November 29, 2007

VIA FACSIMILE AND FEDERAL EXPRESS

Freedom of Information Operations Unit (SARO)
Drug Enforcement Administration
Department of Justice
700 Army Navy Drive
Arlington, VA 22202
Fax: 202.307.8556

Re: REQUEST UNDER FREEDOM OF INFORMATION ACT / Expedited Processing Requested

Attention:

This letter constitutes a request by the American Civil Liberties Union and the American Civil Liberties Union Foundation ("ACLU") under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 *et seq.*, and the Department of Justice implementing regulations, 28 C.F.R. § 16.1 *et seq.*[1]

I. The Request for Information

Recent court decisions and media reports reveal that law enforcement officers, frequently from the Drug Enforcement Administration ("DEA"), are obtaining information from mobile carriers that enable officers to track the location of individuals' mobile phones.[2] Court decisions indicate that the government claims not to need probable cause to obtain real-time tracking information. News reports further suggest that some United States Attorneys' Offices are violating a Department of Justice "internal recommendation" that "federal prosecutors seek warrants based on probable cause to obtain precise location data in private areas."[3] Also, news reports raise the possibility that

[1] The American Civil Liberties Union Foundation is a 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, and educates the public about civil rights and civil liberties issues. The American Civil Liberties Union is a separate non-profit, non-partisan, 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analyses of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

[2] Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444_2.html?hpid=topnews.

[3] *Id.*

on at least some occasions, law enforcement officers obtain tracking data directly from mobile carriers without any court involvement whatsoever.[4]

This request seeks information regarding these practices. Accordingly, the ACLU seeks disclosure of records regarding:

1. Policies, procedures, and practices followed to obtain mobile phone location information for law enforcement purposes;

2. The "internal recommendation" that "federal prosecutors seek warrants based on probable cause to obtain precise location data in private areas" described in Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007, attached as Appendix A;

3. Any violations of the "internal recommendation";

4. The number of times the government has applied for a court order, based on less than probable cause, authorizing it to obtain mobile phone location information, and whether such applications were successful;

5. The case name, docket number, and court of all criminal prosecutions, current or past, of individuals who were tracked using mobile location data, where the government did not first secure a warrant based on probable cause for such data.

II. Limitation of Processing Fees

The ACLU requests a limitation of processing fees pursuant to 5 U.S.C. § 552(a)(4)(A)(ii)(II) ("fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by . . . a representative of the news media . . .") and 28 C.F.R. §§ 16.11(c)(1)(i), 16.11(d)(1) (search and review fees shall not be charged to "representatives of the news media."). As a "representative of the news media," the ACLU fits within this statutory and regulatory mandate. Fees associated with the processing of this request should, therefore, be limited accordingly.

The ACLU meets the definition of a "representative of the news media" because it is "an entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn raw materials into a

[4] *Id.* ("Justice Department officials said to the best of their knowledge, agents are obtaining court approval unless the carriers provide the data voluntarily.")

distinct work, and distributes that work to an audience." *National Security Archive v. Department of Defense*, 880 F.2d 1381, 1387 (D.C. Cir. 1989).

The ACLU is a national organization dedicated to the defense of civil rights and civil liberties. Dissemination of information to the public is a critical and substantial component of the ACLU's mission and work. Specifically, the ACLU publishes newsletters, news briefings, right-to-know documents, and other educational and informational materials that are broadly disseminated to the public. Such material is widely available to everyone, including individuals, tax-exempt organizations, not-for-profit groups, law students and faculty, for no cost or for a nominal fee through its public education department. The ACLU also disseminates information through its heavily visited web site: http://www.aclu.org/. The web site addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The website specifically includes features on information obtained through the FOIA. *See, e.g.*, www.aclu.org/patriot_foia; www.aclu.org/torturefoia; http://www.aclu.org/spyfiles. The ACLU also publishes an electronic newsletter, which is distributed to subscribers by e-mail.

In addition to the national ACLU offices, there are 53 ACLU affiliate and national chapter offices located throughout the United States and Puerto Rico. These offices further disseminate ACLU material to local residents, schools and organizations through a variety of means including their own websites, publications and newsletters. Further, the ACLU makes archived material available at the American Civil Liberties Union Archives, Public Policy Papers, Department of Rare Books and Special Collections, Princeton University Library. ACLU publications are often disseminated to relevant groups across the country, which then further distribute them to their members or to other parties.

