs will be required to show a direct objective link between the chill and the governmental actions, and not their subjective state of mind.[93]

In *Smith v. Maryland*,[94] the Supreme Court held that people had "no legitimate expectation of privacy" in the telephone numbers they dialed because they *voluntarily conveyed* such information to the telephone companies.[95] In *Jones*, Justice Sotomayor expressed concern with this interpretation: "this approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[96] Indeed, third parties collect mobile device location data regularly while the device is in operation, and sometimes, even beyond the times when the user is actively using the mobile device.[97]

C. Balancing National Security and the First Amendment

The nexus of the government's interest in strong national security and their duty to preserve, protect, and defend the freedoms guaranteed by the First Amendment creates a web of difficult policy choices. Preservation of the security of the United States from its enemies, foreign and domestic, is a critical obligation of the government; in fact, it is one of the foremost reasons governments exist. At

---

[90] *Id.*

[91] *Id.*

[92] *See* Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionally of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMEND. L. REV. 234, 269 (2007).

[93] *Id.*

[94] Smith v. Maryland, 442 U.S. 735 (1979).

[95] *Id.* at 744.

[96] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[97] *See supra* Part I.B and associated footnotes.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

times, the pursuit of this important goal leads governmental agents to trespass in areas protected by the guarantees of expression.

The Foreign Intelligence Surveillance Act (FISA)[98] is perhaps the most visible tool used by government agents to acquire and analyze data outside of the typical channels of judicial review. Obtaining business records is expressly provided for under FISA.[99] These records are often obtained through the use of National Security Letters (NSLs) authorized by the USA Patriot Act.[100] The NSLs may be issued without oversight from courts, and they effectively function as administrative subpoenas that place an additional gag order on the recipient from disclosing even the existence of the demand.[101] Their use by law enforcement is widespread,[102] however, a recent court ruling[103] found the NSLs to be unconstitutional on First Amendment grounds, noting that the enabling legislation is "impermissibly overbroad and not narrowly tailored."[104]

III. THE NEXUS BETWEEN SURVEILLANCE AND EXPRESSIVE ASSOCIATION

Broad and sweeping surveillance programs[105] can infringe upon the freedom of association. Compared to the relatively brief intrusions that occurred in past cases,[106] the intrusion inflicted by prolonged electronic monitoring of mobile device location data is far more revealing. Additionally, the ultimate intrusion exacted by prolonged monitoring is greater than any other invasive police practice deemed to be a "search" by the Supreme Court. Because GPS monitoring is

[98] 50 U.S.C. §§ 1801–1885 (2006).

[99] 50 U.S.C. § 1861 (2006).

[100] 18 U.S.C. § 2709 (2006) (NSL enablement within the Stored Communications Act); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. No. 107-56, § 505, 115 Stat. 272 (2001).

[101] *My National Security Letter Gag Order*, WASH. POST (Mar. 23, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html.

[102] Lorenzo Franceschi-Bicchierai, *Google Releases First Data on National Security Letters*, MASHABLE (Mar. 5, 2013), http://mashable.com/2013/03/05/google-releases-data-on-nsls/; GOOGLE, *supra* note 38.

[103] *In re* Nat'l Sec. Letter, 2013 WL 1095417 (N.D. Cal. Mar. 14, 2013). *See also* Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006) (holding the nondisclosure provisions of an NSL themselves to be a First Amendment violation).

[104] *In re* Nat'l Sec. Letter, 2013 WL 1095417.

[105] *See supra* Part II.A.2 and associated footnotes.

[106] *See, e.g.*, *supra* Part II.B and associated footnotes.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

relatively cheap compared to "conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[107] Thus, "[a]wareness that the Government may be watching chills associational and expressive freedoms" and "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[108]

Moreover, "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical."[109] Furthermore, it was noted that if traditional methods had been used to achieve a similar result to the prolonged GPS monitoring in *Jones*, then large quantities of personnel, vehicles, time, and expenses would have been required. The best solution to circumstances involving significant developments in technology may be found through legislative action, as articulated by Justice Alito.[110]

IV. CONCERNS AND RECOMMENDATIONS

The recommendations discussed in this section are tailored to the challenges faced by the Federal Government; however, many of the same values can be directly translated to state and local levels of government.

