

FILED
JUL 29 A 9 35
FEDERAL DISTRICT COURT
SAN FRANCISCO, CALIFORNIA

1 Michael T. Risher (CA SBN 191627)

mrisher@aclunc.org

2 Nicole A. Ozer (CA SBN 228643)

nozer@aclunc.org

3 Christopher J. Conley (CA SBN 290747)

cconley@aclunc.org

4 AMERICAN CIVIL LIBERTIES UNION

5 FOUNDATION OF NORTHERN CALIFORNIA, INC.

39 Drumm Street, 2nd Floor

6 San Francisco, California 94111

7 Tel.: (415) 621-2493

8 Fax: (415) 255-8437

9 ATTORNEYS FOR *AMICUS* AMERICAN CIVIL

LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA

10 Nathan Freed Wessler

nwessler@aclu.org

11 AMERICAN CIVIL LIBERTIES UNION FOUNDATION

12 125 Broad Street, 18th Floor

13 New York, NY 10004

14 Tel.: (212) 549-2500

Fax: (212) 549-2654

15 ATTORNEYS FOR *AMICUS*

16 AMERICAN CIVIL LIBERTIES UNION

17
18 UNITED STATES DISTRICT COURT
19 FOR THE NORTHERN DISTRICT OF CALIFORNIA
20 SAN FRANCISCO DIVISION

21 In re Telephone Information Needed for a
22 Criminal Investigation

No.: CR 14-90532 Misc NC

23 **Brief *amici curiae* of ACLU and ACLU of**
24 **Northern California in support of federal**
25 **public defender's brief**

TABLE OF CONTENTS

1

2 INTRODUCTION 1

3 ARGUMENT 1

4 I. The Volume of Government Requests for Cell Site Location Information and

5 Barriers to Later Review Highlight the Importance of Careful Review

6 and Published Decisions Requiring a Probable Cause Warrant for Historical

7 CSLI 1

8 A. The Government is Obtaining Enormous Amounts of Personal Data

9 through Requests for CSLI 1

10 B. The Process by Which the Government Obtains These Data Is

11 Insulated from Scrutiny of the Appellate Courts, Criminal

12 Defendants, or the Public 4

13 II. Cell Phone Customers Retain Their Reasonable Expectation of Privacy in Their

14 Cell Site Location Information Because They Do Not “Voluntarily” Disclose

15 Such Information to Cell Carriers 8

16 A. Cell Phone Customers Do Not Voluntarily Disclose CSLI Through

17 Ordinary Use of Their Phones 8

18 B. Privacy Policies Do Not Convert CSLI Into Voluntarily Disclosed

19 Information 10

20 CONCLUSION 14

21

22

23

24

25

26

27

28

TABLE OF AUTHORITIES

Cases	Page(s)
<i>American Civil Liberties Union of N. Cal. v. Dep’t of Justice</i> , No. 12-CV-4008-MEJ, ECF No. 43-1 (N.D. Cal. Sept. 23, 2013).....	4, 6
<i>In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Info.</i> , 736 F. Supp. 2d 578 (E.D.N.Y. 2010)	4
<i>In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t. (“Third Circuit Opinion”)</i> , 620 F.3d 304, 317 (3d Cir. 2010).....	8, 9, 10
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	14
<i>Messerschmidt v. Millender</i> , 132 S. Ct. 1235 (2012).....	7
<i>Pearson v. Callahan</i> , 555 U.S. 223 (2009).....	6
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	1
<i>In re Sealing & Non-Disclosure of Pen/Trap/2703(D) Orders</i> , 562 F. Supp. 2d 876 (S.D. Tex. 2008)	4, 5
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	8, 9, 10
<i>State v. Subdiaz-Osorio</i> , __ N.W. 2d __, 2014 WL 3634768 (Wis. July 24, 2014).....	10
<i>State v. Tate</i> , __ N.W. 2d __, 2014 WL 3672705 (Wis. July 24, 2014).....	10, 13
<i>United States v. Barajas</i> , 710 F.3d 1102 (10th Cir. 2013)	7
<i>United States v. Davis</i> , No. 12-12928, __ F.3d __, 2014 WL 2599917 (11th Cir. June 11, 2014).....	3, 8
<i>United States v. Graham</i> , No. 12-4659 (4th Cir.)	3

1 *United States v. Hardrick*,
 Criminal Action No. 10–202, 2012 WL 4883666 (E.D. La. Oct. 15, 2012)7

2

3 *United States v. Herron*,
 ___ F. Supp. 2d ___, 2014 WL 824291 (E.D.N.Y. Mar. 3, 2014)7

4

5 *United States v. Jones*,
 132 S.Ct. 945 (2012).....13, 15

6 *United States v. Jones*,
 908 F. Supp. 2d 203 (D.D.C. 2012)7

7

8 *United States v. Katzin*,
 732 F.3d 187 (3d Cir. 2013).....15

9

10 *United States v. Miller*,
 425 U.S. 435 (1976).....8, 9

11 *United States v. Warshak*,
 631 F.3d 266 (6th Cir. 2010)13

12

13 **Statutes**

14 18 U.S.C. § 2703.....4, 6, 11

15 **Other Authorities**

16 Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA’s Secret*
 Docket, 6 Harv. L. & Pol’y Rev. 313 (2012).....6

17

18 Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3
 Fed. Cts. L. Rev. 177 (2009).....7

19

20 Victoria C. Plaut & Robert P. Bartlett, III, *Blind Consent? A Social Psychological*
Investigation of Non-Readership of Click-Through Agreements, 36 Law &
 Hum. Behav. 293 (2012).....13

21

22

23

24

25

26

27

28

INTRODUCTION

The ACLU and the ACLU of Northern California believe that it is improper for the government to seek and obtain sensitive location information without obtaining a warrant supported by probable cause. This practice has been allowed to proliferate because the government so often obtains orders for this information ex parte and under procedures that shield it both from public scrutiny and from appellate review. Amici urge the Court to deny the government’s application and to hold that the government must have a warrant to obtain cell-site-location information (“CSLI”).

ARGUMENT

I. The Volume of Government Requests for Cell Site Location Information and Barriers to Later Review Highlight the Importance of Careful Review and Published Decisions Requiring a Probable Cause Warrant for Historical CSLI.

A. The Government is Obtaining Enormous Amounts of Personal Data through Requests for CSLI.

Cell phone use has become ubiquitous: the number of wireless accounts now exceeds the total population of the United States,¹ and 41% of U.S. households have only wireless telephones.² As wireless use has grown, law enforcement demands for cell phone location information, most often without a probable cause warrant, have also increased.

In 2011, the ACLU sent hundreds of public records requests to state and local law

¹ CTIA — The Wireless Association, *Annual Wireless Industry Survey* (2014), <http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey>.

² Stephen J. Blumberg & Julian V. Luke, Nat’l Center for Health Statistics, *Wireless Substitution: Early Release of Estimates from the National Health Interview Survey, July–December 2013*, at 1 (2014), *available at* <http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201407.pdf>. *See Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (“According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.”) (citation omitted).

1 enforcement agencies across the nation seeking information about use of cell site location
2 information. Approximately 250 agencies responded, with nearly all of them disclosing that they
3 request cell phone location information from service providers to aid in investigations.³ While a
4 few agencies routinely seek probable cause warrants when requesting CSLI, most reported
5 requesting CSLI based on a lower standard.⁴
6

7 Cell service providers have also started to release transparency reports in recent years,
8 revealing that each year they receive tens of thousands of law-enforcement requests for location
9 information, most of which lack a warrant. AT&T, for example, reported receiving 31,000
10 requests for historical CSLI and 46,800 requests for real-time cell phone location information in
11 2012.⁵ In 2013, it reported receiving 24,229 requests for historical location information and
12 12,576 requests for real-time data.⁶ Verizon reported receiving 30,000 requests for historical
13 CSLI in 2012⁷ and 35,000 requests for location information in 2013.⁸ Verizon received 15,950
14 requests for location information in the first half of 2014 and has publicly stated that “two-thirds
15
16
17

18 ³ ACLU, Cell Phone Location Tracking Public Records Request,
19 <https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request>.

20 ⁴ ACLU Affiliate Nationwide Cell Phone Tracking Public Records Requests: Findings and
21 Analysis 3–4 (2012), https://www.aclu.org/files/assets/cell_phone_tracking_documents_-_final.pdf.

22 ⁵ Letter from Timothy P. McKone, Executive Vice President, AT&T, to Sen. Edward J. Markey,
23 Attachment A (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-10-03_ATT_re_Carrier.pdf.

24 ⁶ AT&T, Transparency Report, <http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html>.

25 ⁷ Letter from William B. Petersen, General Counsel, Verizon Wireless, to Sen. Edward J.
26 Markey 2 (Oct. 3, 2013), *available at* http://www.markey.senate.gov/imo/media/doc/2013-12-09_VZ_CarrierResponse.pdf.

27 ⁸ Nicole A. Ozer, *Verizon Begins to Clear the Air—Issues First Transparency Report*, ACLU of
28 Northern California (Jan. 22, 2014), <https://www.aclunc.org/blog/verizon-begins-clear-air-issues-first-transparency-report>.

1 of those were through orders” rather than warrants.⁹ From 2007 to 2012, Sprint/Nextel received
 2 nearly 200,000 court orders for cell phone location information.¹⁰

3 The data that the government is obtaining through these requests can reveal great
 4 quantities of private and sensitive information about a person’s location and movements over
 5 time. In *United States v. Davis*, No. 12-12928, ___ F.3d ___, 2014 WL 2599917 (11th Cir. June 11,
 6 2014), for example, law enforcement obtained 67 days’ worth of historical CSLI for a Florida
 7 man, revealing 11,606 cell site location data points.¹¹ In *United States v. Graham*, No. 12-4659
 8 (4th Cir.) (appeal pending), the government obtained more than 7 months of historical CSLI,
 9 comprising 29,659 cell site location data points for one co-defendant and 28,410 for the other.¹²
 10 This data can reveal when a person was at home, where he slept, when he traveled to the doctor’s
 11 office, and other “privacies of life.”¹³ *Davis*, 2014 WL 2599917, at *4 (quoting *Olmstead v.*
 12 *United States*, 277 U.S. 438, 473 (Brandeis, J., dissenting)) (internal quotation marks and
 13 emphasis omitted). And the technology is allowing CSLI to become ever more precise,¹⁴ making
 14 it crucial for courts to provide guidance to law enforcement and the public about the scope of the
 15 Fourth Amendment.
 16
 17
 18
 19
 20

21 ⁹ Verizon, Transparency Report for the First Half of 2014, <http://transparency.verizon.com/us-report>.

22 ¹⁰ Letter from Vonya B. McCann, Senior Vice President, Sprint, to Rep. Edward J. Markey 4
 23 (May 23, 2012), available at
 24 <http://web.archive.org/web/20120709202732/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf>.

25 ¹¹ Brief of *Amici Curiae* American Civil Liberties Union Foundation, et al. at 13–14, *Davis*, No.
 12-12928, available at https://www.aclu.org/files/assets/filed_q_davis_amicus_br_0.pdf.

26 ¹² Brief of *Amici Curiae* American Civil Liberties Union, et al. at 12, *Graham*, No. 12-4659,
 27 available at https://www.aclu.org/files/assets/2013.07.02_-_doc_60_-_corrected_aclu_et_al_amicus_brief.pdf.

28 ¹³ *Id.* at 13–15.

