Harvard Journal of Law & Technology
Volume 26, Number 2 Spring 2013

TRACKERS THAT MAKE PHONE CALLS: CONSIDERING FIRST AMENDMENT PROTECTION FOR LOCATION DATA†

*Andrew Crocker**

TABLE OF CONTENTS

---

† Winner of the biannual *Harvard Journal of Law & Technology* Prize for Outstanding Student Note.

* Harvard Law School, Candidate for J.D., 2013. Many thanks to Professor Susan Crawford for her wisdom and generosity in advising the paper that led to this Note, Ritu Gupta for her sharp-eyed and insightful editing, Michael Hoven, Nathan Lovejoy and the rest of the *Harvard Journal of Law & Technology* staff for improving my work, and to Z. Crocker for keeping me on my toes. All opinions and errors are the author's.

I. INTRODUCTION

On October 1, 2011, about fifteen hundred protesters from the Occupy Wall Street ("Occupy") encampment in Zuccotti Park in Lower Manhattan marched north and east onto the Brooklyn Bridge.[1] Police arrested more than seven hundred demonstrators for disorderly conduct, including Malcolm Harris, a blogger and prominent Occupy participant.[2] Harris planned to contest his charge by claiming that the police had "led or escorted" him and other protesters onto the roadway, but the prosecution claimed that tweets posted to Harris's Twitter account during the march contradicted this story.[3] In January 2012, the New York County Assistant District Attorney served Twitter with a grand jury subpoena compelling it to turn over Harris's tweets.[4] Twitter notified Harris of the order, and Harris's subsequent motion to quash the subpoena failed.[5] Harris later pled guilty after the tweets revealed that he had heard police warnings not to march in the road.[6]

Struggles between political activists and police, as well as difficulties in balancing First Amendment values against public safety and order, are not new.[7] The Occupy movement used largely traditional tactics of direct political engagement: noisy, physical occupation of public space, disruptive marches, and civil disobedience.[8] Yet the

1. Al Baker, Colin Moynihan & Sarah Maslin Nir, *Police Arrest More Than 700 Protestors on Brooklyn Bridge*, N.Y. TIMES (Oct. 1, 2011, 4:29 PM), http://cityroom.blogs.nytimes.com/2011/10/01/police-arresting-protesters-on-brooklyn-bridge.

2. *Id.*; Seth Ackerman, *VIDEO: #OWS, A Debate on Left Politics and Strategy*, JACOBIN (Oct. 19, 2011), http://jacobinmag.com/2011/10/video-ows-a-debate-on-left-politics-and-strategy-oct-14-in-nyc.

3. People v. Harris, 945 N.Y.S.2d 505, 512 (Crim. Ct. 2012); *see also* Malcolm Harris, *A Bridge to Somewhere*, NEW INQUIRY (Oct. 3, 2011), http://thenewinquiry.com/essays/a-bridge-to-somewhere (relating Harris's description of events on the bridge).

4. *Harris*, 945 N.Y.S.2d at 506.

5. *Id.* at 506, 511.

6. Russ Buettner, *A Brooklyn Protester Pleads Guilty After His Twitter Posts Sink His Case*, N.Y. TIMES, Dec. 13, 2012, at A31, *available at* https://www.nytimes.com/2012/12/13/nyregion/malcolm-harris-pleads-guilty-over-2011-march.html.

7. *See, e.g.*, Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 296 (1984) (holding regulation prohibiting camping in National Parks as applied to demonstrators served a substantial government interest and was narrowly tailored); Cox v. Louisiana, 379 U.S. 536, 552 (1965) (holding Louisiana breach of the peace statute unconstitutionally vague in cases involving large nonviolent protests).

8. *See* David Graeber, *Occupy and Anarchism's Gift of Democracy*, GUARDIAN (Nov. 15, 2011), http://www.guardian.co.uk/commentisfree/cifamerica/2011/nov/15/occupy-anarchism-gift-democracy (placing the Occupy movement in the history of direct democracy).

movement began with an online call to action,[9] and its message spread widely over the Internet as participants posted accounts of protests and shared grainy smartphone videos of alleged police misconduct.[10] In recent years, law enforcement has responded to this union of physical protest and networked communication with a dual strategy of its own: arrests and traditional crowd control tactics, coupled with an increased focus on monitoring and controlling communications devices and infrastructure.[11]

More troublingly, however, these sociopolitical movements are occurring against a backdrop of increased government surveillance, both online[12] and in the real world.[13] Recent press reports indicate that the Occupy movement was under surveillance as a part of federal counterterrorism investigations.[14] Individual Occupy participants further allege that police detained them to hamper their participation in the movement.[15] Using the rubric of "chilling effects," commentators have long recognized the risks that surveillance poses to robust political activity and free thought in a democratic society, as well as the

---

9. *Occupy Wall Street*, WIKIPEDIA, https://en.wikipedia.org/wiki/Occupy_Wall_Street (last visited May 9, 2012) (describing online origin of Occupy movement).

10. Radley Balko, *Tech-Savvy Occupy Protesters Use Cellphone Video, Social Networking to Publicize Police Abuse*, HUFFINGTON POST (Oct. 29, 2011, 7:49 PM), http://www.huffingtonpost.com/2011/10/29/occupy-protesters-armed-with-technology_n_1063706.html.

11. *See, e.g.*, Eva Galperin, *Cell Phone Guide for Occupy Wall Street Protesters (and Everyone Else)*, ELECTRONIC FRONTIER FOUND. (Oct. 14, 2011), https://www.eff.org/deeplinks/2011/10/cell-phone-guide-occupy-wall-street-protesters-and-everyone-else (offering advice for protesters whose cell phones are searched by police). In addition to arresting unruly individuals, authorities seeking to control protests have found it effective to simply undercut the communications infrastructure supporting mobile communications. *See* Andrew Dalton, *BART Called for (Possibly Illegal) Cell Phone Service Cutoff To Prevent Protests*, SFIST (Aug. 12, 2011, 4:25 PM), http://sfist.com/2011/08/12/bart_called_for_possibly_illegal_ce.php.

12. *See* Dana Priest & William M. Arkin, *A Hidden World, Growing Beyond Control*, WASH. POST, July 19, 2010, at A1, *available at* http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control (reporting that the National Security Agency intercepts 1.7 billion e-mails and other communications every day).

13. This buildup is nowhere more apparent than in Lower Manhattan, site of the September 11 attacks and the home of Occupy, where the New York City Police Department has installed thousands of surveillance cameras as part of the "Domain Awareness System." *See* Olivia J. Greer, Note, *No Cause of Action: Video Surveillance in New York City*, 18 MICH. TELECOMM. & TECH. L. REV. 589, 606 (2012) (discussing lack of legal challenge against video surveillance); Neal Ungerleider, *NYPD, Microsoft Launch All-Seeing "Domain Awareness System" with Real-Time CCTV, License Plate Monitoring*, FAST CO. (Aug. 8, 2012), http://www.fastcompany.com/3000272/nypd-microsoft-launch-all-seeing-domain-awareness-system-real-time-cctv-license-plate-monito.

14. Michael S. Schmidt & Colin Moynihan, *F.B.I. Counterterrorism Agents Monitored Occupy Movement, Records Show*, N.Y. TIMES, Dec. 25, 2012, at A18, *available at* https://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html.

15. *See* Colin Moynihan, *Wall Street Protesters Complain of Police Surveillance*, N.Y. TIMES, Mar. 12, 2012, at A17, *available at* https://www.nytimes.com/2012/03/12/nyregion/occupy-wall-street-protesters-complain-of-police-monitoring.html.

double-edged role played by technology.[16] The same technologies embraced by Occupy to spread its message — particularly smartphones — are easily susceptible to widespread, detailed information collection by law enforcement.[17] Speaking to a writer affiliated with Occupy, technologist and Wikileaks supporter Jacob Appelbaum commented, "Cell phones are tracking devices that make phone calls."[18] Cell phone tracking requires the collection of location data — information that can locate a device and its user in space and time. In recent years, scholars and some judges have contended that the Fourth Amendment and existing statutory law do not sufficiently constrain government collection and use of location data.[19] In particular, under the Electronic Communications Privacy Act ("ECPA"), the government routinely obtains location data through sealed, ex parte proceedings, sometimes without ever notifying affected individuals.[20]

While Fourth Amendment doctrine and the operation of ECPA make it difficult to challenge government collection of location data, such surveillance can chill political activity — particularly modern movements like Occupy, with their dual reliance on protesters' physical engagement and mobile, networked technology. This Note examines the present status of location data under the First Amendment,

---

16. For example, in *United States v. Jones*, Justice Sotomayor wrote, "Awareness that the Government may be watching chills associational and expressive freedoms. . . . The net result is that [surveillance like] GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)). Neil Richards has argued that surveillance harms the First Amendment's "constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy." Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. (forthcoming 2013) (manuscript at 18) *available at* http://ssrn.com/abstract=2239412. It does so by interfering with individuals' intellectual privacy, which Richards defines as the idea "that new ideas often develop best away from the intense scrutiny of public exposure [and] that people should be able to make up their minds at times and places of their own choosing." *Id.* at 13.