A. Legislative Actions

Congress has the ability to amend existing laws to clarify when a governmental agent has the authority to obtain mobile device location data without prior judicial authorization.[111] Additionally, and perhaps more importantly, Congress has the authority to legislate on the topic directly, and specifically, Congress can limit the acquisition and analysis of mobile device location data.

[107] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 429 (2004)).

[108] *Jones*, 132 S. Ct. at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). For an argument that the use of GPS technology may also violate the First Amendment's right to association, see Courtney Burten, *Unwarranted! Privacy in a Technological Age: The Fourth Amendment Difficulty in Protecting Against Warrantless GPS Tracking and the Substantive Due Process and First Amendment Boost*, 21 S. CAL. INTERDISC. L.J. 359, 383 (2012).

[109] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

[110] *Id.* at 964 (Alito, J., concurring).

[111] *See generally* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313 (2012) (advocating the elimination of automatic gagging and sealing of surveillance orders).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

Certain efforts have been initiated.[112] These efforts should be embraced and enacted.

Congress should also create positions within executive agencies that routinely review the actions within their respective agencies to assure that the government agents are acting within their mandate so that the government can prevent the collection and analysis of mobile device location data of innocent people in this country.[113]

B. Executive Actions

The President of the United States, the Cabinet Secretaries, and the Agency Directors have broad discretion in deciding the policies, procedures, and methods used by their agents to gather mobile device location data. Here are a few examples of actions that can be reasonably taken by the Executive Branch.

The Department of Justice can direct the various law enforcement agencies within the department to limit their intake of mobile device location data to specific investigations with narrowly tailored objectives. It can end the "cell records data dumps" currently used that seek wide portions of location records, often sweeping in the data of innocent individuals otherwise free of suspicion.[114]

The FCC can announce guidelines[115] for mobile device network operators regarding the length of time records that should be kept, and advocate the deletion of records that no longer support the growth of cellular networks.

The Federal Trade Commission (FTC) has significant authority over the business conduct of both the telecommunications industry, as well as the third party application authors. The FTC should articulate the harms faced by the unauthorized use of mobile device location data, and develop transparent guidelines for the collection and storage of mobile device location data, including providing that data to the users who created it.[116]

---

[112] *See, e.g.*, Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2011); *reintroduced as* H.R. 1312, 113th Cong. (2013).

[113] Balkin, *supra* note 5, at 207.

[114] *See* ED MARKEY, *supra* note 40.

[115] These guidelines do not need to be mandatory regulations.

[116] *See, e.g.*, Megha Rajagopalan, *Cellphone Companies Will Share Your Location Data—Just Not With You*, PRO PUBLICA (June 26, 2012), http://www.propublica.org/article/cellphone-companies-will-share-your-location-data-just-not-with-you (noting that while telecommunications companies collect locational data, their users are often unable to see the scope of the data collection, or have access to the records).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu

C. Judicial Remedies

In the near terms, the courts will have little ability to directly confront the issue of the collection and use of mobile device location data by government agents. In addition to waiting until a case in controversy presents itself, when a case is actually posed to the court, the plaintiff will have to prove they have the standing to bring such a claim. This has proven difficult in past cases.

Traditional constitutional protections under the Fourth Amendment may be inadequate. Indeed, in the cases of the targets of foreign intelligence surveillance, Congress has limited the application of the Fourth Amendment through FISA.[117]

In cases similar to *Smith v. Maryland*, where courts are faced with records obtained from third parties, they should take a skeptical stance instead of blindly applying the Supreme Court's precedent.[118] Cases that involve significant collections of electronic data should be viewed as factually dissimilar to *Smith*, and thus subject to a different standard that requires direct judicial oversight.

CONCLUSION

Government agencies should be permitted to acquire and analyze mobile device location data for legitimate, limited investigations of criminal activity. Those activities should operate within a Fourth Amendment search regime, where a narrowly tailored warrant is granted by an independent, disinterested magistrate. All government programs that acquire and analyze mobile device location data which are not subject to a warrant requirement should face strict scrutiny review, where the government must show that the program supports a vital government interest and that the means chosen to further the compelling interest are the least restrictive to the freedoms of expression and association.

[117] Balkin, *supra* note 5, at 205.

[118] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.121 ● http://tlp.law.pitt.edu