¹⁴ See Ctr. for Democracy & Tech., Cell Phone Tracking: Trends in Cell Site Precision (2013),
 available at <https://www.cdt.org/files/file/cell-location-precision.pdf>.

B. The Process by Which the Government Obtains These Data Is Insulated from Scrutiny of the Appellate Courts, Criminal Defendants, or the Public.

The secrecy often accompanying government requests for CSLI and barriers to later review make it particularly crucial that “magistrate judges presented with *ex parte* requests for authority to deploy various forms of warrantless location-tracking must carefully reexamine the constitutionality of such investigative techniques.” *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Info.*, 736 F. Supp. 2d 578, 582 (E.D.N.Y. 2010) (Orenstein, M.J.), *reversed by district court without opinion* Nov 29, 2010.

The government’s standard practice when applying for orders under 18 U.S.C. § 2703(d) is to request that the application and order be sealed, and under current practice almost all of the orders remained sealed indefinitely. As an Assistant United States Attorney in this District has explained, “[w]hen using investigative tools such as applying for an order seeking location tracking information, the general practice at the [U.S. Attorney’s Office] is also to apply to seal the application (if any), affidavit (if any) and order.” Decl. of Patricia J. Kenney ¶ 7, *American Civil Liberties Union of N. Cal. v. Dep’t of Justice*, No. 12-CV-4008-MEJ, ECF No. 43-1 (N.D. Cal. Sept. 23, 2013); *see id.* ¶ 10.¹⁵ Once sealed, applications and orders remain under seal “until further order of the court.” *In re Sealing & Non-Disclosure of Pen/Trap/2703(D) Orders*, 562 F. Supp. 2d 876, 877–78 (S.D. Tex. 2008) (Smith, M.J.). The government seldom seeks unsealing. In this District, for example, the U.S. Attorney’s Office (“USAO”) conducts “no systematic review on an ongoing basis of the sealed applications to determine whether the conditions requiring sealing continue.” Kenney Decl. ¶ 9. And judges rarely unseal these materials *sua sponte*. Therefore, in practice “indefinitely sealed means permanently sealed.” *In re Sealing &*

¹⁵ A copy of the Kenney Declaration is attached to this brief as “Exhibit A”.

1 *Non-Disclosure of Pen/Trap/2703(D) Orders*, 562 F. Supp. 2d at 878. In the words of one
2 magistrate judge, “[t]he result has been a kudzu of sealed manila envelopes overflowing the
3 clerk’s office vault.” *Id.*

4 A survey by Magistrate Judge Smith of electronic surveillance orders issued in the
5 Southern District of Texas over a 13-year period revealed that “out of 3,886 orders sealed ‘until
6 further order of the court,’ 99.7% remain under seal today, many years after issuance.” *Id.* A
7 recent investigation by the Wall Street Journal revealed that the vast majority of electronic-
8 surveillance applications and orders in district courts across the country are listed as being under
9 seal: for example, only about two percent of sampled electronic surveillance orders in the
10 Southern District of Florida have been unsealed, and 99% of surveyed electronic
11 communications surveillance records in the Eastern District of Virginia are under seal. Jennifer
12 Valentino-Devries, *Sealed Court Files Obscure Rise in Electronic Surveillance*, Wall St. J., June
13 2, 2014¹⁶; Jennifer Valentino-Devries & Andrea Fuller, *How the Journal Evaluated Sealed*
14 *Surveillance Orders*, Wall St. J., June 2, 2014.¹⁷

15 Even when the public specifically seeks records, useful information is rarely
16 forthcoming. The majority of 25 federal districts queried by the Wall Street Journal, including
17 the Northern District of California, provided no data on electronic surveillance orders
18 whatsoever. *See Electronic-Surveillance Orders in Federal District Courts*, Wall St. J., June 2,
19 2014.¹⁸ In this district, after the ACLU of Northern California submitted a Freedom of
20 21 22 23 24

25 ¹⁶ Available at <http://online.wsj.com/articles/sealed-court-files-obscure-rise-in-electronic-surveillance-1401761770>.

26 ¹⁷ Available at <http://blogs.wsj.com/law/2014/06/02/how-the-journal-evaluated-sealed-surveillance-orders/>.

27 ¹⁸ <https://docs.google.com/spreadsheets/d/1kUL3Ou7Zifjrkaepvd9jMD8RZHUnZyOKrejLk5K2zI/pubhtml>.

1 Information Act request to the U.S. Attorney's Office seeking applications for CSLI and other
2 location tracking orders, the USAO identified 760 responsive files but explained that only six of
3 those files were public. Kenney Decl. ¶ 19. The government further asserted that it had no
4 practical way to evaluate applications and orders in *closed* cases to determine which ones it
5 believes can be unsealed. *Id.* ¶ 9. The ACLU's request is currently in litigation before Judge
6 James. *Am. Civil Liberties Union of N. Cal. v. Dep't of Justice*, No. 12-CV-4008-MEJ.
7

8 Because most applications and orders for CSLI remain indefinitely sealed, most people
9 never learn that their location information was sought or obtained, and therefore cannot bring a
10 Fourth Amendment challenge. The "government is generally not required to provide notice to the
11 subscriber or customer before compelling disclosure from the provider via a 2703(d) order," and
12 sealed orders under § 2703(d) typically include a gag provision precluding the service provider
13 from notifying the subject of the investigation about the search. Stephen Wm. Smith, *Gagged,*
14 *Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 324–25
15 (2012). Only if a person is investigated *and* indicted *and* prosecuted *and* the government chooses
16 to use the CSLI as evidence at trial will she typically receive notice that her location information
17 has been searched. People who are investigated and determined to be innocent will generally
18 never learn that the government obtained their location records; likewise defendants whose CSLI
19 records are neither inculpatory nor exculpatory and therefore neither introduced at trial nor
20 disclosed pursuant to *Brady*. The majority of instances of warrantless CSLI collection will go
21 unchallenged.
22
23
24

25 Even in the rare case where an individual learns that the government acquired their cell
26 phone location information without a warrant, immunity and justiciability doctrines can impede
27 review of the constitutional question. *Pearson v. Callahan*, 555 U.S. 223 (2009) (courts may
28

1 address qualified immunity before determining whether the government has violated a plaintiff's
2 constitutional rights); *see also Messerschmidt v. Millender*, 132 S. Ct. 1235 (2012) (finding
3 qualified immunity and declining to rule on whether facts stated in a warrant application
4 established probable cause). Similarly, government invocation of the good-faith exception to the
5 exclusionary rule can thwart appropriate Fourth Amendment analysis in cases involving CSLI.
6
7 *See, e.g., United States v. Jones*, 908 F. Supp. 2d 203, 213–14 (D.D.C. 2012) (“[T]his Court need
8 not decide whether the government violated the Fourth Amendment when it obtained the cell
9 data from Cingular Wireless, since the well-recognized good-faith exception bars the application
10 of the exclusionary rule to this case.”); *United States v. Herron*, ___ F. Supp. 2d ___, 2014 WL
11 824291, at *10–11 (E.D.N.Y. Mar. 3, 2014) (similar); *United States v. Hardrick*, Criminal
12 Action No. 10–202, 2012 WL 4883666, at *4 (E.D. La. Oct. 15, 2012) (similar); *cf. United*
13 *States v. Barajas*, 710 F.3d 1102, 1109–11 (10th Cir. 2013) (applying good-faith exception to
14 avoid deciding whether law enforcement had probable cause to obtain real-time cell phone
15 location information). These numerous barriers mean that *ex post* review of unconstitutional
16 acquisition of CSLI will often prove inadequate to cure the violation or even to provide a clear
17 statement of what the Fourth Amendment requires. As Judge Smith has explained, “these sealed
18 orders are entirely off the radar screen, not only for the public at large, but also for appellate
19 courts.”¹⁹ This creates a “breakdown in the normal process of appellate review” that could
20 otherwise serve to ensure that they comply with the Constitution.²⁰ Magistrate judges thus have
21
22
23
24

25 ¹⁹ Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L.
26 Rev. 177, 212 (2009).

27 ²⁰ Hearing on Electronic Communications Privacy Act Reform and the Revolution in Location
28 Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and
Civil Liberties of the House Comm. on the Judiciary, 111th Cong. 12 (2010) (statement of U.S
Magistrate Judge Stephen Wm. Smith), *available at* <http://ssrn.com/abstract=2173529>.

1 not only the first but often the only opportunity to evaluate the constitutionality of warrantless
2 demands for sensitive location information.

3 **II. Cell Phone Customers Retain Their Reasonable Expectation of Privacy in Their**
4 **Cell Site Location Information Because They Do Not “Voluntarily” Disclose**
5 **Such Information to Cell Carriers.**

6 **A. Cell Phone Customers Do Not Voluntarily Disclose CSLI Through Ordinary**
7 **Use of Their Phones.**

8 Cell phone users have a reasonable expectation of privacy in their cell site location
9 information. *Davis*, 2014 WL 2599917, at *8–10. That expectation is not undermined simply by
10 the fact that cell service providers are able to access customers’ location data. Instead, the
11 threshold question is whether the users “voluntarily convey[]” CSLI to the carrier. *See United*
12 *States v. Miller*, 425 U.S. 435, 442 (1976). And ““a cell phone customer has not “voluntarily”

13 shared his location information with a cellular provider in any meaningful way.” *Davis*, 2014
14 WL 2599917, at *9 (quoting *In re Application of U.S. for an Order Directing a Provider of Elec.*
15 *Comm’n Serv. to Disclose Records to the Gov’t. (“Third Circuit Opinion”)*, 620 F.3d 304, 317
16 (3d Cir. 2010)). Many if not most cell phone customers are unaware that providers collect and
17 store historical location information at all, let alone the quantity of such records collected and
18 stored. *See id.* Moreover, even customers who are aware that CSLI is being generated by their
19 cell phone provider cannot prevent that from happening without disabling their phone’s ability to
20 receive calls and other communications, which for many is not a truly available option. *Cf. Smith*
21 *v. Maryland*, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting). Because CSLI is not
22 voluntarily shared with cell phone providers, cell phone customers retain a reasonable
23 expectation of privacy in such information.
24
25

26
27 There is nothing inherent in carrying or using a cell phone that would indicate to
28 customers that they are exposing their location information to their wireless carrier. The user

1 does not input her location information into the phone, and the phone does not notify the user
 2 that her location has been logged. In fact, cell phones generate CSLI without any user activity at
 3 all. As the Third Circuit has explained:

4 “[w]hen a cell phone user makes a call, the only information that is voluntarily
 5 and knowingly conveyed to the phone company is the number that is dialed and
 6 there is no indication to the user that making that call will also locate the caller;
 7 when a cell phone user receives a call, he hasn’t voluntarily exposed anything at
 all.”²¹

8 There is nothing analogous to writing a recipient’s name on a check or dialing a telephone
 9 number to suggest a knowing and voluntary transfer of CSLI information. *Cf. Smith*, 442 U.S.
 10 735 (dialed phone numbers voluntarily conveyed); *Miller*, 425 U.S. 435 (bank transaction
 11 information voluntarily conveyed). In addition, unlike a dialed phone number, location
 12 information does not appear on a typical user’s monthly bill. *Cf. Third Circuit Opinion*, 620 F.3d
 13 at 742.