17. Geoffrey Ingersoll, *EXPERT: If You Were at Occupy Wall Street, Your Phone Was Probably Surveyed*, BUS. INSIDER (Sept. 24, 2012, 5:51 PM), http://www.businessinsider.com/steven-rambam-on-police-surveying-phones-2012-9. Police in the United States and abroad have used social networks to identify participants in real-world protests and riots. *See, e.g.*, Quinn Norton, *Boston D.A. Subpoenas Twitter over Occupy Boston, Anonymous*, WIRED THREAT LEVEL (Dec. 30, 2011, 4:00 PM), http://www.wired.com/threatlevel/2011/12/boston-subpoena-twitter (subpoena to Twitter to compel production of tweets and user information); Fred Petrossian, *Iranian Officials 'Crowd-source' Protester Identities*, GLOBAL VOICES (June 27, 2009, 5:28 PM), http://globalvoicesonline.org/2009/06/27/iranian-officials-crowd-source-protester-identities-online (crowdsourced identification of photos); *Vancouver Riot 2011: Help Identify Suspects*, VANCOUVER POLICE DEP'T, https://riot2011.vpd.ca (last visited May 9, 2013) (crowdsourced identification of CCTV photos).

18. Sarah Resnick, *Leave Your Cellphone at Home*, N+1, (Apr. 26, 2012), http://nplusonemag.com/leave-your-cellphone-at-home.

19. *See infra* Part III.

20. Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 321 (2012) (estimating more than 30,000 sealed ECPA proceedings in 2006).

focusing on scenarios derived from Malcolm Harris's prosecution for disorderly conduct in *People v. Harris*.[21] It argues that the collection of location data can be highly revealing of political activity and, under certain circumstances, can even constitute speech under the First Amendment.[22]

The argument proceeds in four parts. Part II describes the scope of location data and the various technical methods that law enforcement uses to obtain it. Part III discusses how ECPA and the Fourth Amendment apply to location data and presents commentators' criticisms of the current regime as a tool for heightened government surveillance. Part IV raises the possibility of affording First Amendment protection to location data and discusses how a court might evaluate such claims. Part V concludes.

II. THE USE OF LOCATION DATA IN SURVEILLANCE

Traditional police surveillance involved following individuals through public spaces in real time,[23] but law enforcement has become highly sophisticated at tracking suspects remotely. From using short-range "beeper" trackers[24] to specialized Global Positioning System ("GPS") devices placed on vehicles,[25] law enforcement increasingly employs techniques that can either be used to generate real-time, ongoing location data or to retroactively compile a suspect's movements over long periods of time.[26] This Part discusses the increase in law enforcement's access to location data from mobile devices, describes the forms this data can take, and places requests for location data in the broader context of law enforcement investigations.

---

21. People v. Harris, 949 N.Y.S.2d 590, 598 (Crim. Ct. 2012) (denying Twitter's motion to quash); People v. Harris, 945 N.Y.S.2d 505, 512–13 (Crim. Ct. 2012) (denying Harris's motion to quash).

22. *See infra* Part IV. *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007) (discussing application of First Amendment to government information gathering).

23. United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that the Fourth Amendment does not protect "[a] person traveling in an automobile on public thoroughfares" from ordinary police surveillance). This form of surveillance was constrained by "the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

24. *Knotts*, 460 U.S. at 277–78 ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.").

25. *Jones*, 132 S. Ct. at 948–49 (describing the government's use of a GPS device on a target's vehicle to monitor the vehicle's movements).

26. *See infra* Part II.B.

A. The Explosion in Cell Phone Surveillance

The most significant sources of location data are likely cell phones and other mobile, networked devices, including smartphones. This is due to the staggering growth in the public's use of these devices in the last five years.[27] As of December 2012, half of the adult population of the U.S. owned either a smartphone or a tablet with a connection to the Internet,[28] while nearly ninety percent of U.S. adults owned a cell phone.[29]

These devices generate a vast amount of data that resides in the hands of third parties — primarily mobile cell and Internet Service Providers ("ISPs") like AT&T and Verizon, as well as Online Service Providers ("OSPs") like Google and Twitter.[30] Under existing law, law enforcement officials can easily obtain such third-party data.[31] Recent reports generated in response to inquiries by Congress and civil liberties groups indicate that the government is taking advantage of this low bar,[32] leading to "an explosion in cellphone surveillance in the last five years."[33] As one measure, the major cell carriers reported receiving 1.3 million requests from law enforcement officials in 2011,[34] likely implicating millions of users' records. Even this measure of cell phone surveillance is underinclusive, however, since certain techniques do not generate comprehensive requests to cell providers. For example, a technology called an International Mobile Subscriber Identity catcher, commonly known as a "stingray," acts as a dummy cell tower, capturing information about any device within its

27. *Device Ownership*, PEW INTERNET, http://pewinternet.org/Trend-Data-%28Adults%29/Device-Ownership.aspx (last visited May 9, 2013).

28. Amy Mitchell et al., *The Explosion in Mobile Audiences and a Close Look at What It Means for News*, JOURNALISM.ORG (Oct. 1, 2012), http://www.journalism.org/analysis_report/future_mobile_news.

29. *Device Ownership*, *supra* note 27.

30. *Cell Phone Location Tracking Request Response — Cell Phone Company Data Retention Chart*, AM. CIVIL LIBERTIES UNION ("ACLU"), http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart (last visited May 9, 2013); *see also* Timothy B. Lee, *My Smartphone, the Spy: Protecting Privacy in a Mobile Age*, ARS TECHNICA (Mar. 14, 2012, 11:00 AM), http://arstechnica.com/business/2012/03/my-smartphone-the-spy-protecting-privacy-in-a-mobile-age.

31. *See infra* Part III.

32. *See* Press Release, Congressman Ed Markey, Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers (July 9, 2012), http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers; *Cell Phone Location Tracking Public Records Request*, ACLU (Sept. 10, 2012), http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request (reporting results of Freedom of Information Act requests on law enforcement agencies' use of cell phone tracking).

33. Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1.

34. *Id.*

range.[35] Thus, while a stingray can be used to find a single suspect, police may capture information about hundreds of unrelated individuals in the process. Though the extent of stingray usage is uncertain, the *Wall Street Journal* reported in 2011 that stingrays have been used by the FBI and at least a handful of local police departments.[36] An ACLU blogger even suggested that New York City police officials used a stingray to remotely capture information about Occupy participants' location and aggregate activities through their mobile devices.[37]

B. The Forms of Mobile Location Data

Mobile devices vary in complexity, but they are all fundamentally two-way radios that communicate wirelessly via fixed infrastructure.[38] Cell networks consist of interconnected radio base stations ("cell sites") that route traditional voice calls, text messages, and Internet data from cellular devices.[39] Cell sites detect signals from phones and other devices and periodically engage in an automatic "registration" process, "hand[ing] off" the device to other sites as the user moves.[40]

As a result, mobile devices generate data that can be used to locate them in space and time.[41] This location data may be grouped into two categories: (1) "historical" information resulting from normal cell network operation, and (2) real-time or "prospective" data from active surveillance.[42] Furthermore, when users of these devices participate in IP-based communications, including web browsing and e-mail, the devices leave IP address trails, which can also be used to infer location.

1. Historical Location Data

Because cell sites automatically collect data during normal usage, cellular providers accumulate logs ("call detail records")[43] linking

35. Linda Lye, *In Court: Uncovering Stingrays, a Troubling New Location Tracking Device*, ACLU (Oct. 22, 2012, 12:42 PM), http://www.aclu.org/blog/national-security-technology-and-liberty/court-uncovering-stingrays-troubling-new-location.

36. Jennifer Valentino-DeVries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL ST. J., Sept. 22, 2011, at A1, *available at* http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html.

37. Ingersoll, *supra* note 17.

38. *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 831 (S.D. Tex. 2010) [hereinafter *S.D. Tex. 2010 Cell Site Decision*]

39. *Id.* at 832.

40. This process occurs whether or not the device is in use. *Id.* at 831.

41. *See id.* at 833.

42. *See* Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 126 (2012); *see also S.D. Tex. 2010 Cell Site Decision*, *supra* note 38, at 833 (discussing automatic data collection by cell phone networks).

43. *S.D. Tex. 2010 Cell Site Decision*, *supra* note 38 at 833.

specific subscriber accounts, call and Internet connection data, and the nearest cell sector or base station.[44] These passively generated "historical" records can, at the least, be used to determine that a user is located within a certain radius of the cell site at a specific date and time.[45] However, as networks and phone technology have evolved, the logs have become increasingly detailed.[46] This additional detail is also driven by recent Federal Communication Commission ("FCC") rules that set increasingly stringent benchmarks for locating 911 calls placed from cell phones,[47] such that by 2016, first responders must be able to trace sixty-seven percent of 911 calls in all coverage areas to within one hundred meters.[48] Cell providers achieve this accuracy in part by increasing cell site density and triangulating users' positions from the geographic coordinates of two or three cell sites.[49] Termed historical cell site location information ("CSLI"),[50] this method can be quite accurate in determining a user's approximate location, depending on network density and the technique employed.[51] Although the FCC rules are intended to improve emergency response, cell providers' implementation of these requirements has had the side effect of giving law enforcement access to more accurate location information.[52]

Additional built-in technologies — foremost among them GPS hardware and associated software — can be used to locate users.[53] GPS can be even more accurate than cell site triangulation, tracing the location of a user's call to within ten meters under ideal conditions.[54] GPS location can be combined with the cell network location methods described above to provide further accuracy.[55]

---

44. Pell & Soghoian, *supra* note 42, at 128.

45. *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 702–03, 713 (2011).

46. *See* Pell & Soghoian, *supra* note 42, at 128.

47. 47 C.F.R. § 20.18(d)(1) (2012).

48. *See id.* § 20.18(h)(1)(i)(C).