Depending on the results of the Request, the ACLU plans to "disseminate the information" gathered by this Request "among the public" through these kinds of publications in these kinds of channels. The ACLU is therefore a "news media entity." *Cf. Electronic Privacy Information Ctr. v. Department of Defense*, 241 F. Supp. 2d 5, 10-15 (D.D.C. 2003) (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the media" for purposes of FOIA).

Disclosure is not in the ACLU's commercial interest. The ACLU is a "non-profit, non-partisan, public interest organization." *See Judicial Watch*

Inc. v. Rossotti, 326 F.3d 1309, 1310 (D.C. Cir. 2003). Any information disclosed by the ACLU as a result of this FOIA will be available to the public at no cost.

III. Waiver of all Costs

The ACLU additionally requests a waiver of all costs pursuant to 5 U.S.C. § 552(a)(4)(A)(iii) ("Documents shall be furnished without any charge . . . if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester."). Disclosure in this case meets the statutory criteria, and a fee waiver would fulfill Congress's legislative intent in amending FOIA. *See Judicial Watch, Inc. v. Rossotti*, 326 F.3d 1309, 1312 (D.C. Cir. 2003) ("Congress amended FOIA to ensure that it be 'liberally construed in favor of waivers for noncommercial requesters.'").

Disclosure of the requested information will help members of the public understand the privacy risks of carrying a mobile phone. The government's policies and practices for monitoring the locations of mobile phones are unclear. It is not even apparent whether the government routinely obtains mobile phone location information without any court supervision whatsoever. Under these circumstances, there is little doubt that the requested information will "contribute significantly to public understanding." 5 U.S.C. § 552(a)(4)(A)(iii).

As a nonprofit 501(c)(3) organization and "representative of the news media" as discussed in Section II, the ACLU is well-situated to disseminate information it gains from this request to the general public and to groups that protect constitutional rights. Because the ACLU meets the test for a fee waiver, fees associated with responding to FOIA requests are regularly waived for the ACLU.[5]

---

[5] For example, in May 2005, the United States Department of Commerce granted a fee waiver to the ACLU with respect to its request for information regarding the radio frequency identification chips in United States passports. In March 2005, the Department of State granted a fee waiver to the ACLU with regard to a request submitted that month regarding the use of immigration laws to exclude prominent non-citizen scholars and intellectuals from the country because of their political views, statements, or associations. Also, the Department of Health and Human Services granted a fee waiver to the ACLU with regard to a FOIA request submitted in August of 2004. In addition, the Office of Science and Technology Policy in the Executive Office of the President said it would waive the fees associated with a FOIA request submitted by the ACLU in August 2003. In addition, three separate agencies – the Federal Bureau of Investigation, the Office of Intelligence Policy and Review, and the Office of

The records requested are not sought for commercial use, and the requesters plan to disseminate the information disclosed as a result of this FOIA request through the channels described in Section II. As also stated in Section II, the ACLU will make any information disclosed as a result of this FOIA available to the public at no cost.

IV. Expedited Processing Request

Expedited processing is warranted because there is "[a]n urgency to inform the public about an actual or alleged federal government activity" by organizations "primarily engaged in disseminating information." 28 C.F.R. § 16.5(d)(1)(ii).[6]

The overwhelming majority of Americans—over 200 million people—carry mobile phones.[7] This large number is steadily increasing. The information the ACLU seeks therefore bears on the privacy of a vast segment of the United States population.

The limited information currently available about the government's tracking practices raises serious questions about whether the government is complying with the law and the Constitution. The courts are divided on whether it is lawful for the government to track individuals without first obtaining a warrant based on probable cause. Several judges have held that the government lacks this authority.[8] It now seems likely that the government's view of its surveillance powers is even more expansive than

---

Information and Privacy in the Department of Justice – did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002.

[6] The ACLU is "primarily engaged in disseminating information," as discussed in Sections II and III.

[7] CTIA—The Wireless Association—Survey Results, June 2007, available at http://www.ctia.org/media/press/body.cfm/prid/1717.

[8] *See, e.g.*, In the Matter of the Application of the UNITED STATES of America for ORDERS AUTHORIZING the INSTALLATION and Use of PEN REGISTERS and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed], 416 F.Supp.2d 390, 391 (D. Md. 2006) ("Unless and until Congress takes further action, the court may only authorize disclosure of prospective cell site information upon a showing of probable cause pursuant to Rule 41."); In the Matter of an APPLICATION OF THE UNITED STATES FOR AN ORDER (1) AUTHORIZING THE USE OF A PEN REGISTER AND A TRAP AND TRACE DEVICE and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F.Supp.2d 294, 295 (E.D.N.Y. 2005) ("[E]xisting law does not permit the government to obtain the requested information on a prospective, real-time basis without a showing of probable cause.").

previously thought, and that it believes it can access such information without any court oversight whatsoever.