14 In fact, information available to cell phone users is likely to lead them to believe that they
 15 have more control over their location information than they actually do, thus heightening their
 16 expectation of privacy. Many smartphones have an overarching location-privacy setting that,
 17 when enabled, prevents all apps on the phone from accessing the phone’s location. *See, e.g.*,
 18 Apple, iPhone User Guide For iOS 7.1 Software 36 (2014)²² (“Privacy settings let you see and
 19 control which apps and system services have access to Location Services....”); Google, Android
 20 Quick Start Guide 11 (2013)²³ (“You can control how Google Now uses your current location.
 21
 22
 23
 24

25 ²¹ *Third Circuit Opinion*, 620 F.3d at 317–18 (alteration in original) (citation omitted).

26 ²² Available at
 27 https://a248.e.akamai.net/7/248/51/20120908/manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf.

28 ²³ Available at http://nexus5manual.com/wp-content/uploads/2013/11/Google_Nexus_5_Android-4.4-Kit-Kat_User_Manual_Guide.pdf.

1 To view the relevant settings, go to Settings > Personal > Location. When location services are
2 turned on for your account on a given device, certain apps can use them....”). However, these
3 settings have no impact at all upon *carriers*’ ability to learn the cell sector in use. Even a
4 privacy-conscious cell phone user who disables the location tracking function on her phone
5 cannot prevent the cell service provider from logging and retaining CSLI. Yet there is nothing
6 about the user’s interaction with her phone that would so indicate.
7

8 Further, even cell phone customers who are aware of the possibility that their carrier may
9 collect and retain CSLI have no realistic alternative to prevent that from happening. As noted
10 above, CSLI can be collected even without any action on the part of the user, as when she
11 receives a phone call. *Third Circuit Opinion*, 620 F.3d at 317–18. The only way to prevent CSLI
12 from being collected at any given point in time is to turn a cell phone completely off, which
13 prevents it from receiving calls or other communications. And the only way to completely
14 prevent the collection of CSLI is to not possess a cell phone at all. But in today’s world,
15 possession of a cell phone is for many necessary, not voluntary. *Cf. Smith*, 442 U.S. at 750
16 (Marshall, J., dissenting) (“[U]nless a person is prepared to forgo use of what for many has
17 become a personal or professional necessity, he cannot help but accept the risk of
18 surveillance It is idle to speak of ‘assuming’ risks in contexts where, as a practical matter,
19 individuals have no realistic alternative.” (internal citation omitted)).
20
21

22 **B. Privacy Policies Do Not Convert CSLI Into Voluntarily Disclosed** 23 **Information.**

24 Contrary to the government’s assertion, *see* Gov’t Ltr.-Br. at 4–5, the existence of
25 privacy policies on cell service providers’ websites does not convert automatic, involuntary
26 retention of location information into voluntary conveyance of such data. *See State v. Subdiaz-*
27 *Osorio*, __ N.W. 2d __, 2014 WL 3634768, at *13–15 (Wis. July 24, 2014) (Prosser, J., lead
28

1 op.); *Id.* at *34 (Abrahamson, C.J., dissenting); *State v. Tate*, __ N.W. 2d __, 2014 WL 3672705,
2 at *19 (Wis. July 24, 2014) (Abrahamson, C.J., dissenting). Extensive research shows that few
3 consumers read privacy policies and even fewer really understand them.²⁴ The policies
4 themselves do not contain sufficient detail to fully inform any consumer who does read the
5 policy about CSLI collection and retention or about the legal process by which law enforcement
6 may demand such records. And most policies are worded to reassure consumers that information
7 such as CSLI is securely protected, reinforcing rather than undermining a reasonable expectation
8 of privacy in such information.
9

10 Even the minority of people who read and understand their carrier's privacy policy lack
11 crucial information about the privacy of their location information. Although the versions of the
12 policies cited by the government provide some discussion of the location data automatically
13 stored by service providers, they do not specify what legal process the companies deem
14 sufficient to turn over CSLI—a warrant, a § 2703(d) order, or something else. The T-Mobile
15 policy, for example, says only that it “can also disclose your device location to the government
16 or law enforcement when T-Mobile is served with lawful process.” T-Mobile, Privacy Policy
17
18
19

20
21 ²⁴ Academic research indicates that consumers “rarely read” privacy policies. Janice Y. Tsai et
22 al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*,
23 22 *Info. Sys. Res.* 254, 256 (2011), available at
24 <http://www.guanotronic.com/~serge/papers/isr10.pdf>; see also Carlos Jensen et al., *Privacy*
25 *Practices of Internet Users: Self Reports Versus Observed Behavior*, 63 *Int'l J. Human-*
26 *Computer Stud.* 203, 223 (2005), available at <http://www.idi.ntnu.no/emner/tdt60/papers/P4.pdf>;
27 M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 *Notre Dame L. Rev.*
28 1027, 1032 & n.34 (2012). This is understandable given the length and complexity of such
policies. At more than 9,000 and 8,000 words, respectively, it is understandable why individual
customers might not wade through the details of the T-Mobile and AT&T privacy policies. See
T-Mobile, Privacy Policy (Dec. 30, 2013), [http://www.t-](http://www.t-mobile.com//company/website/privacypolicy.aspx)
mobile.com//company/website/privacypolicy.aspx; AT&T, Privacy Policy (Sept. 16, 2013),
http://www.att.com/Common/about_us/privacy_policy/print_policy.html.

1 (Dec. 30, 2013).²⁵ The policies also do not disclose how frequently CSLI records are generated
2 or the length of time such information is retained.²⁶ Although this kind of information is crucial
3 to informing people about the privacy of their location data and law enforcement's ability to
4 obtain it, the CSLI retention periods appear nowhere in the carriers' privacy policies. Thus, even
5 a sophisticated consumer who read and understood carriers' privacy policies would lack the
6 information to understand how her location privacy would be affected by signing up for cell
7 phone service or to make an informed choice between available cell service providers to pick one
8 offering greater protection for location privacy.
9

10 In fact, cell phone customers may well believe that privacy policies *protect against*
11 collection and disclosure of information, not facilitate it. As one group of researchers has
12 explained: "Americans believe, logically, that the phrase 'privacy policy' signifies that their
13

14
15
16 ²⁵ Available at <http://www.t-mobile.com/company/website/privacypolicy.aspx>.

17 ²⁶ The availability of historical cell site location information and the length of time it is stored
18 depends on the policies of individual wireless carriers. Until recently, the only publicly available
19 information about carriers' retention policies came from documents obtained by the ACLU via
20 public records requests to local police departments. See U.S. Dep't of Justice, Retention Periods
21 of Major Cellular Service Providers (Aug. 2010), available at [https://www.aclu.org/cell-phone-
location-tracking-request-response-cell-phone-company-data-retention-chart](https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart). According to those
22 records, T-Mobile stores CSLI "[o]fficially 4-6 months, really a year or more," and
23 AT&T/Cingular stores CSLI indefinitely "from July 2008." *Id.* Last year, cell service providers
24 revealed their current retention policies in response to queries from U.S. Senator Ed Markey. See
25 Press Release, Sen. Ed Markey, For Second Year in a Row, Markey Investigation Reveals More
26 Than One Million Requests by Law Enforcement for Americans Mobile Phone Data (Dec. 9,
27 2013), available at [http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-
row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-
americans-mobile-phone-data](http://www.markey.senate.gov/news/press-releases/for-second-year-in-a-row-markey-investigation-reveals-more-than-one-million-requests-by-law-enforcement-for-americans-mobile-phone-data). According to the companies, T-Mobile stores historical CSLI for
28 "180 [d]ays" and AT&T for "5 years." Letter from Tony Russo, Vice President, T-Mobile, to
Sen. Edward J. Markey 3 (Oct. 3, 2013), available at
http://www.markey.senate.gov/imo/media/doc/2013-12-09_Tmobile_CarrierResponse.pdf;
Letter from Timothy P. McKone, Executive Vice President, AT&T, to Sen. Edward J. Markey 3
(Oct. 3, 2013).

1 information will be kept private.”²⁷

2 Even if contract language could sometimes diminish expectations of privacy, the
3 government’s argument defies “the reality of cell phone usage by the everyday purchaser of a
4 cell phone: When accepting an adhesion contract to purchase cell phone service—an increasingly
5 necessary component of everyday life—the purchaser is not bargaining for unfettered
6 government access to the purchaser’s cell phone location data.” *Tate*, 2014 WL 3672705, at *19
7 (Abrahamson, C.J., dissenting). A cell service provider’s contractually reserved ability to access
8 location information for particular network administration purposes does not waive a customer’s
9 reasonable expectation of privacy in that data. The Supreme Court has long held that people have
10 a reasonable expectation of privacy in the contents of their telephone calls notwithstanding the
11 phone company’s right to listen to calls “to ‘protect themselves and their properties against the
12 improper and illegal use of their facilities’” and for other purposes. *United States v. Warshak*,
13 631 F.3d 266, 286–87 (6th Cir. 2010) (citing *Katz v. United States*, 389 U.S. 347 (1967) and
14 *Smith*, 442 U.S. at 746–47 (Stewart, J., dissenting)) (additional citation omitted); *see also id.*
15 (Fourth Amendment protection for email notwithstanding terms-of-service provisions allowing
16 provider to access contents under limited circumstances). This is particularly true given the
17 sensitive information that can be revealed through detailed location records. *Cf. United States v.*
18
19
20
21
22

23 ²⁷ Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming*
24 *Decade*, 3 I/S: J.L. & Pol’y for Info. Soc’y 723, 732 (2007); *see also* Joseph Turow et al.,
25 *Research Report: Consumers Fundamentally Misunderstand the Online Advertising Marketplace*
26 1 (2007), available at http://www.law.berkeley.edu/files/annenberg_samuelson_advertising.pdf
27 (reporting that most people think the mere existence of a privacy policy on a website means “the
28 site will not share my information with other websites or companies”); *cf.* Victoria C. Plaut &
Robert P. Bartlett, III, *Blind Consent? A Social Psychological Investigation of Non-Readership*
of Click-Through Agreements, 36 Law & Hum. Behav. 293, 299 (2012) (“[Study] participants
have little comprehension of the [online contract] terms to which they have agreed.”).

1 *Jones*, 132 S.Ct. 945, 955 (2012) (Sotomayor, J., concurring) (“GPS monitoring generates a
2 precise, comprehensive record of a person’s public movements that reflects a wealth of detail
3 about her familial, political, professional, religious, and sexual associations.”).

4 The existence of a privacy policy, particularly one that is rarely read and even more
5 rarely understood and that lacks essential information about the collection of CSLI, does not
6 eliminate cell phone customers’ reasonable expectation of privacy in detailed and extensive
7 records of their location. Cell phone customers have a reasonable expectation of privacy in their
8 cell phone location information because of the sensitivity of the data and because they do not
9 voluntarily convey it to cell service providers. Provisions in a privacy policy or terms of service
10 granting the company the power to access location information for certain purposes do not and
11 should not give the police a blank check to conduct surveillance without complying with the
12 requirements of the Fourth Amendment.
13
14

15 CONCLUSION

16 When the courts are asked to allow the government to engage in new forms of
17 surveillance, they must not “permit police technology to erode the privacy guaranteed by the
18 Fourth Amendment.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001). Owning a cell phone is for
19 many Americans a near-necessity of life that they use to keep in touch with their children’s
20 school or a demanding boss. When they put their phone in their pocket as they head out the door
21 in the morning, they do not expect that the government will be able to track their every move,
22 any more than they would expect the police to be able to look through the walls of their house.
23 *See id.* at 34–35. And just as the police must obtain a warrant, supported by probable cause,
24 before they use new technology to peer into a person’s house, or to use a GPS device to follow
25
26
27
28

1 his car's movements,²⁸ they must obtain one before they use a person's cell phone to track him.