49. Christopher Fox, Comment, *Checking In: Historic Cell Location Information and the Stored Communications Act*, 42 SETON HALL L. REV. 769, 776 (2012) (discussing "Angle of Arrival" and "Time Distance of Arrival" as two methods to determine the approximate location of a phone). Cell providers can also use smartphones' built-in GPS devices or a "blended" method of network triangulation and device-based location. *See* 47 C.F.R. § 20.18 (h)(1)(iv) (2012).

50. Fox, *supra* note 49, at 770.

51. *S.D. Tex. 2010 Cell Site Decision*, *supra* note 38, at 832–34; Pell & Soghoian, *supra* note 42, at 128.

52. Fox, *supra* note 49, at 777.

53. Pell & Soghoian, *supra* note 42, at 128–29.

54. Freiwald, *supra* note 45, at 713 n.199.

55. *See* 47 C.F.R. § 20.18(d)(1) (2012). In addition, services offered by Apple and Google can use a device's built-in Wi-Fi hardware to compare signal strength from nearby wireless access points to triangulate the device's location. Julia Angwin & Jennifer Valentino-DeVries, *Apple, Google Collect User Data*, WALL ST. J., Apr. 22, 2011, at B1, *available at* http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html; *Configure Access Points with Google Location Service*, GOOGLE MAPS, https://

When law enforcement knows the identity of the device or user it is looking for, it can request CSLI from providers for that device or user.[56] If, on the other hand, the identity of the suspect or device connected to criminal activity in a specific location is unknown, investigators may seek a "cell tower dump," in which providers are compelled to turn over information on all devices in the vicinity of a cell site in that location for a given period of time.[57]

2. Active, Prospective Location Data

Because cell providers are increasingly equipped to determine users' locations, law enforcement officers tracking a suspect can simply request this information from providers as they passively collect it from a user's device.[58] In addition, law enforcement officials can take advantage of the capabilities of mobile devices and cell networks to actively generate location data. For instance, they can ask providers to surreptitiously "ping" a device and request it to transmit location data back to the provider or directly to them.[59] In addition, officers in the field can even bypass providers to hone in on suspects by using and dynamically repositioning stingrays.[60]

3. IP Addresses and Location

Mobile users' locations can be determined from data generated specifically for this purpose — such as GPS and CSLI — and can be inferred with less accuracy from basic call detail records. Another type of general-use data that can be roughly translated to a user's location is an IP address — the numeric identifier associated with all Internet traffic, including traffic originating from mobile devices. OSPs such as Google and Yahoo, among others, routinely maintain logs of users' IP addresses and connection times.[61] IP addresses are

---

support.google.com/maps/bin/answer.py?hl=en&answer=1725632 (last visited May 9, 2013).

56. *See* Pell & Soghoian, *supra* note 42, at 128.

57. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), Nos. C-12-670M, C-12-671M, C-12-672M, C-12-673M, 2012 WL 4717778, at *1 (S.D. Tex. Sept. 26, 2012) (order denying the government's requests for cell tower dumps) [hereinafter *S.D. Tex. 2012 Decision*].

58. Pell & Soghoian, *supra* note 42, at 131.

59. *Id.* Law enforcement pinging of cell phones can be used to acquire cell site information, GPS data, or both. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012) (describing law enforcement's use of ping data to locate and track a drug suspect); Devega v. State, 689 S.E.2d 293, 299 (Ga. 2010) (describing law enforcement's use of pinging to obtain GPS data); Stone v. State, 941 A.2d 1238, 1244 (Md. Ct. Spec. App. 2008) (describing the pinging of appellant's cellphone, which revealed its location within a two-mile radius).

60. *See supra* notes 35–36 and accompanying text.

61. IP retention by OSPs varies by provider. *See* Nate Anderson, *Why Google Keeps Your Data Forever, Tracks You with Ads*, ARS TECHNICA (Mar. 8, 2010, 9:20 AM),

also included in e-mail headers.[62] Having obtained an IP address from website traffic or an e-mail, law enforcement can locate the associated user in several ways. First, because IP addresses are allocated to ISPs geographically, they can be translated with varying degrees of accuracy to a specific region using publicly available tools.[63] Second, although most ISPs assign IP addresses dynamically, they keep time-stamped records of which addresses are assigned to which subscribers.[64] Thus, law enforcement agents who know an individual's IP address can identify that individual by compelling production of an ISP's record of subscriber addresses.[65]

C. The Mosaic of Location Data

In 2010, the D.C. Circuit described Fourth Amendment concerns about law enforcement's prolonged use of location surveillance by invoking the concept of a mosaic pieced together from individual data points.[66] Extended use of a single tracking technology can create the mosaic (as in the D.C. Circuit's discussion of a GPS device placed on a suspect's car), or investigators can draw on many sources to form an overall picture.[67]

The facts of a recent case, *United States v. Rigmaiden*, demonstrate the latter concept of a mosaic and the evolving nature of loca-

---

http://arstechnica.com/tech-policy/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys.

62. The inclusion of IP addresses in e-mail headers depends on the provider and the client used to send the e-mail. Neal Ungerleider, *The Real Cyberforensics Used To Snoop on Petraeus (and You)*, FAST CO. (Nov. 14, 2012), http://www.fastcompany.com/3003061/real-cyberforensics-used-snoop-petraeus-and-you.

63. *See* IP LOCATION, http://www.iplocation.net (last visited May 9, 2013) (using IP addresses to generate geographical location information).

64. IP log retention times currently vary by provider. *See* Ernesto, *How Long Does Your ISP Store IP Address Logs?*, TORRENTFREAK (June 29, 2012), https://torrentfreak.com/how-long-does-your-isp-store-ip-address-logs-120629.

65. *See* Laura J. Tyson, Comment, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content To Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1284 (2010).

66. The D.C. Circuit described the "mosaic theory" as:

> Prolonged surveillance [that] reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. . . . A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.

United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in part sub nom*. United States v. Jones, 132 S. Ct. 945 (2012).

67. *See, e.g.*, Kim Zetter, *Public Buses Across Country Quietly Adding Microphones to Record Passenger Conversations*, WIRED THREAT LEVEL (Dec. 10, 2012, 4:46 PM), http://www.wired.com/threatlevel/2012/12/public-bus-audio-surveillance (describing correlation of municipal bus security cameras with GPS data to track passenger movements).

tion tracking as a component of traditional police work. In 2008, criminal investigators from the IRS, FBI, and USPS attempted to find a suspect they referred to as "the Hacker,"[68] who had been filing fraudulent tax returns in the names of deceased people.[69] The investigators successfully tracked IP addresses in e-mails between the Hacker and two confidential informants, leading them to traffic associated with online bank accounts opened under false names.[70] The IP addresses were registered to Verizon, and a subpoena showed that Verizon had assigned them to a single wireless broadband card.[71] From there, investigators tracked the broadband card through what agents called "historical cell tower information,"[72] later revealed to be a stingray device.[73] The stingray tracked the broadband card to an apartment building in Santa Clara, California.[74] Further investigation led police to raid an apartment, arresting Daniel Rigmaiden and seizing property, including the Verizon broadband card.[75]

Law enforcement agents seeking to track an individual's movements have a number of technological options. These techniques can involve obtaining complementary data from multiple third parties — as when an IP address associated with traffic at an OSP is traced to the assigning ISP and, if the user is connected via a mobile device, to cell site data. These techniques also range from being highly targeted (as with pings of individual devices), to extremely broad (as with cell site dumps and stingrays, which can sweep in hundreds of unrelated users). The widespread use of these techniques, particularly those involving untargeted collection, suggests that current legal constraints may be insufficient to prevent "dragnet" surveillance,[76] a concern taken up by the next Part.

---

68. Valentino-DeVries, *supra* note 36; *see* Kim Zetter, *Identity Thieves Filed for $4 Million in Tax Refunds Using Names of Living and Dead*, WIRED THREAT LEVEL (Apr. 8, 2010, 7:40 PM), http://www.wired.com/threatlevel/2010/04/fake-tax-returns.

69. An affidavit filed by an IRS Special Agent describes the steps leading to Rigmaiden's arrest. *See* Application and Affidavit for Seizure Warrant, *In re* the Seizure of the Entire Monetary Balance of the Prepaid Cards at The Bancorp Bank Identified in Attachment A1, (D. Ariz. Sept. 22, 2008) (No. 08-3397MB), *available at* http://www.wired.com/images_blogs/threatlevel/2010/04/rigmaiden-seizure-affidavit.pdf [hereinafter Rigmaiden Affidavit]; *see also* Zetter, *supra* note 67.

70. Rigmaiden Affidavit, *supra* note 69, at 13–15.

71. *Id.* at 12.

72. *Id.* at 32.

73. Valentino-DeVries, *supra* note 36.

74. Rigmaiden Affidavit, *supra* note 69, at 32.

75. *Id.* at 12; Kim Zetter, *Feds' Use of Fake Cell Tower: Did It Constitute a Search?*, WIRED THREAT LEVEL (Nov. 3, 2011, 5:46 PM), http://www.wired.com/threatlevel/2011/11/feds-fake-cell-phone-tower.