Given the pervasive nature of cell phone ownership, and the lack of clarity regarding the privacy individuals using cell phones can expect, there is "[a]n urgency to inform the public about an actual or alleged federal government activity." 28 C.F.R. § 16.5(d)(1)(ii).

This FOIA request is entitled to expedited processing for a second reason. The information sought relates to "a matter of widespread and exceptional media interest in which there exist possible questions about the government's integrity which affect public confidence." 28 C.F.R. § 16.5(d)(1)(iv).

The dubious legality of the government's actions, described above, raise questions about the government's integrity. Further, there is exceptional media interest in the government's tracking of mobile phones. The most recent rash of news coverage was prompted by the Washington Post story discussed above.[9] Newspapers across the country deemed the Washington Post article sufficiently important that it was reprinted in the Charlotte Observer, Chicago Tribune, Cincinnati Post, Houston Chronicle, Lexington Herald-Leader, Pittsburgh Post-Gazette, Seattle Times, South Florida Sun-Sentinel, and St. Paul Pioneer Press. Other publications ran their own stories on the subject.[10] National television stations immediately devoted coverage to the story.[11] The revelations in the Washington Post story prompted editorial boards around the country to voice concern over Justice Department practices.[12] This recent coverage is only the most current example of persistent press interest in the government's use of cell phones as tracking devices.[13] Of course, the more general issue of the government's expansive

---

[9] Ellen Nakashima, *Cellphone Tracking Powers on Request*, Washington Post, Page A01, Nov. 23, 2007, Appendix A.

[10] *Justice Department Defends Use of Cell-Phone Tracking Data*, Fox News, Nov. 24, 2007, at http://www.foxnews.com/story/0,2933,312647,00.html; *Feds Push for Real-Time Cell-Phone Tracking Data*, San Jose Mercury News, Nov. 23, 2007, at 4a; *Phone Tech Raises Privacy Concerns*, United Press International, Nov. 23, 2007.

[11] Cable News Network, Kelli Arena interviews Mark Rotenberg, Nov. 23, 2007, transcript available at 2007 WLNR 23221490; Fox News coverage, Nov. 23, 2007, transcript available at 2007 WLNR 23256527.

[12] Editorial, *Probable Abuse*, Albany Times Union, Nov. 27, 2007; Editorial, *Privacy Threat, Congress and the Judiciary Should Promulgate Tighter Rules for Government Access to Cell Phone Data*, Houston Chronicle, Nov. 25, 2007; Editorial, *Tracking You Down*, Syracuse Post-Standard, Nov. 25, 2007.

[13] Brendan I. Koerner, *Your Cellphone is a Homing Device*, Legal Affairs, July/August 2003; William B. Baker, *New York Case Tests Law of Surveillance on Cell Phone Location Data*,

view of its surveillance powers has been the subject of sustained news coverage, extensive congressional oversight hearings, and numerous lawsuits throughout the country.

The ACLU expects the determination of this request for expedited processing within 10 calendar days and the determination of this request for documents within 20 days. *See* 28 CFR § 16.5(d)(4); 5 U.S.C. § 552(a)(6)(A)(i). If this request is denied in whole or in part, we ask that you justify all deletions by reference to specific exemptions to FOIA. We request the release of all segregable portions of otherwise exempt material. The ACLU reserves the right to appeal a decision to withhold any information or to deny a waiver of fees.

Thank you for your prompt attention to this matter. Please furnish all applicable records to:

Catherine Crump
Staff Attorney
American Civil Liberties Union Foundation
125 Broad Street, 17th floor
New York, NY 10004