2
3 Dated: July 28, 2014

Respectfully Submitted,

4 By: /s/ Michael T. Risher
5 Michael T. Risher

6
7 Michael T. Risher
8 Nicole A. Ozer
9 Christopher Conley
10 AMERICAN CIVIL LIBERTIES UNION
11 FOUNDATION OF NORTHERN CALIFORNIA
12 39 Drumm Street, 2nd Floor
13 San Francisco, California 94111
14 Tel.: (415) 621-2493
15 Fax: (415) 255-8437

16 Attorneys for *Amicus* American Civil Liberties Union
17 Foundation of Northern California, Inc.

18 Nathan Freed Wessler
19 AMERICAN CIVIL LIBERTIES UNION
20 FOUNDATION
21 125 Broad Street, 18th Floor
22 New York, NY 10004
23 Tel.: (212) 549-2500
24 Fax: (212) 549-2654

25 Attorney for *Amicus* American Civil Liberties Union
26

27 ²⁸ See *Jones*, 132 S. Ct. 945; *United States v. Katzin*, 732 F.3d 187, 204–05 (3d Cir. 2013),
28 *vacated pending en banc reh'g*, No. 12-2548, 2013 WL 7033666 (3d Cir. Dec. 12, 2013); *id.* at
217 (Van Antwerpen, J., concurring in part and dissenting in part).

EXHIBIT A

1 STUART F. DELERY
Assistant Attorney General

2 ELIZABETH J. SHAPIRO (D.C. Bar No. 418925)
3 Deputy Branch Director

4 BRAD P. ROSENBERG (D.C. Bar No. 467513)
Trial Attorney
5 U.S. Department of Justice
Civil Division, Federal Programs Branch
6 P.O. Box 883
Washington, D.C. 20044
7 Telephone: (202) 514-3374
Facsimile: (202) 616-8460
8 E-mail: brad.rosenberg@usdoj.gov

9 Attorneys for Defendant
U.S. Department of Justice

10
11 UNITED STATES DISTRICT COURT
12 NORTHERN DISTRICT OF CALIFORNIA
13 SAN FRANCISCO DIVISION

14 AMERICAN CIVIL LIBERTIES UNION)
15 OF NORTHERN CALIFORNIA;)
SAN FRANCISCO BAY GUARDIAN,)

16 Plaintiffs,)

17 v.)

18 DEPARTMENT OF JUSTICE)

19 Defendant.)

No. 12-CV-4008-MEJ

DECLARATION OF PATRICIA J. KENNEY
IN SUPPORT OF THE DEPARTMENT OF
JUSTICE'S MOTION FOR SUMMARY
JUDGMENT AS TO PART 1 OF PLAINTIFF'S
FREEDOM OF INFORMATION ACT REQUEST

20
21
22 I, Patricia J. Kenney, declare pursuant to 28 U.S.C. § 1746 as follows:

23 1. I am an Assistant United States Attorney ("AUSA") in the Criminal Division of the
24 Office of the United States Attorney ("USAO") for the Northern District of California ("NDCA"), and
25 am admitted to practice law in the State of California. Since the spring of 2011, I have been assigned as
26 a collateral duty, in addition to my regular duties, the responsibility in the NDCA Criminal Division
27 ("Criminal Division") for advising management on its responsibilities under the Freedom of Information
28

1 Act ("FOIA"), for advising other AUSAs in the Criminal Division on FOIA matters and to work with
2 the FOIA contact paralegal in the Criminal Division. I have experience in handling FOIA matters,
3 having handled a substantial number of FOIA cases in the USAO in the District of Columbia where I
4 was an AUSA in the Civil Division from 1979 to 1985, and in the NDCA where I was an AUSA in the
5 Civil Division from 1990 until about 2002. In addition, I was asked to be the liaison with the
6 Department of Justice to assist with this litigation, again in addition to my regular duties. The
7 information in this declaration is based on my personal knowledge, or knowledge which has come to me
8 in the ordinary course of my duties as an AUSA, in providing FOIA advice, and in working as a liaison
9 in this litigation with USAO managers, supervisors and line AUSAs as well as DOJ attorneys and staff.

10 2. As explained below, Part 1 of the ACLU April 13, 2012 FOIA request (Exhibit A
11 attached without exhibits) seeks applications for orders seeking location tracking information. One
12 purpose of this declaration is to describe efforts the USAO has made to identify USAO files with
13 applications for orders seeking location tracking information, and explain why the search for those
14 records cannot reasonably be performed because the USAO's filing system, which serves its own
15 purposes well, is not constructed in a manner to permit identification and retrieval of records the ACLU
16 requests. The USAO does not maintain its case files electronically. Rather, the USAO maintains paper
17 files identified by USAO numbers for matters that it opens to investigate. Tools that prosecutors use for
18 developing evidence during the course of an investigation – such as search warrants or pen registers –
19 are generally not filed separately, but are preserved in the USAO paper file for that USAO investigation.
20 Although search warrants and pen registers can be used to obtain location tracking information, these
21 investigative tools have much broader application. Because Part 1 of the ACLU's request seeks only a
22 narrow subset of search warrants and pen registers (those seeking location tracking information), it
23 further complicates a search to identify responsive records. As a result, the USAO is unable to identify
24 and retrieve all documents responsive to Part 1 of the ACLU FOIA request without manually retrieving
25 and reviewing all the paper files for all matters opened since January 1, 2008.

26 Another purpose of this declaration is to explain the general practice of AUSAs in the Criminal
27 Division to request that the Court seal applications and orders seeking location tracking information to
28

1 protect the investigation. The sealing orders bar the USAO from publically disclosing the records.
2 Thus, if the USAO were compelled to identify and retrieve documents responsive to Part 1 of the ACLU
3 FOIA request by manually retrieving and reviewing all the paper files for all matters opened since
4 January 1, 2008, the end result of that onerous search would be to identify documents that the have been
5 filed-stamped as sealed by the Court, *e.g.*, stamped “sealed by the Court” or “UNDERSEAL.” Finding
6 responsive records will not resolve whether the record is still under seal. Although USAO records may
7 reflect the matter is sealed, an unsealing order entered months or years later may not be in the USAO file
8 (as happened in some instances described below) and only further research (such as a check of court
9 records using PACER as happened in some instances described below) might allow someone to
10 determine whether the matter was subsequently unsealed.

11 **The ACLU’S April 13, 2012 FOIA Request**

12 3. By letter dated April 13, 2012, plaintiffs American Civil Liberties Union of Northern
13 California and the San Francisco Bay Guardian (collectively the “ACLU”) sent a 4-part FOIA request to
14 the United States Attorney for the NDCA and to the Department of Justice. *See* Exhibit A attached
15 (without exhibits). This declaration pertains only to the first part of the ACLU’s 4-part request which is
16 for “[a]ll requests, subpoenas, and applications for court orders or warrants seeking location information
17 since January 1, 2008.” The ACLU defined “location information” as used in its FOIA request to mean:

18 any information that helps to ascertain the location of an individual or
19 particular electronic device that, in whole or in part, is generated or
20 derived from the operation of an electronic device, including but not
21 limited to a cell phone, smartphone, cell site, global positioning system,
22 cell-site simulator, digital analyzer, stingray, triggerfish, amberjack,
23 kingfish loggerhead, or other electronic device, including both historical
24 and real-time information.

25 *See* Exhibit A, at 3. In this declaration, when I refer to applications for court orders seeking location
26 information, I am using that as short hand to refer to Part 1 of the ACLU FOIA request.

27 **Difficulty of Searching for Documents Responsive to Part 1**

28 4. Part 1 of the ACLU FOIA request asks for responsive documents matters pending on
January 1, 2008. The USAO cannot determine from its paper filing system which matters were actually
pending on January 1, 2008. The USAO has no central, searchable, electronic filing system in which it

1 maintains copies of records. Nor can the USAO's Information Technology Staff ("IT Staff") use our
2 case management system, also known as the Legal Information Office Network System ("LIONS"), to
3 obtain a snapshot of how many, or which, matters were pending on January 1, 2008. LIONS is an
4 electronic tracking system for cases that is more akin to an indexing system; it does not store
5 electronically the actual documents from matters assigned a USAO number.

6 5. The remainder of the ACLU's request in Part 1 is for applications and orders seeking
7 location tracking information filed since January 1, 2008. At the USAO, such requests take the form of
8 search warrants or pen registers which are but two investigative tools that prosecutors use to develop
9 evidence of criminal activities in a matter being investigated. The USAO, however, does not generally
10 file documents by the type of investigative tool that AUSAs use. Rather, the USAO generally maintains
11 its paper filing system in connection with the matter under investigation to which the USAO number is
12 assigned. Closed matters are stored at the USAO for approximately six months before being sent to the
13 Federal Records Center. A closed file is only retrievable by its USAO number. Of course, individual
14 AUSAs prepare documents for filing in court on their individual computers, but how each AUSA
15 electronically stores such documents, if at all, is a matter of personal preference. After an AUSA leaves
16 the office, a supervisor may opt to retain some of his or her files; otherwise, files on server backups are
17 destroyed within six months. Thus, the USAO is unable to identify and retrieve all documents
18 responsive to Part 1 of the ACLU FOIA request without manually retrieving and reviewing all the paper
19 files for all matters which have been opened since January 1, 2008. Considering that between January 1,
20 2008 and September 1, 2013, the USAO assigned new USAO numbers to 12,699 matters, a search
21 would be a gargantuan task. While some matters that were opened since 2008 may consist of a simple
22 folder, many matters turn into long term investigations and later cases which are ongoing for a number
23 of years, and the paper files associated with these matters can be voluminous, filling multiple bankers
24 boxes and in some cases entire storage rooms.

25 6. An application for an order seeking location tracking information takes the form of a
26 search warrant or a pen register, but search warrants and pen registers have wide spread use as criminal
27 investigative tools beyond just seeking court-ordered location tracking information. Thus, even if the
28

1 USAO could identify and locate all search warrants or pen registers, not all of them would be responsive
2 to Part 1. The frequency that an application for an order seeking location tracking information is used as
3 an investigative tool depends on the type of criminal investigation involved. For example, AUSAs
4 developing white collar cases involving economic crimes or securities fraud, as well as those
5 investigating criminal matters involving national security, make far fewer applications for location
6 tracking information than do AUSAs developing criminal cases involving street gangs, violent crimes or
7 drug trafficking. For the latter AUSAs, the use of pen registers and search warrants is an essential
8 investigative technique. Thus, looking for responsive records in the files generated in connection with
9 the investigation of economic crimes, securities fraud or national security matters would be like looking
10 for needles in a haystack – requiring a search of the entire, often voluminous, file even though that file
11 may have few or no documents responsive to Part 1 of the ACLU's request. Further complicating a
12 search are the practices among Criminal Sections in the USAO and among the AUSAs within those
13 sections as to whether they obtain a new USAO number when applying for orders, including orders
14 seeking location tracking information, or whether they make applications for orders using a USAO
15 number already assigned to an investigation. There is no uniform office practice.