76. United States v. Knotts, 460 U.S. 276, 284 (1983); *see also* United States v. Pineda-Moreno, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc) ("When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say

III. LOCATION DATA AND GAPS IN CONSTITUTIONAL AND STATUTORY PRIVACY LAW

Following the contributions of other commentators, judges, and industry and civil liberties coalitions, this Note contends that neither the Fourth Amendment nor statutory law covering law enforcement acquisition of location data has been sufficient to limit the potential harms of overbroad surveillance described in Part I. Commentators have suggested legislative fixes or modifications to Fourth Amendment doctrine.[77] While these fixes might address the structural problems with the law, they do not squarely address First Amendment concerns, which are analyzed in Part IV. The most salient aspects of the gaps in constitutional and statutory protections for such surveillance are addressed below.[78]

A. Location Data and the Problems of ECPA

The primary statute governing surveillance of communications networks, including location data, is the Electronic Communications Privacy Act ("ECPA") of 1986.[79] Under ECPA, the government may seek orders to compel providers to turn over the contents of wire, oral, and electronic communications and related records.[80] With respect to location data, critics have identified two structural problems with ECPA: (1) the frequency with which the government obtains orders under inconsistent (and relatively undemanding) standards, and (2) the secrecy and lack of review surrounding these orders. These problems are discussed in turn.

1. The Fractured Regime of D and Hybrid Orders and Subpoenas

ECPA presents the government with an array of legal authorities when it seeks to compel data from providers, depending on whether a communication is prospective or retrospective and whether the infor-

---

that 'such dragnet-type law enforcement practices' are already in use." (quoting *Knotts*, 460 U.S. at 284)).

77. *See* Pell & Soghoian, *supra* note 42, at 181–93 (proposing legislative changes); *About the Issue*, DIGITAL DUE PROCESS COALITION, http://digitaldueprocess.org (last visited May 9, 2013) (advocating ECPA reform). *See generally* Freiwald, *supra* note 45 (arguing for Fourth Amendment protection for location data).

78. A complete discussion of the gaps in statutory and constitutional protections is beyond the scope of this Note.

79. ECPA has three parts, each covering a distinct topic: wiretaps, 18 U.S.C.A. §§ 2510–2522 (2013); access to stored communications, 18 U.S.C.A. §§ 2701–12 (2013); and pen register trap and trace devices, 18 U.S.C. §§ 3121–27 (2006 & Supp. V 2012). For a summary of ECPA's authorities, see generally CHARLES DOYLE, CONG. RESEARCH SERV., R41733, PRIVACY: AN OVERVIEW OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (2012), *available at* www.fas.org/sgp/crs/misc/R41733.pdf.

80. ORIN S. KERR, COMPUTER CRIME LAW 448–49 (2006).

mation obtained is the "content" of a communication.[81] Because ECPA was enacted before cell site and GPS location technologies matured,[82] it is unclear which authorities apply and under which standard — probable cause, reasonable suspicion, or something else — the government may seek orders for data obtained using these technologies.[83]

For the categories of both historical and prospective cell site location data, Stephanie Pell and Chris Soghoian explain that the Department of Justice's ("DOJ") standard practice has been to seek orders based on reasonable suspicion[84] unless seeking "more precise" location information (such as GPS data), for which it sometimes seeks a warrant based on probable cause.[85] For historical location data, DOJ usually seeks an order under 18 U.S.C. § 2703(d) ("D Orders") for "a record or other information pertaining to a subscriber or customer."[86] For prospective data, the DOJ also seeks a § 2703 D Order and additionally requests a "Pen/Trap Order" under § 3123, which covers non-content "dialing, routing address or signaling information," creating a so-called "Hybrid Order."[87] Stingrays have at times been authorized under Hybrid Orders,[88] but discussion of stingrays in the press has

81. *Id.* at 450 (explaining that "content" is the substance of a communicated message, while "non-content" information is the information that is used in delivering a message. For example, the content of a telephone call is the conversation itself, while other factors, such as call duration and phone numbers, are non-content information).

82. *See supra* Part II.

83. Pell & Soghoian, *supra* note 42, at 134–35. The Communication Assistance for Law Enforcement Act ("CALEA"), passed in 1994, complicates this analysis by providing that "any information that may disclose the physical location of a subscriber" may not be acquired "solely pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2) (2006); *see also In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313–14 (3d Cir. 2010) [hereinafter *Third Circuit Opinion*] (analyzing legislative history of CALEA in context).

84. There are two relevant statutory standards. To obtain stored communications and records, investigators must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2006 & Supp. V 2012). To obtain a Pen and Trap Order, investigators must demonstrate that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1) (2006). DOJ interprets the "specific and articulable facts" requirement as equivalent to the Supreme Court's *Terry* reasonable suspicion standard. Pell & Soghoian, *supra* note 42, at 152.

85. Pell & Soghoian, *supra* note 42, at 141. However, this policy is inconsistently applied. *See* Orin Kerr, *Looking into the Record of* United States v. Skinner*, the Sixth Circuit Phone Location Case*, VOLOKH CONSPIRACY (Aug. 17, 2012, 2:53 AM), http://www.volokh.com/2012/08/17/looking-into-the-record-of-united-states-v-skinner-the-sixth-circuit-phone-location-case (noting that in *United States v. Skinner*, DOJ obtained a Hybrid Order for GPS data).

86. 18 U.S.C. § 2703(c) (2006 & Supp. V 2012).

87. *Id.* § 3123 (2006). The Hybrid Order strategy is the result of DOJ's interpretation of CALEA. *See* Pell & Soghoian, *supra* note 42, at 135–36.

88. *See, e.g.*, *In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, No. C-12-534M, 2012 WL

fueled debate over the appropriateness of such authorization.[89] Some magistrate judges have disagreed with DOJ's interpretation and have required a higher showing — probable cause[90] — for both historical[91] and prospective data.[92]

Finally, it is worth noting that § 2703 also allows the government to obtain stored communications and some so-called "basic subscriber information," including "connection records, or records of session times and durations" and "any temporarily assigned network address," including IP addresses, using only a subpoena and without resort to a court order.[93] In *Rigmaiden*, the government used a grand jury subpoena to link IP addresses to the subscriber information for a broad-

212049, at *1 (S.D. Tex. June 2, 2012) (describing and denying hybrid order request for use of a stingray) [hereinafter *S.D. Tex. Stingray Decision*]. In *Rigmaiden*, the government apparently obtained a Hybrid Order and a search warrant, although the scope of this warrant is disputed. *See* Hanni Fakhoury & Trevor Timm, *Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About*, ELEC. FRONTIER FOUND. (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy (discussing uncertainty in the standards for using a stingray).

89. Valentino-DeVries, *supra* note 36.

90. In the case of historical data, two federal appellate courts have considered whether magistrate judges have discretion under the statute to require a higher probable cause showing. *See Third Circuit Opinion*, *supra* note 83 at 315 (finding that judges do have this discretion). The Fifth Circuit is currently considering this issue on appeal from the *S.D. Tex. 2010 Cell Site Decision*. *See* Chris Soghoian, *Tuesday: Federal Appeals Court Hears Important Cell Phone Tracking Case*, ACLU (Oct. 1, 2012, 3:05 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/tuesday-federal-appeals-court-hears-important-cell.

91. These decisions are motivated both by increasing precision of location data as described in Part III and subsequent Fourth Amendment decisions. *See S.D. Tex. 2010 Cell Site Decision*, *supra* note 38, at 830 (describing developments and denying D Order application based on Fourth Amendment); *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 589–90 (E.D.N.Y. 2010) (discussing precision in light of D.C. Circuit's decision in United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)); *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008) (reading legislative history to require probable cause warrant), *vacated*, *Third Circuit Opinion*, *supra* note 83, at 304.

92. *See* Pell & Soghoian, *supra* note 42, at 137–38 (explaining that the statutory construction of ECPA has led these courts to conclude that a warrant is required, either because Federal Rule of Criminal Procedure 41 requires a warrant application or because this data is akin to a tracking device under 18 U.S.C. § 3117); *see also In re* Application of the United States for an Order Authorizing the Installation and Use of a Pen Register, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006) (finding a lack of evidence that Congress intended to create a "sliding scale pairing mechanism" for ordering disclosures and thus denying the Government's request for an order compelling the production of cell site data); *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 321–22 (E.D.N.Y. 2005) (akin to tracking device and Rule 41 construction); *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005) (request akin to a tracking device under § 3117). *But see In re* Application of the United States for an Order for Disclosure of Telecomms. Records, 405 F. Supp. 2d 435, 437–38 (S.D.N.Y. 2005) (distinguishing information sought from S.D. Tex. and E.D.N.Y. cases).

93. *See* 18 U.S.C. § 2703(c) (2006 & Supp. V 2012).

band card, prompting the use of a stingray.[94] In *Harris*, the prosecution initially issued a subpoena to Twitter for both subscriber information and stored communications (i.e. tweets) and then sought a D Order after Twitter's opposition to the subpoena.[95] As Judge Sciarrino noted in an earlier proceeding, "the legal threshold for issuing a subpoena is low."[96] The productive use of subpoenas in both cases suggests that subpoenas are an important tool in obtaining general-purpose data like IP addresses, which can then be used to obtain more precise location information through the methods described in Part II.

In brief, the inconsistent and increasingly fractured standards for obtaining location data under ECPA have led commentators and civil liberties groups to bemoan the state of the law and call for judicial and legislative reform. Courts could require probable cause,[97] or Congress could add language codifying the forms of location data and clarifying more specific application of ECPA authorities.[98]

2. "[T]he most secret court docket in America"[99]

Perhaps even more troubling than ECPA's fractured legal regime is its secrecy. Through a combination of delayed notice[100] to targets of investigation, gag orders on telecommunications providers, and indefinitely sealed judicial orders, "it is as if [ECPA surveillance orders] were written in invisible ink,"[101] according to Magistrate Judge Stephen Smith. As Judge Smith explains, subscribers, who would have the most incentive to challenge ECPA orders, are usually precluded from doing so by ECPA's notice and secrecy provisions. As a result, a person whose location data is obtained via an ECPA order may only find out about this collection if it is associated with a criminal charge,

---

94. *See supra* notes 69–75 and accompanying text. *See* Rigmaiden Affidavit, *supra* note 69, at 12.