Privacy in Focus, Sept. 2005; Declan McCullagh, *Police Blotter: Cell Phone Tracking Rejected*, CNET News.com, Sept. 2, 2005, at: http://www.news.com/Police-blotter-Cell-phone-tracking-rejected/2100-1030_3-5846037.html; Al Gidari, *Yet Another Court Rules that Disclosure of Cell Site/Location Information Requires Probable Cause Showing*, Digestible Law: Perkins Coie's Internet Case Digest, Oct. 21, 2005; Ryan Singel, *U.S. Cell-Phone Tracking Clipped*, Wired, Oct. 27, 2005; Anita Ramasastry, *Every Move You Make, Part Three: Why Law Enforcement Should Have to Get a Warrant Before Tracking Us Via our Cell Phones*, FindLaw.com, Nov. 10, 2005, at: http://writ.news.findlaw.com/ramasastry/20051110.html; Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, New York Times, Dec. 10, 2005, at A1; Neal Conan, *NPR Talk of the Nation: Surveillance Via Cell Phone*, National Public Radio, Dec. 14, 2005; Tresa Baldas, *Feds' Cell Phone Tracking Divides the Courts*, The National Law Journal, Jan. 19, 2006; Scott Cameron, *Your Cell Phone Is A Homing Beacon – Should The Government Be Allowed To Use It Without Showing Probable Cause?*, The IP Law Blog, April 12, 2006; Stephen V. Treglia, *Trailing Cell Phones: Courts Grapple With Requests from Prosecutors Seeking Prospective Tracking*, New York Law Journal, July 18, 2006; Daniel R. Sovocool & Kristin Jamberdino, *Tracking a User's Location Via Cell Phone*, ipFrontline.com, Nov. 16, 2006, at: http://www.ipfrontline.com/depts/article.asp?id=9633&deptid=5; Linda Coady, *Government May Track Cell Phone Movements, N.Y. Court Says*, Privacy Litigation Reporter, Vol. 4:3, Nov. 17, 2006.

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

Sincerely,

Catherine Crump
Staff Attorney
American Civil Liberties Union

Appendix

washingtonpost.com

Cellphone Tracking Powers on Request

Secret Warrants Granted Without Probable Cause

By Ellen Nakashima
Washington Post Staff Writer
Friday, November 23, 2007; A01

Federal officials are routinely asking courts to order cellphone companies to furnish real-time tracking data so they can pinpoint the whereabouts of drug traffickers, fugitives and other criminal suspects, according to judges and industry lawyers.

In some cases, judges have granted the requests without requiring the government to demonstrate that there is probable cause to believe that a crime is taking place or that the inquiry will yield evidence of a crime. Privacy advocates fear such a practice may expose average Americans to a new level of government scrutiny of their daily lives.

Such requests run counter to the Justice Department's internal recommendation that federal prosecutors seek warrants based on probable cause to obtain precise location data in private areas. The requests and orders are sealed at the government's request, so it is difficult to know how often the orders are issued or denied.

The issue is taking on greater relevance as wireless carriers are racing to offer sleek services that allow cellphone users to know with the touch of a button where their friends or families are. The companies are hoping to recoup investments they have made to meet a federal mandate to provide enhanced 911 (E911) location tracking. Sprint Nextel, for instance, boasts that its "loopt" service even sends an alert when a friend is near, "putting an end to missed connections in the mall, at the movies or around town."

With Verizon's Chaperone service, parents can set up a "geofence" around, say, a few city blocks and receive an automatic text message if their child, holding the cellphone, travels outside that area.

"Most people don't realize it, but they're carrying a tracking device in their pocket," said Kevin Bankston of the privacy advocacy group Electronic Frontier Foundation. "Cellphones can reveal very precise information about your location, and yet legal protections are very much up in the air."

In a stinging opinion this month, a federal judge in Texas denied a request by a Drug Enforcement Administration agent for data that would identify a drug trafficker's phone location by using the carrier's E911 tracking capability. E911 tracking systems read signals sent to satellites from a phone's Global Positioning System (GPS) chip or triangulated radio signals sent from phones to cell towers. Magistrate Judge Brian L. Owsley, of the Corpus Christi division of the Southern District of Texas, said the agent's affidavit failed to focus on "specifics necessary to establish probable cause, such as relevant dates, names and places."

Owsley decided to publish his opinion, which explained that the agent failed to provide "sufficient specific information to support the assertion" that the phone was being used in "criminal" activity. Instead, Owsley wrote, the agent simply alleged that the subject trafficked in narcotics and used the phone to do so. The agent stated that the DEA had " 'identified' or 'determined' certain matters," Owsley wrote, but "these identifications, determinations or revelations are not facts, but simply

conclusions by the agency."

Instead of seeking warrants based on probable cause, some federal prosecutors are applying for orders based on a standard lower than probable cause derived from two statutes: the Stored Communications Act and the Pen Register Statute, according to judges and industry lawyers. The orders are typically issued by magistrate judges in U.S. district courts, who often handle applications for search warrants.