16 7. When using investigative tools such as applying for an order seeking location tracking
17 information, the general practice at the USAO is also to apply to seal the application (if any), affidavit
18 (if any) and order. A sealing order prohibits the USAO from disclosing sealed documents to the public.
19 Sealing investigative tools requiring a court order – such as applications and orders seeking location
20 tracking information – is critical. AUSAs who apply for such orders do so to develop evidence of the
21 criminal activities of one or more targets who likely are unaware of the investigation. Sealing the
22 applications and orders avoids jeopardizing the investigation by its premature disclosure. Even after the
23 indictment of one target, the AUSA often has an interest in not letting the target's associates who are
24 still under investigation become aware of specific investigative techniques which the AUSA may
25 continue to use to develop evidence of criminal activities. In a complex, multi-year, investigation, there
26 are often multiple defendants who could include fugitives from whom the AUSA wants to withhold the
27 investigative techniques used. The sealed applications for location tracking information may be
28

1 supported by affidavits which identify confidential informants (“CIs”) or confidential sources (“CSs”),
2 or include information which could lead to the identification of those CIs or CSs. Disclosure could
3 endanger the CIs or CSs, particularly in investigations involving street gangs, violent crimes and drug
4 trafficking. Finally, as described below, of the files the USAO identified as possibly containing
5 applications and orders for location tracking information, the supervisor of OCDETF/Narcotics
6 determined that approximately 50% of those files involve open, ongoing OCDETF/Narcotics
7 investigations which may be subject to withholding under Exemption 7, and supervisors from other
8 sections have not yet reviewed the other 50% of the files to determine how many of those files involve
9 open, ongoing investigations in other sections.

10 8. There is no uniform practice in the USAO for opening or closing matters which use
11 investigative techniques such as sealed applications and orders seeking location tracking information.
12 For example, the general practice in OCDETF/Narcotics is to obtain a new USAO number for each
13 application for a pen register or search warrant, including those seeking location tracking information,
14 and to close the matter at the end of the time period for which the order authorized use of a particular
15 device (including extensions), even though the related investigation under a separate USAO number
16 may be ongoing for a considerable amount of time. In other sections, such as Special Prosecutions/
17 National Security and Economic Crimes/Securities Fraud, the usual practice appears to be to use the
18 same USAO number of the underlying investigation when applying to the court for a sealed order
19 seeking location tracking information. That said, the actual practice used can vary from attorney-to-
20 attorney and case-to-case.

21 9. There is no systematic review on an ongoing basis of the sealed applications to determine
22 whether the conditions requiring sealing continue, and such a review would be impractical, particularly
23 in investigations or cases which continue for several years. It is difficult, years after the sealing of
24 applications and orders, to determine the potential harm from the unsealing of these documents even if
25 the AUSA is still in the office and the agent is in the area. Often the agent or AUSA originally handling
26 the application (or both) has become unavailable. Nevertheless, the need to keep confidential

27 ///

28

1 information regarding confidential sources and informants does not necessarily diminish with the
2 passage of time, even though the USAO's ability to evaluate that need does diminish with time.

3 10. During the course of working on the USAO's response to Part 1 of the ACLU's FOIA
4 request, I am aware of only one exception to the general practice of asking the Court to seal an
5 application for an order seeking location tracking information. In one case, an AUSA made two
6 applications for orders to obtain location tracking information without requesting the Court to seal those
7 applications and orders. In that case, the AUSA did not request sealing because the target knew of the
8 investigation. We have produced those two applications and orders to the ACLU in response to Part 1
9 by letter dated September 13, 2013.

10 **Searches to Identify and Locate Part 1 Documents**

11 11. Because of the impractical task of searching paper files for documents responsive to Part
12 1, the USAO explored using its electronic case management system, LIONS, to identify files in which
13 there might be documents responsive to Part 1 of the ACLU's FOIA request. To do so, the USAO
14 leadership developed a list of search terms and the USAO IT Staff, using those terms, conducted key
15 word searches of the "caption" field and the "comment" field in LIONS for the period from January 1,
16 2008 through January 3, 2013 – the same search period that the parties agreed to in conducting the
17 search for documents responsive to Parts 2 through 4 of the ACLU's FOIA request.

18 12. The search terms were developed by knowledgeable AUSAs and supervisors and shared
19 with the ACLU. Additional terms were used based on input from the ACLU. Initially, the USAO
20 searched only the "caption" field, a required field, but later added a search of the "comment" field, an
21 optional field, at the request of the ACLU. Because the search function could not be used to do a single
22 search in both fields, the IT Staff performed a search in each field and spent several hours eliminating by
23 hand the duplicate entries.

24 13. The search terms, which follow, are ones that are believed to have been most likely used
25 by AUSAs and USAO docket clerks in the "caption" field when opening new matters involving
26 applications for orders seeking location tracking information, and also by AUSAs in the "comment"
27 field when updating matters in connection with the same type of applications:

28 ///

1 GPS
cell
2 location
phone
3 2703
track
4 triggerfish
stingray
5 witt
kingfish
6 amberjack
digital
7 loggerhead
ping
8 slap
Rule 41
9 monitor
pen register
10 global positioning system
mobile

11 The IT Staff used a search function that would locate the word as well as variations on the word. Thus,
12 by using "track," the search identified files which contained the words "mobile tracking," "tracking
13 mission" or "tracking device." Similarly, the use of "cell," the search would have identified files which
14 had the words "cell site" or "cell sites." And, use of "digital" as a search term would have retrieved files
15 which had the words "digital analyzer." Despite best efforts, the search using these key words likely
16 was under inclusive. If the AUSA or the USAO's docketing clerks failed to use the above key words
17 either when opening a matter, or when the AUSA inserted comments on a case which involved an
18 application for location tracking information, then the search would not have identified that matter.
19

20
21 14. The "caption" field is a required field for AUSAs to fill out when opening a matter under
22 a new USAO number. Once the AUSA completes the form, a USAO docketing clerk inputs the
23 information from the form into LIONS in the "caption" field. The "comment" field, however, is not a
24 required field and often AUSAs do not use software in managing their cases. An AUSA who chooses to
25 update cases using the software inputs status information about the matter that the AUSA is handling
26 into a computerized system which acts as an overlay to LIONS. Such information could include, among
27 other things, a plan to use, or the actual use of an investigative tool, such as applying for a sealed order
28

1 seeking location information. Once inputted through the overlay, the information appears in the
2 “comment” field of LIONS. Despite best efforts, the search using these fields was under inclusive.
3 Many, if not most, AUSAs do not use the optional software to manage their cases and, thus, if an AUSA
4 in the midst of an investigation decides to use as an investigative tool a search warrant or pen register
5 seeking location tracking information, that information would not be in LIONS unless the AUSA
6 opened a new USAO number for that search warrant or pen register.

7 15. The result of the search was to identify 1184 matters by USAO numbers in which a
8 search term was used. For each of these 1184 matters, we obtained, among other things: caption
9 information, the court docket number (when available), the Criminal Section in which the matter was
10 opened, the AUSA’s name and the comments that the AUSA inputted if that AUSA opted to do so.
11 Although 1184 matters were identified by USAO number, the search produced key words in 3692 lines
12 of data because of multiple hits for a single USAO number. The multiple hits for a single USAO
13 number are because of entries into the “comment” field by AUSAs who do use the optional software to
14 manage their cases. A cursory review of entries shows that not all entries which have the key word
15 identify an application for an order for location tracking information. For example, one entry indicated a
16 plan to use a particular investigative tool in the future. Thus, additional entries for a single USAO
17 number do not necessarily indicate additional applications for location tracking information.

18 16. The search was substantially overly inclusive. The Chief of the Criminal Division spent
19 a considerable amount of time for someone in a senior management position – close to 8 hours –
20 reviewing information from the 1184 matters identified by USAO number and was able to conclude
21 reasonably, without retrieving the files, that approximately one third of the 1184 matters (424) likely do
22 not have responsive documents. To give just one example, the comment section in one matter stated:
23 “The defedant shll prtptcte in the location monitoring prgm for a prd of six months, directed by the po,
24 and abide by the rules of the program.” Although the comment used a form of the word “monitor,” the
25 context makes clear that defendant was participating in program supervised by the Probation Officer
26 where the defendant was monitored for a period of time.

27 ///

28

1 17. Of the 760 remaining USAO matters identified, the Chief of OCDEFT/Narcotics who
2 spent a number of hours analyzing the information determined that approximately 50% (386) are USAO
3 numbers assigned to open, ongoing investigations which may be subject to claims of Exemption 7. As
4 to the remaining 374 matters, other Section Chiefs have not yet reviewed the information to determine
5 how many of the matters identified involve open, ongoing investigations in their respective Sections
6 which may also be subject to claims of Exemption 7, but it is reasonably anticipated there are more
7 matters involved in open, ongoing investigations.

8 **The General Practice of AUSAs is to Obtain a Sealing Order for Search Warrants**
9 **And Pen Registers, Including those Seeking Location Tracking Information**

10 18. Knowledgeable managers, supervisors and AUSAs confirmed that when developing
11 evidence using an investigative tool, such as a search warrant or pen register, including those seeking
12 location tracking information, that they ask the court to seal the application and order. Various statutes
13 are cited as the authority for sealing a file, including 18 U.S.C. § 2705(b) and 18 U.S.C. § 3123(d).

14 19. As mentioned, 760 matters were identified through the LIONS search as possibly having
15 responsive documents to Part 1 of the ACLU's request. One piece of information requested when the
16 search was conducted was court information, if any, that had been input into LIONS. A DOJ lawyer and
17 DOJ paralegal used the docket number, when provided, for a matter to search the Court's electronic
18 filing system also known PACER (Public Access to Court Records). In 566 of the 760 matters, PACER
19 returned the message "Case Under Seal," confirming the general practice in the USAO of sealing the
20 files. In 115 of the 760 matters, PACER returned the message "Cannot find case." In 73 of the 760
21 matters, the LIONS database did not include a docket number and, thus, there was no way to conduct a
22 PACER search. In the remaining six files, PACER returned a message which suggested that the matter
23 on file was public.

24 20. From the 115 matters that PACER could not find, the USAO using the matter's USAO
25 number retrieved a random, 10% sample – a total of 12 matters. The purpose in retrieving the matters
26 was to review them to determine whether the files contain applications for an order seeking location
27 information along with an order and, if so, to confirm whether the AUSA who sought the order also
28

1 obtained a sealing order. I found 11 matters involved applications for orders seeking location tracking
2 information for which a sealing order was obtained and which, based on the information in the file,
3 appear to remain under seal from the public. The remaining matter retrieved had no documents in the
4 file, albeit the file cover suggested that the matter involved an application for an order seeking location
5 tracking information.

6 21. From the 73 matters for which there was no court docket number to search, the USAO
7 using the matter's USAO number retrieved a random, 10% sample – seven matters. Again, the purpose
8 in retrieving the matters was to review them to determine whether the files contain applications for an
9 order seeking location information along with an order and, if so, to confirm whether the AUSA who
10 sought the order also obtained a sealing order. I found that four of the matters retrieved did not involve
11 an application for an order seeking location tracking information (and therefore not responsive to Part 1
12 of the ACLU request). The remaining three matters retrieved did include a total of 19 applications and
13 orders for location tracking information for which a sealing order was obtained and which, based on the
14 information in the file, appear to remain under seal from the public.