95. People v. Harris, 949 N.Y.S.2d 590, 591–92 (Crim. Ct. 2012).

96. People v. Harris, 945 N.Y.S.2d 505, 512 (Crim. Ct. 2012). *See generally* Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J.L. & TECH. 543, 543–62 (2011) (discussing the far-reaching scope of subpoenas in digital searches).

97. *See* Freiwald, *supra* note 45, at 748–49. *But see* Fox, *supra* note 49, at 773 (arguing that historic CSLI should not be protected by the Fourth Amendment).

98. *See supra* note 77.

99. Smith, *supra* note 20, at 313.

100. Under a D Order, the government can seek a "delay" or an indefinite "preclusion of notice" upon determining that one of several "adverse result[s]" will result from notification to the subscriber. 18 U.S.C. § 2705 (2006). Notice is not required at all when the government obtains the content of stored communications. *See* 18 U.S.C. § 2703(b)(1)(B) (2006 & Supp. V 2012). Similarly, Pen/Trap Orders actually require that providers "*not* disclose the existence of the pen register or trap and trace device . . . to the listed subscriber, or to any other person, unless or until otherwise ordered by the court" (emphasis added). 18 U.S.C. § 3123(d)(2) (2006). *See also* Smith, *supra* note 20, at 324–25.

101. Smith, *supra* note 20, at 314. Judge Smith estimates that there were 30,000 sealed ECPA orders in 2006 alone. *Id.* at 321–22.

as in *Rigmaiden*; those whose data is collected inadvertently may never know.[102] For criminal defendants, this notification is often irrelevant anyway, because ECPA has no suppression remedy.[103] Meanwhile, statutory guidelines often bar telecommunications providers and OSPs from notifying the subscriber, and providers usually lack the incentive to challenge the requests made by law enforcement themselves.[104] One notable exception is Twitter, which has taken the position that it will notify subscribers unless barred by law.[105] However, at least with respect to location data, cell providers are far more important players, and they have been notoriously secretive about law enforcement requests.[106] As a result, Judge Smith and others have suggested changes to bring transparency to ECPA.[107] The status quo, however, is that law enforcement seeks most location data under the relatively low reasonable suspicion standard, largely in secret, and without appellate review.[108]

B. Location Data and the Fourth Amendment

1. *United States v. Jones*

Application of the Fourth Amendment to location data is far from uniform, and the lack of judicial guidance has provoked criticism from commentators and civil liberties groups.[109] Until its 2012 ruling in *United States v. Jones*, the Supreme Court had never held that sur-

102. *Id.* at 330. Of course, notification during an investigation may undermine law enforcement's interests, but Smith notes that most subscribers are not notified even after the investigation concludes. *Id.*

103. KERR, *supra* note 80, at 450.

104. This leaves the government as the only party with a meaningful opportunity to appeal; however, it has little incentive to do so since government requests denied at the magistrate or district court level do not create binding precedent. Smith, *supra* note 20, at 327–28. The result is no judicial oversight of a complex, frequently used, and potentially invasive statute. *Id.* at 331.

105. *Guidelines for Law Enforcement*, TWITTER HELP CENTER, https://support.twitter.com/articles/41949-guidelines-for-law-enforcement#section5 (last visited May 9, 2013). Twitter has itself challenged high-profile subpoenas. *See* Somini Sengupta, *Twitter's Free Speech Defender*, N.Y. TIMES, Sept. 3, 2012, at B1, *available at* https://www.nytimes.com/2012/09/03/technology/twitter-chief-lawyer-alexander-macgillivray-defender-free-speech.html.

106. Trevor Timm, *Law Enforcement Agencies Demanded Cell Phone User Info Far More Than 1.3 Million Times Last Year*, ELECTRONIC FRONTIER FOUND. (July 9, 2012), https://www.eff.org/deeplinks/2012/07/law-enforcement-agencies-demanded-cell-phone-user-info-much-more-13-million-times.

107. *See, e.g.*, Smith, *supra* note 20, at 331–36 (describing a three-part proposal to: (1) provide notice to targets of ECPA orders, (2) open court orders for public view, and (3) provide statistics on ECPA surveillance orders to Congress).

108. *Id.* at 330–32; *see supra* Part III.A.1.

109. *See, e.g.*, Freiwald, *supra* note 45, at 682–83; Catherine Crump, *ACLU Asks Appeals Court To Reconsider Cell Phone Tracking Decision*, ACLU (Sept. 5, 2012, 2:22 PM), http://www.aclu.org/blog/technology-and-liberty/aclu-asks-appeals-court-reconsider-cell-phone-tracking-decision.

veillance of a person on public streets could constitute a search under the Fourth Amendment.[110] In *Jones*, the Court unanimously held that the installation and use of a GPS tracker on the defendant's car for twenty-eight days constituted a search, but it did not rule on whether a warrant was required for this search because that issue was not raised on appeal.[111] Although the ruling in *Jones* marks a significant change to Fourth Amendment doctrine, whether it applies to mobile location data — described in Part II — is unclear because the Court's reasoning was divided.[112] Justice Scalia's majority opinion relied on the *physical* trespass to the defendant's car in the installation of the GPS tracker, while a different five-justice coalition — including Justices Alito and Sotomayor — held that the use of the tracker violated the reasonable-expectation-of-privacy test derived from *Katz v. United States*.[113] None of the methods of obtaining location data described in Part II involve a physical trespass; hence, they would not constitute "searches" under Scalia's analysis.[114] The use of CSLI or prospective location data likely constitutes a search under the reasonable-expectation-of-privacy analysis favored by Justices Alito and Sotomayor, but only if it reveals an individual's "every single movement . . . for a very long period" of time.[115] Furthermore, a warrant would not necessarily be required to conduct this search.[116]

2. The Third-Party Doctrine

Location data may fall outside the Fourth Amendment's protection against unreasonable searches for another reason — the so-called "Third-Party Doctrine,"[117] which holds that some information voluntarily supplied to third parties, such as business records, is not protect-

110. *See* 132 S. Ct. 945, 948, 954 (2012). In *United States v. Karo*, however, the Court ruled that surveillance that revealed people's movements in the home, "a location not open to visual surveillance," constituted an unreasonable search without a warrant. 468 U.S. 705, 714 (1984). This is likely why DOJ policy was to seek a warrant for precise location data, such as GPS data, obtained from cell phones even prior to the *Jones* decision, though this policy was not uniformly applied. *See supra* note 85.

111. *Jones*, 132 S. Ct. at 954.

112. *See* United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012) ("*Jones* does not apply to Skinner's case because, as Justice Sotomayor stated in her concurrence, 'the majority opinion's trespassory test' provides little guidance on 'cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property.").

113. *See Jones,* 132 S. Ct. at 949; *id.* at 957–64 (Alito, J., concurring) (putting forth reasonable-expectation-of-privacy analysis); *id.* at 955 (Sotomayor, J., concurring) (agreeing in part with Alito's concurrence). For the genesis of the reasonable-expectation-of-privacy test, see *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

114. *See Skinner*, 690 F.3d at 779–80.

115. *Jones*, 132 S. Ct. at 964.

116. *See Skinner*, 690 F.3d at 779.

117. *See generally* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (describing function of the Third-Party Doctrine).

ed by the Fourth Amendment.[118] Many courts considering the use of cell site data have held that it is beyond the reach of the Fourth Amendment.[119] In *Harris*, for example, Judge Sciarrino relied, in part, on the Third-Party Doctrine, which he found defeated Harris' reasonable expectation of privacy in the tweets and associated user data, when denying Twitter's motion to quash the subpoena.[120] Meanwhile, in *Rigmaiden*, the prosecution did not preserve the information obtained from the stingray, making a constitutional analysis difficult.[121] Other courts have sidestepped the constitutional question by focusing on statutory authority, but the Third Circuit and a growing number of magistrate judges, including Judge Smith, have questioned the appropriateness of the Third-Party Doctrine.[122] Thus, because of the current flux in these decisions in various jurisdictions, the application of the Fourth Amendment to location data is imprecise at best and nonexistent at worst.[123]

IV. CONSIDERING FIRST AMENDMENT PROTECTIONS FOR LOCATION DATA

The gaps in Fourth Amendment doctrine and ECPA's fractured, secret standard for obtaining location information leave few options for those who seek to rein in location tracking. In the meantime, a few subscribers[124] and civil liberties groups[125] have begun to suggest that

118. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

119. *Skinner*, 690 F.3d at 779; United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012); Orin Kerr, *Two District Court Rulings That Cell-Site Data Not Protected Under the Fourth Amendment*, VOLOKH CONSPIRACY (Sept. 6, 2012, 1:41 PM), http://www.volokh.com/2012/09/06/two-district-court-rulings-that-cell-site-data-not-protected-under-the-fourth-amendment.

120. People v. Harris, 945 N.Y.S.2d 505, 508 (Crim. Ct. 2012).

121. Valentino-DeVries, *supra* note 36.

122. *See supra* notes 90–92; Justice Sotomayor noted in *United States v. Jones* that:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.

132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

123. Somini Sengupta, *Courts Divided over Searches of Cellphones*, N.Y. TIMES, Nov. 26, 2012, at A1, *available at* https://www.nytimes.com/2012/11/26/technology/legality-of-warrantless-cellphone-searches-goes-to-courts-and-legislatures.html.