In one case last month in a southwestern state, an FBI agent obtained precise location data with a court order based on the lower standard, citing "specific and articulable facts" showing reasonable grounds to believe the data are "relevant to an ongoing criminal investigation," said Al Gidari, a partner at Perkins Coie in Seattle, who reviews data requests for carriers.

Another magistrate judge, who has denied about a dozen such requests in the past six months, said some agents attach affidavits to their applications that merely assert that the evidence offered is "consistent with the probable cause standard" of Rule 41 of the Federal Rules of Criminal Procedure. The judge spoke on condition of anonymity because of the sensitivity of the issue.

"Law enforcement routinely now requests carriers to continuously 'ping' wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target," wrote Christopher Guttman-McCabe, vice president of regulatory affairs for CTIA -- the Wireless Association, in a July comment to the Federal Communications Commission. He said the "lack of a consistent legal standard for tracking a user's location has made it difficult for carriers to comply" with law enforcement agencies' demands.

Gidari, who also represents CTIA, said he has never seen such a request that was based on probable cause.

Justice Department spokesman Dean Boyd said field attorneys should follow the department's policy. "We strongly recommend that prosecutors in the field obtain a warrant based on probable cause" to get location data "in a private area not accessible to the public," he said. "When we become aware of situations where this has not occurred, we contact the field office and discuss the matter."

The phone data can home in on a target to within about 30 feet, experts said.

Federal agents used exact real-time data in October 2006 to track a serial killer in Florida who was linked to at least six murders in four states, including that of a University of Virginia graduate student, whose body was found along the Blue Ridge Parkway. The killer died in a police shooting in Florida as he was attempting to flee.

"Law enforcement has absolutely no interest in tracking the locations of law-abiding citizens. None whatsoever," Boyd said. "What we're doing is going through the courts to lawfully obtain data that will help us locate criminal targets, sometimes in cases where lives are literally hanging in the balance, such as a child abduction or serial murderer on the loose."

In many cases, orders are being issued for cell-tower site data, which are less precise than the data derived from E911 signals. While the E911 technology could possibly tell officers what building a suspect was in, cell-tower site data give an area that could range from about three to 300 square miles.

Since 2005, federal magistrate judges in at least 17 cases have denied federal requests for the

less-precise cellphone tracking data absent a demonstration of probable cause that a crime is being committed. Some went out of their way to issue published opinions in these otherwise sealed cases.

"Permitting surreptitious conversion of a cellphone into a tracking device without probable cause raises serious Fourth Amendment concerns especially when the phone is in a house or other place where privacy is reasonably expected," said Judge Stephen William Smith of the Southern District of Texas, whose 2005 opinion on the matter was among the first published.

But judges in a majority of districts have ruled otherwise on this issue, Boyd said. Shortly after Smith issued his decision, a magistrate judge in the same district approved a federal request for cell-tower data without requiring probable cause. And in December 2005, Magistrate Judge Gabriel W. Gorenstein of the Southern District of New York, approving a request for cell-site data, wrote that because the government did not install the "tracking device" and the user chose to carry the phone and permit transmission of its information to a carrier, no warrant was needed.

These judges are issuing orders based on the lower standard, requiring a showing of "specific and articulable facts" showing reasonable grounds to believe the data will be "relevant and material" to a criminal investigation.

Boyd said the government believes this standard is sufficient for cell-site data. "This type of location information, which even in the best case only narrows a suspect's location to an area of several city blocks, is routinely generated, used and retained by wireless carriers in the normal course of business," he said.

The trend's secrecy is troubling, privacy advocates said. No government body tracks the number of cellphone location orders sought or obtained. Congressional oversight in this area is lacking, they said. And precise location data will be easier to get if the Federal Communication Commission adopts a Justice Department proposal to make the most detailed GPS data available automatically.

Often, Gidari said, federal agents tell a carrier they need real-time tracking data in an emergency but fail to follow up with the required court approval. Justice Department officials said to the best of their knowledge, agents are obtaining court approval unless the carriersprovide the data voluntarily.

To guard against abuse, Congress should require comprehensive reporting to the court and to Congress about how and how often the emergency authority is used, said John Morris, senior counsel for the Center for Democracy and Technology.

Staff researcher Richard Drezen contributed to this report.

View all comments that have been posted about this article.

Post a Comment

View all comments that have been posted about this article.