15 22. As to the six matters which appeared in PACER not to be sealed, the USAO retrieved its
16 copy of the six files – one file had two responsive applications and orders under seal with an unsealing
17 order; one file had one responsive application and order under seal as well as an unsealing order; one file
18 had no court documents in it; one file had a single page of a sealed order for location tracking
19 information; and the last two files had responsive applications and orders which were never sealed. As
20 previously mentioned as to the last two responsive applications that were never sealed, the AUSA did
21 not request the Court to seal the applications and orders because the target was aware of the
22 investigation. *See* ¶ 11, *supra*. In the file with two sealed responsive applications and orders from July
23 2008, I found that the Court unsealed that file three years later in August 2012 at the request of the then
24 Deputy Criminal Chief J. Douglas Wilson in connection with an Arizona criminal case. Before applying
25 to unseal the documents, the Deputy Criminal Chief consulted with the agency which he considered
26 essential and, in this case, the agency acquiesced in the unsealing of the matters. The ACLU obtained
27 those documents at about the same time, in August 2012. Of note, however, are the two USAO files –
28

1 one of which had no documents in it and the other of which had a single page which appeared to be the
2 first page of an order authorizing location tracking information. I had no way of determining if the
3 USAO file with no documents should have had documents that were responsive, whether the documents
4 were sealed or whether, at a later date, the documents had been unsealed. As to the file with a single
5 page of sealed order for location tracking information, there was no application and I had no way of
6 determining if the sealed order had been later unsealed. Although the docket was unsealed in PACER,
7 there were no links to retrieve any documents. I asked a clerk to go to the Court in San Jose to review
8 the two files, copy the sealed applications and orders for location tracking information and copy also the
9 unsealing orders.

10 23. On September 13, 2013, the Department of Justice released the unsealing orders and the
11 seven previously sealed applications and orders (two in their entirety and the remaining five with minor
12 redactions pursuant to Exemption 7(C) to protect against an unwarranted invasion of personal privacy).
13 The released documents reflect yet another difficulty in searching for documents responsive to Part 1.
14 When the AUSAs place a copy of the sealed application and order in their files at the time the
15 application was made, the documents are stamped by the Court as sealed. Months or years later, if the
16 Court unseals documents, there is only the unsealing order and no indication on the sealed documents
17 themselves that they have later been unsealed. Thus, the USAO can only determine that the sealed
18 documents have been unsealed by finding a subsequent unsealing order which months or years later may
19 not be in the USAO file, particularly in the case of matters which were closed out shortly after the
20 sealing order was obtained. The documents disclosed on September 13, 2013 provide examples of this.

21 * * * * *

22 I, Patricia J. Kenney, declare pursuant to 28 U.S.C. § 1746 on information and belief that the
23 foregoing is true and correct. Executed in San Francisco, California, this 20th day of September, 2013.

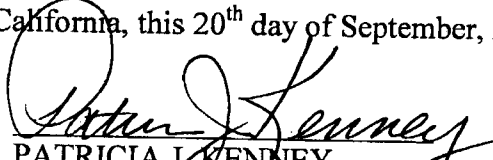
24 
25 PATRICIA J. KENNEY
26 Assistant United States Attorney
27
28

EXHIBIT A



2/17/12 11:15

April 13, 2012

Via Certified Mail

Melinda Haag
United States Attorney
Northern District of California
Federal Courthouse
450 Golden Gate Avenue, 11th Floor
San Francisco, CA 94102

Office of Public Affairs
United States Department of Justice
950 Pennsylvania Ave, NW, Room 1128
Washington, DC 20530

Re: Freedom of Information Act Request regarding location tracking
Expedited Processing Requested

Dear Ms. Haag,

The American Civil Liberties Union of Northern California (ACLU-NC) and *San Francisco Bay Guardian (Bay Guardian)* submit this expedited Freedom of Information Act (FOIA) request for records in the possession of the United States Attorneys' Office for the Northern District of California pertaining to efforts to seek or obtain location information. We submit this request pursuant to the FOIA, 5 U.S.C. § 552, implementing regulations 28 CFR §16.1 *et seq.*, and any other applicable regulations.

Recent revelations have made clear that government agencies are engaged in seeking and acquiring the location information of individuals for tracking and surveillance purposes, utilizing varying technologies and varying legal standards that frequently fall short of constitutional protections designed to protect the public from intrusive government searches. Previous ACLU Freedom of Information Act requests have revealed that the Department of Justice has maintained since at least 2007 that the government need not obtain a warrant and show probable cause to track people's location with only one exception: real-time GPS and triangulation data, and that U.S. Attorneys around the country are only encouraged to obtain a warrant based on probable cause prior to engaging in precise cell phone tracking.¹ FOIA requests have also revealed that some U.S. Attorney offices do not even comply even with this set of guidelines.²

¹ Email from Brian Klebba, *GPS or "E-911-data" Warrants*, November 17, 2009, available at http://www.aclu.org/pdfs/freespeech/cellfoia_dojrecommendation.pdf.

² Letter from William G. Stewart II, to Catherine Crump, *Mobile Phone Tracking (Items 3-5)/DNJ*, Dec. 31, 2008, available at http://www.aclu.org/pdfs/freespeech/cellfoia_released_074132_12312008.pdf; Letter from William G. Stewart II to Catherine Crump, *Mobile Phone Tracking(Items 3-5)FLS*, Dec. 31, 2008, available at http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf.

MICHELLE A. WELSH, CHAIRPERSON | DENNIS McNALLY, AJAY KRISHNAN, FARAH BRELVI, ALLEN ASCH, VICE CHAIRPERSONS | KENNETH SUGARMAN, SECRETARY/TREASURER
ABDI SOLTANI, EXECUTIVE DIRECTOR | KELLI EVANS, ASSOCIATE DIRECTOR | CHERI BRYANT, DEVELOPMENT DIRECTOR | SHAYNA GELENDER, ORGANIZING & COMMUNITY ENGAGEMENT DIRECTOR
A SAPONARA, COMMUNICATIONS DIRECTOR | ALAN SCHLOSSER, LEGAL DIRECTOR | MARGARET C. CROSBY, ELIZABETH OILL, LINDA LYE, JULIA HARUMI MASS, MICHAEL RISHER, JORY STEELE, STAFF ATTORNEYS
PHYLLIDA BURLINGAME, ALLEN HOPPER, NATASHA MINSKER, NICOLE A. OZER, DIANA TATE VERMEIRE, POLICY DIRECTORS | STEPHEN V. BOMSE, GENERAL COUNSEL

April 13, 2012
Page 2

In December 2009, it was revealed that telecommunications provider, Sprint Nextel, received over 8 million demands from government agencies for access to customer location information between September 2008 and October 2009.³ In September 2011, it was also revealed that federal authorities had utilized a “stingray” device to track a mobile device and locate an individual in a California home.⁴

Following the Supreme Court’s January 23, 2012 decision in *United States v. Jones*, U.S., 132 S.Ct. 945 (2012), in which the Court unanimously held that it was unconstitutional to install a global positioning device (GPS) on an individual’s car and utilize it to track the individual for 28 days without a warrant, the FBI was forced to turn off nearly 3,000 active GPS devices in the field.⁵ On April 4, 2012, the American Civil Liberties Union released findings from a 32-state coordinated public records act request seeking the policies, procedures, and practices of state and local law enforcement agencies related to cell tracking, revealing that many government entities were violating the privacy rights of Americans by obtaining location information without a probable cause warrant.⁶

There has been widespread media interest and public concern related to government tracking and surveillance of location information. There is also great urgency to inform the public about governmental efforts to track and surveil individuals because members of Congress and California state legislators are currently weighing new laws related to location tracking – and information shedding lights on the government’s current practices would inform those pending legislative debates. It is imperative that Northern California community members and policymakers representing this region immediately gain a full and complete understanding of how the United States Attorneys for the Northern District are seeking or obtaining location information and whether these activities comport with constitutional rights. Access to this information is necessary for a meaningful and informed public debate over these pressing public policy issues and pending legislative debates.

I. REQUEST FOR INFORMATION

We request disclosure of agency records⁷ in your possession created since January 1, 2008,⁸ pertaining to efforts to seek or obtain location information utilizing any means.

³ <http://www.wired.com/threatlevel/2009/12/gps-data/>

⁴ See Jennifer Valentino-Devries, “‘Stingray’ Phone Tracker Fuels Constitutional Clash,” *Wall Street Journal*, September 21, 2011 (Tab 35).

⁵ FBI General Counsel Andrew Weissmann. <http://news.yahoo.com/supreme-court-ruling-prompts-fbi-turn-off-3-154046722-abc-news.html>

⁶ <http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request>

⁷ The term “records” as used herein includes all records preserved in written or electronic form, including but not limited to: court filings, correspondence, documents, data, videotapes, audio tapes, emails, faxes, files, guidance, guidelines, evaluations, instructions, analyses, memoranda, agreements, notes, orders, policies, procedures, protocols, reports, rules, training materials, manuals, studies, text messages, social networking posts or messages. To the extent the agency chooses to redact identifying information of individuals, we request that individuals be identified with an alphanumeric code so that multiple records related to the same individual can be recognized as such.

April 13, 2012
Page 3

“Location information” as used in this request means any information that helps to ascertain the location of an individual or particular electronic device that, in whole or in part, is generated or derived from the operation of an electronic device, including but not limited to a cell phone, smartphone, cell site, global positioning system, cell-site simulator, digital analyzer, stingray, triggerfish, amberjack, kingfish loggerhead, or other electronic device, including both historical and real-time information.

In particular, we seek the following:

- 1) All requests, subpoenas, and applications for court orders or warrants seeking location information since January 1, 2008.
- 2) Any template applications or orders that have been utilized by United States Attorneys in the Northern District to seek or acquire location information since January 1, 2008.
- 3) Any documents since January 1, 2008, related to the use or policies of utilizing any location tracking technology, including but not limited to cell-site simulators or digital analyzers such as devices known as Stingray, Triggerfish, AmberJack, KingFish or Loggerhead.
- 4) Any records related to the Supreme Court’s holding in *United States v. Jones*, excluding pleadings or court opinions filed in the matter in the Supreme Court or courts below.

II. REQUEST FOR EXPEDITED PROCESSING

Requesters seek expedited processing. This request should be granted because there is widespread media interest in government surveillance methods using new technology to collect detailed, sensitive, personal information, and there is urgency to inform the public about the scope of the government’s practices because of pending legislation on these very issues. The information sought in this request is necessary to contribute to that pending legislative debate.

Title 5 U.S.C. §552(a)(6)(E) provides for expedited processing of requests for information in cases in which the person requesting the records demonstrates a compelling need. Department of Justice regulations state that FOIA requests are entitled to expedited processing when information requested involves “[a] matter of widespread and exceptional media interest in which there exist possible questions about the government’s integrity which affect public confidence.” 28 CFR §16.5(d)(1)(iv). In addition, for requests by persons primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged federal government activity constitutes a “compelling need.” 5 U.S.C. §552(a)(6)(E)(v)(II); 28 CFR §16.5(d)(1)(ii).

A. Widespread and exceptional media interest

⁸ Requestors seek records located either at the United State Attorneys’ Northern District San Francisco, Oakland or San Jose offices, or at any other location where records are stored.

April 13, 2012

Page 4

The federal government's surveillance and tracking of individuals using invasive new technologies but without satisfying the Fourth Amendment's requirements for obtaining warrants based on probable cause is a matter of great public concern. Whether and to what extent the United States Attorney for the Northern District of California is seeking or obtaining location information without a probable cause warrant are matters of great public concern. There are dramatic implications for core democratic values when the federal government engage in location surveillance to spy on ordinary members of the public, critics, dissidents, and those who espouse unpopular views, without adequate judicial oversight. As demonstrated by the extensive coverage of this issue, there is widespread media interest regarding governmental collection of location information.