124. *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 127 (E.D. Va. 2011) [hereinafter *E.D. Va. Opinion*].

125. Brief for ACLU et al. as Amici Curiae Supporting Appellants at 23, People v. Harris, 949 N.Y.S.2d 590 (Crim. Ct. 2012) (No. 2011NY080152), *available at* https://www.eff.org/sites/default/files/filenode/2012.08.27amicusbrief.pdf [hereinafter Harris Twitter Appeal Amici Brief].

the First Amendment might be implicated in certain criminal cases where the government seeks to obtain and use location data. However, these arguments have been largely subordinate to claims based on the Fourth Amendment and ECPA, and courts have not considered them at length, if at all.[126] This Part aims to develop a more in-depth analysis of potential First Amendment applications to location data and to explain how these arguments may play out in reality. First, it describes and adapts Daniel Solove's theory applying the First Amendment to criminal procedure.[127] Next, it notes limitations to this analysis. Finally, informed by Solove's conceptual approach and these caveats, it suggests novel First Amendment claims for the protection of location data and how a court evaluating *Harris* could address them.

A. Solove's Argument for First Amendment Limitations to Information Gathering

In his 2007 article, *The First Amendment as Criminal Procedure*, Professor Daniel Solove notes an evolution in the relationship of the First and Fourth Amendments.[128] The Fourth Amendment has traditionally had far greater impact on law enforcement activity because its protection against unreasonable search and seizure traditionally safeguards the physical embodiments of First Amendment activity — papers, books, and pamphlets — which are often located in protected, private places.[129] However, Solove notes that the rise in digital storage of personal information by third parties like ISPs and OSPs, and lower courts' application of the Third-Party Doctrine, means that the Fourth Amendment has limited applicability to such information.[130]

Instead, Solove argues that courts should draw on First Amendment precedent to find an independent basis to protect such digital data from "intrusive government information gathering."[131] Solove locates these protections in several lines of Supreme Court First Amendment cases, including protections for expressive association recognized in *NAACP v. Alabama,*[132] the recognition of anonymous

126. *E.D. Va. Opinion*, *supra* note 124, at 146.

127. *See generally* Solove, *supra* note 22.

128. *Id.* at 118–19.

129. *Id.* at 113–14, 126.

130. *Id.* at 125–26 (noting that law enforcement can obtain much information about First Amendment activities via subpoena).

131. *Id.* at 132. Solove is not alone in making these claims. *See* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 748 (2008) (arguing that the First Amendment provides "an additional check . . . on overreaching relational surveillance potential" beyond the Fourth Amendment's protections).

132. 357 U.S. 449, 460 (1958).

speech rights in *Talley v. California*[133] and *McIntyre v. Ohio Elections Commission*,[134] as well as precedent relating to the surveillance of political activities,[135] the receipt of information,[136] and subpoenas to the press.[137]

In assessing whether law enforcement collection of information impinges on these First Amendment protections, Solove suggests a court ask two questions: (1) whether the information collection affects activities protected by the First Amendment, and (2) whether it has a chilling effect on these activities.[138] When confronted with law enforcement information-gathering that chills First Amendment activity, Solove proposes a test adapted from the Supreme Court's familiar strict scrutiny inquiry: (1) whether the government has a significant interest in the information and (2) whether the government's request is narrowly tailored to achieve that interest.[139] Where the information at issue is associated with a criminal investigation, Solove contends, the probable cause standard for obtaining warrants should be imported from the Fourth Amendment, such that law enforcement officials would have to apply for "First Amendment warrant[s]."[140] The exclusionary rule would ordinarily be applied to any such information gathered without a warrant.[141] Where there is no criminal investigation, and a litigant instead claims that surveillance is overbroad, Solove envisions courts fashioning injunctive or other equitable relief to narrow the surveillance.[142]

B. Challenges to the First Amendment Criminal Procedural Approach

1. The Creation of New Criminal Procedure?

Solove acknowledges that his argument faces procedural obstacles,[143] and to date, courts have not adopted this idea of an independ-

133. 362 U.S. 60, 64 (1960).

134. 514 U.S. 334, 342 (1995).

135. *See, e.g.*, Laird v. Tatum, 408 U.S. 1, 2 (1972) (considering First Amendment objection to Department of Army program that monitored domestic political groups).

136. *See, e.g.*, Stanley v. Georgia, 394 U.S. 557, 564 (1969) (holding that the Constitution protects rights to receive information).

137. *See, e.g.*, Branzburg v. Hayes, 408 U.S. 665 (1972) (rejecting First Amendment reporter's privilege).

138. Solove, *supra* note 22, at 151–52. Solove argues that the Court's guidance on the values protected by the First Amendment should be used to prevent "unduly limiting government information gathering." *Id.* at 154. Thus, activities that "implicate belief, discourse, or relationships of a political, cultural, or religious nature" should be protected from surveillance, whereas activities implicating unprotected or low-value speech should likely not be. *Id.* at 153.

139. *Id.* at 159. Only if these two criteria are satisfied should courts uphold the activity.

140. *Id.* at 161.

141. *Id.* at 164.

142. *Id.* at 165.

143. *Id.* at 162–63.

ent First Amendment warrant requirement. Yet in several of the First Amendment cases upon which Solove relies, particularly those involving anonymous speech and associational privacy, courts have fashioned heightened scrutiny requirements for subpoenas, quashing those that do not meet the higher bar.[144] While it might seem farfetched to imagine a lower court fashioning entirely new procedural requirements, it is more plausible for a court to apply established First Amendment precedent to analogous facts. This is the approach taken by the defendants and civil liberties groups that have attempted to challenge government requests for information using subpoenas and D Orders on First Amendment grounds.[145] Thus, implicit in Solove's argument is an acknowledgement that such a procedural requirement would develop on a case-by-case basis as courts consider litigants' First Amendment claims. Moreover, since the government can always choose to seek a warrant based on probable cause, courts can deny requests for location data that implicate First Amendment values while falling short of the probable cause threshold and grant those requests that meet the standard.

2. Notice, Standing, and the Overbroad Collection of Location Data

One of the significant gaps in the operation of ECPA is the regularity with which orders are sealed, such that subscribers whose information is accessed are not given timely notice, if given notice at all, to challenge the issuance of an order.[146] This is particularly true with respect to the collection of location data that implicates many people, as well as with cell site dumps and the use of stingrays. Individuals whose location data is accessed but who are not criminally charged may have no knowledge, and thus no opportunity, to challenge its acquisition.[147] Even individuals who are prosecuted based on location data can only challenge the use of this data to the extent that existing law provides a remedy.[148] For this reason, the reforms to

144. *See, e.g.*, Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 545 (1963) ("When, as in this case, the claim is made that particular legislative inquiries and demands [i.e. subpoenas] infringe substantially upon First and Fourteenth Amendment associational rights of individuals, the courts are called upon to, and must, determine the permissibility of the challenged actions . . . ."); *In re* First Nat'l Bank, Englewood, Colo., 701 F.2d 115, 118–19 (10th Cir. 1983) (granting an evidentiary hearing for a subpoena sub duces tecum that petitioners claimed would infringe First Amendment association rights).

145. *E.D. Va. Opinion*, *supra* note 124, at 145–46 (rejecting free association claim); Harris Twitter Appeal Amici Brief, *supra* note 125, at 22–23 (invoking *Gibson* and *McIntyre* to argue that Harris's tweets were entitled to First Amendment protection).

146. *See supra* Part III.A.2.

147. Fakhoury & Timm, *supra* note 88.

148. ECPA provides no suppression remedy. *See* KERR, *supra* note 80, at 450. Even when location data is protected by the Fourth Amendment, a good faith exception may apply. *See* United States v. Jones, No. 05-0386 (ESH), 2012 WL 6443136, at *9 (D.D.C. Dec. 14, 2012) (holding that good faith exception recognized by the Supreme Court in Da-

ECPA's notification and sealing regime suggested by Judge Smith and others are a crucial step toward addressing the First Amendment concerns raised by location data.[149]

Even with sufficient notice, however, an individual who seeks to challenge the collection of location data may be barred by standing doctrine. This is partially the result of a line of cases on government surveillance beginning in 1972 with *Laird v. Tatum*.[150] In *Laird*, the Court held that a Department of the Army program in which agents attended domestic political groups' public meetings and took notes did not interfere with the groups' rights because the groups failed to show that the program had a "chilling effect" to their activities.[151] Emphasizing that it was ruling on "narrow" standing grounds,[152] the Court found that chilling effects do not arise from the "mere existence, without more, of a governmental investigative and data-gathering activity."[153] Instead, it required "a claim of specific present objective harm or a threat of specific future harm."[154]

Some lower courts have interpreted *Laird* as a high bar to claims that surveillance chills First Amendment activity, requiring that plaintiffs must, in the words of then-Judge Scalia, "suffer[] some concrete harm (past or immediately threatened) *apart from* the 'chill' itself," such as denial of admission to the bar or termination of employment.[155] Others, however, have held that where plaintiffs can produce evidence of a chill — for example, through decreased membership or attendance at meetings[156] — or where surveillance necessitates "specific, reasonable actions" made at "tangible, economic cost, in order to carry out . . . legitimate professional activities,"[157] *Laird*'s standing requirements can be satisfied.

---

vis v. United States, 131 S. Ct. 2419, 2427–28 (2011), applies to acquisition of cell site data).

149. *See* Smith, *supra* note 20, at 331–36; *see also supra* text accompanying note 107.