Location information is very sensitive information and can reveal far more than just an individual's latitude and longitude. As the United States Court of Appeals for the D.C. Circuit explained in 2010 in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010):

"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." *Id.* at 562.

As a result, the media has extensively covered the government's use of location tracking devices, and its efforts to do so without obtaining a warrant based on probable cause. *See, e.g.*, Robert Barnes, "Supreme Court: Warrants needed in GPS tracking," *Washington Post*, January 23, 2012 (Tab 1); Rebecca J. Rosen, "Why the Jones Supreme Court Ruling on GPS Tracking Is Worse Than It Sounds," *The Atlantic*, January 23, 2012 (Tab 2); Ariane de Vogue, "GPS Tracking Requires Warrant, Supreme Court Rules," *ABC*, January 23, 2012 (Tab 3); Barry Friedman, "Privacy, Technology and Law," *New York Times*, January 29, 2012 (Tab 4); Greg Stohr, "Police Use of GPS Devices to Track People Limited by U.S. Supreme Court," *Bloomberg*, January 23, 2012 (Tab 5); Jess Bravin, "Justices Rein In Police on GPS Trackers," *Wall Street Journal*, January 24, 2012 (Tab 6); Editorial, "Navigating the Supreme Court's GPS ruling," *Los Angeles Times*, January 25, 2012 (Tab 7); Bob Egelko, "U.S. Supreme Court to decide major legal issues," *San Francisco Chronicle*, September 30, 2011 (Tab 8); Editorial, "The Court's GPS Test," *New York Times*, November 5, 2011 (Tab 9); David G. Savage, "Supreme Court: warrant required for GPS tracking," *San Francisco Chronicle*, January 24, 2012 (Tab 10); Cristian Salazar, "ACLU demands police disclose cell phone tracking," *San Francisco Chronicle*, August 4, 2011 (Tab 11); Adam Liptak, "Court Case Asks if 'Big Brother' Is Spelled GPS," *New York Times*, September 10, 2011 (Tab 12); Editorial, "A court test of privacy in the digital age," *San Francisco Chronicle*, January 29, 2012 (Tab 13); Adam Liptak, "Justices Say GPS Tracker Violated Privacy Rights," *New York Times*, January 24, 2012 (Tab 14); Julia Angwin, "FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling," *Wall Street Journal*, February 25, 2012 (Tab 15); Joan Biskupic, "Supreme Court rules warrant needed for GPS tracking," *USA Today*, January 24, 2012 (Tab 16); Kashmir Hill, "Supreme Court Deals Blow To Government Surveillance, Saying Warrant Needed For GPS Tracking," *Forbes*, January 23, 2012 (Tab 17); Timothy B. Lee, "GPS ruling is 'hard' on the FBI—and that's a feature, not a bug," *Ars Technica*, March 23, 2012 (Tab 18); Renee Hutchins, "A step

April 13, 2012
Page 5

back for rights," *Baltimore Sun*, January 29, 2012 (Tab 19); Debra Cassens Weiss, "Jones Decision Spurs FBI to Disable 3,000 GPS Devices and to Consider Legality of Trash Can Trespass," *ABA Journal*, February 28, 2012 (Tab 20); Nina Totenberg, "High Court: Warrant Needed For GPS Tracking Device," *NPR*, January 23, 2012 (Tab 21); Carl Franzen, "What Does The Supreme Court Ruling Against Warrantless GPS Tracking Mean?," *Talking Points Memo*, January 23, 2012 (Tab 22); James Vicini, "Supreme Court rules police need warrant for GPS tracking," *Reuters*, January 24, 2012 (Tab 23); Bill Mears, "Justices rule against police, say GPS surveillance requires search warrant," *CNN*, January 23, 2012 (Tab 24); Mark Sherman, "Supreme Court questions warrantless GPS tracking," *Business Week*, November 8, 2012 (Tab 25); Alex Fitzpatrick, "Supreme Court: GPS Tracking Is Illegal Without Warrant," *Mashable*, January 23, 2012 (Tab 26); Kashmir Hill, "How Many GPS Trackers Is The FBI Actually Using?," *Forbes*, March 27, 2012 (Tab 27); Jim McElhatton, "Supreme Court says police need warrant for GPS tracking," *The Washington Times*, January 23, 2012 (Tab 28); Jessie J. Holland and Pete Yost, "Warrant needed for GPS tracking, high court says," *The Washington Times*, January 23, 2012 (Tab 29); Catherine Crump, "How GPS tracking threatens our privacy," *CNN*, November 7, 2011 (Tab 30); Adam Cohen, "The Government Can Use GPS to Track Your Moves," *Time*, November 25, 2010 (Tab 31); Timothy B. Lee, "Supreme Court ponders constitutionality of 24/7 GPS tracking," *Ars Technica*, November 1, 2011 (Tab 32); Joshua A. Engel, "In 'U.S. v. Jones,' Supreme Court Rules No Warrantless GPS Tracking," *Law.com*, January 23, 2012 (Tab 33); Dahlia Lithwick, "U.S. v. Jones: Supreme Court Justices Alito and Scalia brwl over technology and privacy," *Slate*, January 26, 2012 (Tab 34); Jennifer Valentino-Devries, "'Stingray' Phone Tracker Fuels Constitutional Clash," *Wall Street Journal*, November 21, 2011 (Tab 35); Lior J. Strailevitz, "Can the police keep up with Jones?," *Chicago Tribune*, January 27, 2012 (Tab 36); "Want to Use a GPS-Tracking Device? Get a Warrant, Supreme Court Tells Police," *PBS*, January 23, 2012 (Tab 37); "Can Feds track the GPS of every American?," *RT*, November 9, 2011 (Tab 38).

The government's efforts to use GPS devices to engage in location tracking without a warrant were recently rebuffed by the United States Supreme Court in *United States v. Jones, supra*. Following that decision, the media continued to report on the issue extensively, including the implications of the *Jones* decision for law enforcement and the fact that the *Jones* decision prompted an increased reliance by law enforcement on cell site location information. See, e.g., David Kravets, "After Car-Tracking Smackdown, Feds Turn to Warrantless Phone Tracking," *Wired*, March 31, 2012 (Tab 39); Editorial, "GPS and the Right to Privacy," *New York Times*, January 25, 2012 (Tab 40); John W. Whitehead, "U.S. v. Jones: The Battle for the Fourth Amendment Continues," *Huffington Post*, January 24, 2012 (Tab 41); Mike Sacks, "Warrantless GPS Tracking Unconstitutional, Supreme Court Rules," *Huffington Post*, January 23, 2012 (Tab 42); David Kravets, "Supreme Court Court Rejects Willy-Nilly GPS Tracking," *Wired*, January 23, 2012 (Tab 43); Dave Bohon, "More Police Agencies Using Warrantless Cell Phone Tracking in Surveillance," *The New American*, April 5, 2012 (Tab 44); Thomas Peracchio, "Supreme court ruling exposes many digital privacy issues," *The Examiner*, April 2, 2012 (Tab 45); Thomas Claburn, "Supreme Court Tackles GPS Tracking Vs. Privacy," *Information Week*, January 23, 2012 (Tab 46); Editorial, "EDITORIAL: Obama wants to track you," *Washington Times*, March 20, 2012 (Tab 47); Emily Babay, "After GPS tracking banned by court, privacy fight turns to cell phone data," *Washington Examiner*, April 1, 2012 (Tab 48).

April 13, 2012
Page 6

Most recently, the ACLU released a report shedding light on disturbing trend across the country of law enforcement agencies obtaining cell phone location information without probable cause warrants. The ACLU report was initially the subject of a front page *New York Times* article. See Eric Lichtblau, "Police Are Using Phone Tracking as a Routine Tool," *New York Times*, March 31, 2012 (Tab 102).

After the *New York Times* piece appeared, a flurry of news articles on the subject followed, as well as numerous editorials emphasizing the importance of a warrant requirement for cell phone location information. See, e.g., Cristian Salazar, "ACLU demands police disclose cell phone tracking," *San Francisco Chronicle*, August 4, 2011 (Tab 49); James Temple, "How California cops grab phone data from Apple, Google, carriers," *San Francisco Chronicle*, April 3, 2012 (Tab 50); Suzy Khimm, "ACLU: Local police departments tracking cellphones without warrants," *Washington Post*, April 2, 2012 (Tab 51); Declan McCullagh, "How Apple and Google help police bypass iPhone, Android lock screens," *CNET*, April 2, 2012 (Tab 52); Athima Chansanchai, "ACLU: Police track cellphones, too," *MSNBC Technology*, April 2, 2012 (Tab 53); Bob Sullivan, "Pricey 'stingray' gadget lets cops track cellphones without telco help," *MSNBC Red Tape*, April 3, 2012 (Tab 54); Peter Doocy, "Law enforcement under scrutiny by ACLU for tracking cell phones," *Fox News*, April 4, 2012 (Tab 55); American Foreign Press, "Many US police use cell phones to track: study," *American Foreign Press*, April 2, 2012 (Tab 56); Gary Johnson, "Privacy: Ditch the Cell Phone or Prepare to Disrobe," *Huffington Post*, April 5, 2012 (Tab 57); Adam Levine, "The New American Pie: Breached, Tracked and Strip Searched," *Huffington Post*, April 5, 2012 (Tab 58); Josh Gerstein, "Key Patriot Act opinions may not be classified," *Politico*, March 16, 2012 (Tab 59); Editorial, "EDITORIAL: Individual cell phone privacy is compromised," *Fresno Bee*, April 11, 2012 (Tab 60); Brendan Sasso, "ACLU report: Warrantless tracking of cellphones 'pervasive and frequent'," *The Hill*, April 2, 2012 (Tab 61); James Temple, "Why cell-phone tracking should require a warrant," *San Francisco Chronicle*, April 2, 2012 (Tab 62); John Moe, "Warrantless cell phone tracking is everywhere," *Marketplace*, April 4, 2012 (Tab 63); Grant Gross, "ACLU: Most US Police Don't Seek Warrants Before Tracking Cell Phones," *PC World*, April 2, 2012 (Tab 64); Josh Smith, "ACLU: Most Police Departments Track Cellphones Without Warrants," *National Journal*, April 2, 2012 (Tab 65); Timothy B. Lee, "Documents show cops making up the rules on mobile surveillance," *Ars Technica*, April 3, 2012 (Tab 66); Jay Bookman, "The dangerous nexus of privacy, liberty and government," *Atlanta Journal Constitution*, April 2, 2012 (Tab 67); Anne Blythe, "Police scrutiny of mobile device data raises concerns," *News & Observer*, April 3, 2012 (Tab 68); Andy Greenberg, "These Are The Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps," *Forbes*, April 3, 2012 (Tab 69); Julian Sanchez, "Cell Phone Location Surveillance: Now at a Police Dept. Near You!," *Cato*, April 2, 2012 (Tab 70); Darlene Storm, "ACLU: Cops often violate Americans' privacy by warrantless cell phone tracking," *Computerworld*, April 2, 2012 (Tab 71); Debra Cassens Weiss, "Local Police Increasingly Use Cellphone Tracking, Sometimes Without a Warrant," *ABA Journal*, April 2, 2012 (Tab 72); David Dayen, "Pervasive Cell Phone Tracking Performed Even By Local Law Enforcement," *Firedoglake*, April 2, 2012 (Tab 73); Kevin Gosztola, "ACLU: US Law Enforcement Often Track Cell Phones Without a Warrant," *Firedoglake*, April 2, 2012 (Tab 74); Jacob Sullum, "ACLU Says Police Often Obtain Cellphone Location Data Without Warrants," *Reason*, April 2,

April 13, 2012
Page 7

2012 (Tab 75); Andrew Jones, "ACLU: Many local police tracking cell phones without warrants," *Raw Story*, April 2, 2012 (Tab 76); Tiffany Kaiser, "ACLU Finds U.S. Police Departments Using Cell Phone Tracking, Sometimes Warrantless," *Daily Tech*, April 4, 2012 (Tab 77); James Gaskin, "Cell phone tracking now routine police action," *IT World*, April 2, 2012 (Tab 78); Scott Daniels, "APD admits to tracking cell phones," *KRQE*, April 2, 2012 (Tab 79); Amy Gahrn, "ACLU: Most police track phones' locations without warrants," *CNN*, April 3, 2012 (Tab 80); Jennifer Waters, "Your cell phone is telling your secrets," *Market Watch*, April 6, 2012 (Tab 81); Helen A.S. Popkin, "Carriers charge cops for cellphone information," *MSNBC Technology*, April 4, 2012 (Tab 82); Jeff Homan, "Technology outpaces laws, raises concerns," *Collegiate Times*, April 5, 2012 (Tab 83); Mike Fossum, "How Cops Get Into Locked iPhone," *Web Pro News*, April 4, 2012 (Tab 84); Scott Schwebke, "ACLU questions cellphone tracking policies of law enforcement," *Standard*, April 4, 2012 (Tab 85); Viviane Vo-Duc, "ACLU: Many law enforcement agencies obtain cellphone tracking information without a warrant," *Deseret News*, April 5, 2012 (Tab 86); Robert Siegel, "Phone Tracking Big Business For Cell Companies," *NPR*, April 5, 2012 (Tab 87); Fox Report, "ACLU Claims Police are Tracking Cell Phones Without a Warrant," *Fox News Insider*, April 4, 2012 (Tab 88); Michael Santo, "ACLU-obtained documents show police use of cell phone tracking becoming routine," *Examiner*, April 1, 2012 (Tab 89); Editorial, "Editorial: Cell phone privacy is on the line," *Sacramento Bee*, April 8, 2012 (Tab 90); Jill Redhage, "Cellphone data draws scrutiny," *Daily Journal*, March 30, 2012 (Tab 91); Levi Sumagaysay, "Watching Big Brother: The cops and cell phones in the U.S., the U.K.'s monitoring plans," *Silicon Valley*, April 2, 2012 (Tab 92); Jack A. Smith, "BIG BROTHER'S GETTING BIGGER," *The People's Voice*, April 10, 2012 (Tab 93); Editorial, "Who's listening? Authorities engaging in cellphone tracking," *Las Vegas Review-Journal*, April 10, 2012 (Tab 94); Brian Duggan, "ACLU: Police using cellphone tracking, including RPD; Reno says court approval always obtained," *Montgomery Advertiser*, April 6, 2012 (Tab 95); Associated Press, "ACLU finds Nevada police use cellphone tracking," *Las Vegas Sun*, April 8, 2012 (Tab 96); "ACLU finds widespread warrantless cell phone tracking by local police," *Info Security*, April 3, 2012 (Tab 97); "Cop's 'ear' in your pocket: Cell phone tracking routine with US police," *RT*, April 1, 2012 (Tab 98); "ACLU: Many local police track cell phones without warrants," *Press TV*, April 2, 2012 (Tab 99); "ACLU: Cell phone tracking by police widespread," *Homeland Security News Wire*, April 4, 2012 (Tab 100); "Cell Phone Tracking Raises Eyebrows," *Fox News*, August 4, 2011 (Tab 101);

B. Urgency to inform the public

There is great urgency in shedding light on location tracking by the government. The information sought in this FOIA request would contribute to the ongoing national debate on this topic generally, as well as specific legislative debates over the legal standard that should apply when the government seeks location information.

Justice Alito in his concurring opinion in *Jones* urges legislative action, noting that "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way. To date,

April 13, 2012
Page 8

however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes.” 132 S.Ct. at 964.

Members of Congress representing Northern California, including Representatives Zoe Lofgren and Barbara Lee, are currently working on bipartisan efforts to pass a federal location privacy bill, the GPS Act,⁹ and state lawmakers, including State Senator Mark Leno, are working on state location privacy laws.¹⁰ There is great urgency in shedding light on whether the Department of Justice is adhering to constitutional standards: The information sought herein would contribute to ongoing societal and legislative debates and help the public and Bay Area policymakers assess what new laws should be implemented to better protect the public from “warrantless surveillance.” *Elec. Priv. Info. Ctr. V. Dept. of Justice*, 416 F.Supp.2d 30, 41 (D.D.C. 2006) (granting preliminary injunction requiring agency to produce information where FOIA request sought information “vital to the current and ongoing debate surrounding the legality of the Administration’s warrantless surveillance program”); *see also Elec. Frontier Fdn. V. Ofc. Of Dir. Of Natl. Intelligence*, 542 F.Supp.2d 1181, 1187 (N.D. Cal. 2008) (granting preliminary injunction requiring agency to produce information where “Congress is considering legislation that would amend the FISA and the records may enable the public to participate meaningfully in the debate over such pending legislation.”).

Further, requesters ACLU-NC and *Bay Guardian* are primarily engaged in disseminating information. The ACLU-NC is an affiliate of the ACLU, a national organization that works to protect the civil liberties of all people, including the safeguarding of the basic constitutional rights to privacy, free expression, and due process of law. The ACLU-NC is responsible for serving the population of northern California. The communications department of the ACLU-NC is the division of the ACLU-NC that is responsible for disseminating information to the public about issues of concern to the ACLU-NC and to the general public.

The *Bay Guardian* is the largest circulation newsweekly in northern California, with an audited weekly distribution of 100,000. Its website (sfbg.com) receives about 350,000 page views per month. The paper is locally owned, independent, and has been published continuously since 1966.

In short, expedited processing is warranted here because there is an urgency to inform the public about actual or alleged location tracking surveillance and requesters are primarily engaged in disseminating information. *See* 5 U.S.C. §552(a)(6)(E)(v)(II); 28 CFR §16.5(d)(1)(ii). Moreover, location tracking by the government is a matter of widespread and exceptional media interest. When the government utilizes technology to spy on citizens without adequate judicial oversight, the public confidence is deeply affected. *See* 28 CFR §16.5(d)(1)(iv). In this regard, this request is very similar other FOIA requests by ACLU-NC and *Bay Guardian*, seeking information about federal government surveillance practices and as to which the Department of

⁹ <http://www.govtrack.us/congress/bills/112/hr2168>

¹⁰ http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_bill_20120409_amended_sen_v98.html

April 13, 2012
Page 9

Justice (Federal Bureau of Investigation) granted expedited processing. See FOIA Request Nos. 1144839-00 & 1184877-000.¹¹

III. REQUEST FOR WAIVER OF PROCESSING FEES

We request a waiver of process fees. In a recent request by requesters ACLU-NC and *Bay Guardian*, the FBI granted the fee waiver. See FOIA Request No. 1144839-000. Such a waiver is appropriate here for two reasons.

First, the *Bay Guardian* and communications department of the ACLU-NC are "representative[s] of the news media." Fees associated with the processing of this request should therefore be "limited to reasonable standard charges for document duplication." 5 U.S.C. §552(a)(4)(A)(ii)(II).

As noted above, the *Bay Guardian*, is the largest circulation newsweekly in northern California, with an audited weekly distribution of 100,000. Its website receives about 350,000 page views per month. The paper is locally owned, independent, and has been continuously published since 1966. The paper covers breaking news, does detailed investigative reporting, publishes editorials and covers arts, entertainment and lifestyle issues. The *Bay Guardian* has received more than 100 state, local, and national awards for journalistic excellence. Executive Editor Tim Redmond, for example, is the recipient of the 2012 Professional Journalist award from the Society of Professional Journalists, Northern California Chapter, for his investigation of state agencies' legally questionable acquisitions of a drug used for lethal injections that is no longer produced in the United States, an investigative series based in part on documents uncovered by the *Bay Guardian* and ACLU-NC in FOIA requests to various federal agencies. The *Bay Guardian* is a member of the California Newspaper Publishers Association and the Association of Alternative Newsweeklies.

Similarly, the ACLU-NC's communication department publishes newsletters, news briefings, right to know materials, and other materials that are disseminated to the public. Its material is widely available to everyone, including tax-exempt organizations, not-for-profit groups, law students and faculty, for no cost or for a nominal fee. The ACLU-NC's communications department also disseminates information through the website <http://www.aclunc.org>, which had 127,475 visitors in 2011. This website addresses civil liberties issues in depth and provides features on civil liberties issues on which the ACLU-NC is focused. ACLU-NC staff persons are frequent spokespersons in television and print media and make frequent public presentations at meetings and events. Finally, the ACLU-NC's communications department disseminates information through newsletters which are distributed

¹¹ See also *ACLU-NC, et al. v. Dept. of Defense*, 2006 WL 1469418, Case No. 06-01698 (N.D. Cal. May 25, 2006) (ordering Department of Defense to comply with request for expedited processing by ACLU-NC and *Bay Guardian*).

April 13, 2012
Page 10

to subscribers by mail. Due to these extensive publication activities, the ACLU-NC is a "representative of the news media" under the FOIA and agency regulations.¹²

The records requested are not sought for commercial use.

Second, a fee waiver for duplication costs should be granted for the independent reason that disclosure of the requested information is in the public interest. *See* 5 U.S.C. §552(a)(4)(ii)(II)-(iii). It will further public understanding of government conduct, in particular, the Department of Justice's policies, practices, and methods of surveillance. The ACLU-NC's communications department is a division of a nonprofit 501(c)(3) organization, and both the ACLU-NC's communications department and the *Bay Guardian* are "representative[s] of the news media." They are well situated to disseminate information gained through this request to the public, to affected communities and to political and religious organizations.

If the fee waivers are denied, the requesters are prepared to pay fees up to \$25 and request to be informed of further fees that may be charged, but reserve the right to appeal a denial of fee waivers.

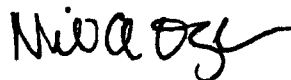
* * *

If this request for information is denied in whole or in part, we ask that you justify all deletions by reference to specific provisions of the Freedom of Information Act. We expect you to release all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information.

Thank you for your prompt attention to this matter. Please furnish all applicable records to Nicole Ozer, American Civil Liberties Union of Northern California, 39 Drumm Street, San Francisco, California, 94111, telephone 415 621 2493.

I affirm that the information provided supporting the request for expedited processing and the fee waiver is true and correct to the best of our knowledge and belief.

Sincerely,



Nicole A. Ozer
Technology and Civil Liberties Policy Director
ACLU of Northern California

Also on behalf of
San Francisco Bay Guardian

¹² Courts have found that organizations with missions similar to that of the ACLU and that engage in similar information dissemination activities are "primarily engaged in disseminating information." *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F.Supp.2d 246, 260 (D.D.C. 2005).