150. 408 U.S. 1 (1972).

151. *Id.* at 13–14. The Court noted that the information gathered was "nothing more than a good newspaper reporter would be able to gather by attendance at public meetings and the clipping of articles from publications available on any newsstand." *Id.* at 9 (quoting Tatum v. Laird, 444 F.2d 947, 953 (D.C. Cir. 1971)).

152. *Id.* at 15.

153. *Id.* at 10. The Court elaborated that a chilling effect did not arise "merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual." *Id.* at 11.

154. *Id.* at 14.

155. United Presbyterian Church in the U.S.A. v. Reagan, 738 F.2d 1375, 1378 (D.C. Cir. 1984) (emphasis added); *see also* ACLU v. NSA, 493 F.3d 644, 660 (6th Cir. 2007) ("I cannot subscribe to a view that the reason the injury in *Laird* was insufficient was because the plaintiffs alleged 'only' chilled speech and that, by something 'more,' the *Laird* Court meant more subjective injury or other injuries that derive from the chilled speech.").

156. Presbyterian Church (U.S.A.) v. United States, 870 F.2d 518, 522 (9th Cir. 1989).

157. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 147 (2d Cir. 2011), *cert. granted*, 132 S. Ct. 2431 (2012), *rev'd* Clapper v. Amnesty Int'l, No. 11-1025, 2013 WL 673253, at *8

Since Solove's framework incorporates a chilling effects inquiry, to survive *Laird*, litigants would need to make a sufficient showing of present or prospective harm flowing from the use of location data in violation of their First Amendment rights. Solove asserts that the threat of prosecution based on surveillance that implicates First Amendment rights would be sufficient to establish standing.[158] An amicus filing by civil liberties groups in *Harris* made such an argument,[159] but the court found, on other grounds, that Harris had no standing to challenge the subpoena, without even addressing his First Amendment rights.[160] To the extent that the Court's jurisprudence on the kind of showing sufficient to establish standing is in flux, this may impede First Amendment challenges to the overbroad collection of location data.

C. Application of the First Amendment to Location Data

With these caveats to asserting First Amendment protections to surveillance in mind, we can begin to sketch how litigants could argue the application of these protections to location data. While no single real-world case has made these arguments crisply, *Harris* and other cases point to three potential arguments for applying the First Amendment to location data: protections for (1) anonymous speakers, (2) location itself as speech, and (3) freedom of expressive association.

1. Location Data and the Protection of Anonymity

The Supreme Court has long recognized "a respected tradition of anonymity in the advocacy of political causes"[161] and has held that laws forcing political speakers to relinquish their anonymity are subject to a high level of scrutiny.[162] The *McIntyre* decision in 1995 coin-

(U.S. Feb. 26, 2013). In its petition for certiorari in *Clapper*, the government argued that the Second Circuit had misapplied *Laird*, writing, "A plaintiff's decision to inflict a self-imposed injury because of fear — a fear that itself is insufficient to confer Article III standing — cannot create a cognizable injury. Adding zero to zero is still zero." Petition for Writ of Certiorari, Clapper v. Amnesty Int'l USA, 2012 WL 549258, at *24–25 (Feb. 17, 2012) (No. 11-1025).

158. Solove, *supra* note 22, at 156–57.

159. *See* Harris Twitter Appeal Amici Brief, *supra* note 125, at 23 (arguing that the subpoena implicated Harris's First Amendment rights).

160. *See generally* People v. Harris, 949 N.Y.S.2d 590 (Crim. Ct. 2012).

161. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343 (1995); *see also* Talley v. California, 362 U.S. 60, 65 (1960).

162. In *McIntyre*, the Supreme Court considered an election law barring distribution of a publication intended to influence an election or "other similar types of general public political advertising" without listing the name and address of the responsible party. 514 U.S. at 338 n.3, 345. Finding that the Ohio law burdened McIntyre's core political speech and was thus subject to strict scrutiny, Justice Stevens held that neither the state's asserted interest in

cided with an explosion in Internet usage by the general public and a corresponding potential for widespread dissemination of anonymous speech.[163] Lower courts have interpreted *McIntyre* to provide protection for a wide range of anonymous speech online, using a balancing test when the government or a private litigant seeks to unmask anonymous speakers (usually via a third-party subpoena to the defendant's ISP).[164] The precise contours of this protection vary by jurisdiction and depend upon case-specific reasons for unmasking the anonymous speakers.[165] In general, courts balance the defendant's right of anonymity against "the strength of the [plaintiff's] prima facie case presented and the necessity for the disclosure."[166] In the criminal context, grand jury subpoenas to OSPs like Twitter to unmask anonymous speakers who have made a "true threat," for example, require demonstration of "'a compelling interest in the sought-after material' and 'a sufficient nexus between the subject matter of the investigation and the information they seek.'"[167]

Harris provides a jumping-off point for a scenario in which a defendant could claim that a subpoena (or D Order) for location data impermissibly burdens his right to anonymous speech. In Malcolm Harris's prosecution for disorderly conduct on the Brooklyn Bridge, he did not dispute that he was the author of the tweets at issue. Furthermore, the judge's denial of Harris's motion turned largely on the

---

"preventing fraudulent and libelous statements [nor] its interest in providing the electorate with relevant information . . . justif[ied] the anonymous speech ban." *Id.* at 348–51.

163. *See* Reno v. ACLU, 521 U.S. 844, 870 (1997) ("Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."). Musetta Durkee, Note, *The Truth Can Catch the Lie: The Flawed Understanding of Online Speech in* In re Anonymous Online Speakers, 26 BERKELEY TECH. L.J. 773, 787–91 (2011) (discussing courts' handling of online anonymous speech).

164. *See* Lyrissa Barnett Lidsky, *Anonymity in Cyberspace: What Can We Learn from John Doe?*, 50 B.C. L. REV. 1373, 1376–77 n.17 (2009) (listing cases and describing evolving standards).

165. Online anonymous speech has received most consideration in the civil context, particularly regarding anonymous speech that allegedly harms a plaintiff's business or personal reputation. *See id.* at 1379–81, 1385 (discussing the variability in these standards and arguing for a uniform standard with respect to anonymous speech that causes reputational harms). In another line of cases, copyright owners seek to identify alleged infringers who have anonymously downloaded or shared copyrighted material. *See, e.g.*, Arista Records, LLC v. Doe 3, 604 F.3d 110, 112–13 (2d Cir. 2010) (finding that copyright owner's assertion of infringement outweighed defendant's right to anonymity, and therefore, upholding subpoena to ISP to unmask defendant).

166. Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756, 760–61 (N.J. Super. Ct. App. Div. 2001); Lidsky, *supra* note 164, at 1378 (arguing that the *Dendrite* standard has become "dominant").

167. *In re* Grand Jury Subpoena No. 11116275, 846 F. Supp. 2d 1, 4–5 (D.D.C. 2012) (quoting *In re* Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461, 706 F. Supp. 2d 11, 18 (D.D.C. 2009)) (denying anonymous Twitter user's motion to quash subpoena related to tweets allegedly constituting a "true threat" to Congresswoman Michelle Bachmann).

fact that Harris's tweets were public, thus defeating his Fourth Amendment expectation of privacy. But as the civil liberties groups noted in their amicus filing, the public nature of Harris's speech alone would not defeat a First Amendment claim to anonymity under *McIntyre*.[168]

Suppose, however, that Harris *did* dispute his authorship (and hence claimed anonymity) and that his presence on the Brooklyn Bridge was further disputed. As a preliminary matter, a subpoena for a Twitter user's account information could directly identify an anonymous Twitter speaker without resort to location data per se, either by revealing his email address or an IP address then tied to ISP records. Yet this variation on *Harris* points to the need for location data to unmask an anonymous speaker in a real-world protest situation — that is, even if Harris was definitively tied to the tweets' content, the prosecution might still need to prove he was on the bridge at the time the posts were made. This might require the prosecution to resort to location data, likely via a D Order to Harris's mobile provider for CSLI that placed Harris within the vicinity of the bridge.[169]

More generally, we can imagine law enforcement's interest in a demonstration that results in injury or property damage in a certain location involving a small group of unknown or anonymous people.[170] In this situation, the collection and cross-referencing of cell-site data could fix owners of nearby mobile devices to a location with varying degrees of accuracy.[171] Thus, the location data itself could unmask participants and tie the expressive activity of the protest to the individuals.

In these situations, a court could take guidance from Solove's procedural framework and from precedent regarding unmasking anonymous speakers to weigh the governmental interest in the location data against the defendant's prima facie case for a First Amendment right to anonymity. In *Harris*, by issuing a subpoena, the prosecution did not even have to make the "specific and articulable

---

168. *See* Harris Twitter Appeal Amici Brief, *supra* note 125, at 16 (noting that the *McIntyre* plaintiff was in fact visible as she distributed her anonymous pamphlets).

169. The IP addresses obtained directly from Twitter might be sufficient to locate Harris in a much larger area, placing him in New York City, for instance. *See supra* Part II. Depending on the facts, the prosecution might require a more precise location. Even CSLI is likely too imprecise to definitively place Harris on the Brooklyn Bridge, but it could locate him within a several-hundred-meter area, strengthening the case against him. Given the timing of the tweets at issue, it seems likely that Harris posted them from a mobile device.

170. On the constitutionality of laws that forbid masked protests, see 1 RODNEY A. SMOLLA & MELVILLE B. NIMMER, SMOLLA AND NIMMER ON FREEDOM OF SPEECH § 11:25 (2012), see also Church of the Am. Knights of the Ku Klux Klan v. Kerik, 356 F.3d 197, 209 (2d Cir. 2004) (holding that anti-mask law does not implicate a right to anonymous speech).

171. *See, e.g.*, *S.D. Tex. 2012 Decision*, *supra* note 57, at *1 (describing government's cell tower dump request in order to identify individuals near a crime scene). Of course, some courts have found that this raises Fourth Amendment concerns as well. *Id.* at *3.

facts" showing required by ECPA to obtain a D Order.[172] Even under a scenario in which the prosecution sought cell site information with a D Order, however, a court could take counsel from Solove's analysis and require a higher probable cause showing before ruling against a claim of anonymity.

2. Location Data as Speech

These variations on *Harris* also suggest that a defendant could argue that her location data itself is speech, protected by the First Amendment. As the civil liberties amici observed in *Harris*:

> [I]nformation about Harris's location may provide meaning to some of his tweets that might not otherwise be apparent . . . . 'Take the bridge' might mean one thing if tweeted from [L]ower Manhattan on October 1, 2011 and a far different thing if tweeted from near the Golden Gate Bridge on September 11, 2001.[173]

Although this argument requires significant elaboration to fit existing doctrine, it could provide strong protection for location data, because the content of speech, including its accompanying context, is subject to the highest protection under the First Amendment.[174] In *City of Ladue v. Gileo*, the Supreme Court held that the location of a sign expressing a homeowner's political views was part of its meaning and therefore part of the protected speech itself.[175] Citing *City of Ladue*, the Court observed in *McIntyre* that anonymity is, in large part, the stripping of context from speech.[176]

To the extent that location data forms part of the context of protected speech and informs its meaning, a party opposing a subpoena could argue it is subject to the same protections as the content itself. In subpoenaing nonpublic IP address information from Harris's Twitter account, the prosecution arguably burdened his political speech by

---

172. 18 U.S.C. § 2703(d) (2006 & Supp. V 2012); *see supra* Part III.A.1.

173. Harris Twitter Appeal Amici Brief, *supra* note 125, at 17–18.

174. 1 SMOLLA & NIMMER, *supra* note 170, § 3:1.

175. *See* 512 U.S. 43, 56 (1994) (finding that sign on residence carries distinct meaning). These cases are classified as dealing with "time, place, and manner" restrictions, where the location of speech activity is often at issue, but context has been held to be part of speech in other First Amendment cases. *See, e.g.*, John Paul Stevens, *The Freedom of Speech*, 102 YALE L.J. 1293, 1295, 1310 (1993) ("Whether a particular act or message is more appropriately deemed 'speech' or 'conduct,' and whether it is entitled to First Amendment protection, turns on context as well as content."); *see also* Galvin v. Hay, 374 F.3d 739, 750 (9th Cir. 2004) (noting that "[t]he Court has recognized that location of speech, like other aspects of presentation, can affect the meaning of communication and merit First Amendment protection for that reason").

176. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342–43 (1995).

changing its public meaning and locating it in physical space. Of course, the prosecution could counter that Harris was being prosecuted not for the content *or* context of his speech but for nonspeech actions constituting disorderly conduct and that the subpoenaed information was essential for establishing this charge.[177] Existing doctrine likely favors the prosecution's argument,[178] but courts are often called on to consider novel First Amendment defenses to criminal charges.[179] Indeed, the facts of *Harris* and the potential for use of location data even in the context of a political demonstration suggest that courts should carefully consider whether such data informs speech in a specific instance.

3. The Unsatisfying Relationship of Location Data and Associational Rights

In a line of cases beginning with *NAACP v. Alabama*,[180] the Supreme Court has protected political and expressive organizations against subpoenas and legislative attempts to reveal their private membership lists.[181] Lower courts have extended this protection to other private records even when the information at issue is held by third parties.[182] In such association cases, the courts require that the government show "a substantial relation between the information sought and a subject of overriding and compelling state interest"[183] in order to compel production.

If police authorities *did* use a stingray to "skim" Occupy participants' mobile devices as privacy activists feared,[184] *Rigmaiden* shows that they might acquire location data on a wide range of individuals. This data could arguably reveal participants' ties to the movement — an activity Professor Katherine Strandburg terms "relational surveil-

177. United States v. O'Brien, 391 U.S. 367, 376 (1968) ("[W]hen 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms.").

178. Despite the arguments of the amici, the *Harris* court apparently saw no need to even address Harris's First Amendment interests in the tweets.

179. *See, e.g.*, Texas v. Johnson 491 U.S. 397, 414–17 (1989) (discussing government's power to impose criminal penalties for expressive conduct); *O'Brien*, 391 U.S. at 376.

180. 357 U.S. 449 (1958).

181. In *NAACP*, Justice Harlan wrote that "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association." *Id.* at 460. Because of the "vital relationship between freedom to associate and privacy in one's associations," the Court held that the disclosure sought by the state would hinder the group's ability to pursue its goals collectively. *Id.* at 462.

182. *See, e.g.*, *In re* First Nat'l Bank, Englewood, Colo., 701 F.2d 115, 118–19 (10th Cir. 1983).

183. Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 546 (1963).

184. *See supra* note 17.

lance."[185] Building on Solove's work, Strandburg argues that relational surveillance programs involving analysis of network traffic data, including phone records, interferes with associational rights in much the same way as forced disclosure of membership.[186]

However, the issue of standing is particularly pronounced for this sort of First Amendment associational claim.[187] *NAACP* and subsequent cases make clear that associational protection hinges on a showing that revelation of the information at issue would likely subject an association's members to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility."[188] In a recent case, the Federal District Court for the Eastern District of Virginia considered these risks in issuing a D Order in connection with the criminal investigation of Wikileaks to compel Twitter to turn over user records related to several prominent Wikileaks supporters.[189] The court reasoned that, unlike the NAACP's membership lists, the associations that the Twitter order would reveal — including the users' connections to Wikileaks — were already public.[190] The court thus found that the users had shown no evidence of "harassment or intimidation" that would flow from the order and thus no "chilling effect."[191]

This decision highlights several weaknesses with associational protection for location data. First, as a practical result, associations like NAACP and Wikileaks must assert such protection on behalf of their supporters, arguing that these unnamed supporters would be injured by the release of membership lists or records.[192] If members publicly assert this protection on their own behalf, they risk forfeiting standing based on associational protections. Second, following *Laird*, it seems that surveillance of public associations through location data,

185. Strandburg, *supra* note 131, at 744; *see also id.* at 755–56 (describing use of location in relational surveillance).

186. *Id.* at 804–05. Strandburg argues that relational surveillance that reveals individuals' expressive associations should require warrants based on probable cause. *Id.* at 820. *But see* Linda E. Fisher, *Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. REV. 621, 627 (2004) (arguing that reasonable suspicion is sufficient).

187. *See supra* Part IV.B.2.

188. NAACP v. Alabama, 357 U.S. 449, 462 (1958); *see also* Strandburg, *supra* note 131, at 744 ("Current legal doctrine . . . does not adequately account for the extent to which relational surveillance threatens to chill expressive association in today's networked world. Courts have yet even to consider the First Amendment implications of relational surveillance of this type.").

189. *E.D. Va. Opinion*, *supra* note 124, at 145–46. The users also argued the D Order violated their Fourth Amendment rights because it would reveal their movements through IP address location. *Id.* at 138.

190. *Id.* at 145–46.

191. *Id.* Because they had not "plausibly argued" a chilling effect, the court noted it was likely the users had "no First Amendment standing" to challenge the order. *Id.* at 145 n.24.

192. *See* Strandburg, *supra* note 131, at 785 (arguing that First Amendment association protections apply to "[e]mergent associations" but noting that precedent is unclear).

as with a political demonstration, is insufficient without more to show a chilling effect. Together, this presents an unsatisfying level of protection for associational rights, despite the potentially revealing nature of this "relational" location surveillance.[193]

V. CONCLUSION

As the forgoing discussion suggests, government collection of location data presents a troubling instance of surveillance that potentially chills First Amendment activity and is not sufficiently limited by current law. At present, courts may not be well equipped to fully consider new First Amendment protections for location data. In the first instance, magistrate judges considering ECPA requests will not have a factual record from which to weigh these interests and will rarely have an opposing party to raise them. To the extent that factual scrutiny is possible, however, Judge Smith has argued that magistrates should "stand up" to "an increasingly surveillance-happy state" as ordinary citizens' user data is implicated in warrantless cell phone tracking.[194] The First Amendment concerns described above should inform this scrutiny, particularly with technologies such as stingrays that can have a broad sweep. Furthermore, amending ECPA could produce more public cases with deeper factual records. Finally, as location-based political speech becomes further entwined with mobile communications and high-profile cases like *Harris* emerge, courts should be prepared to consider First Amendment concerns. Whatever the doctrine or statutory scheme, it is clear that failing to place reasonable, meaningful limits on the use of location data undermines public trust in a technology that increasingly enables communication, free association, and self-expression.

193. *Id.* at 744.

194. Stephen Wm. Smith, *Standing Up for Mr. Nesbitt*, 47 U.S.F. L. REV. 479, 480 (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2143339. Smith argues that magistrate judges can take judicial notice of important facts that are not revealed by a spare ECPA request record. *Id.* at 488 ("The digital revolution has made . . . massive amounts of information just a Google search away." (internal quotations omitted)). Judge Smith is of course responsible for one of the most detailed decisions on CSLI, which relies extensively on legislative testimony and industry data. *See generally S.D. Tex. 2010 Cell Site Decision*, *supra* note 38.