Mapping Our Privacy: The Use and Misuse of Location Data (A Law Enforcement Perspective and Legislative Balancing)

By STEPHANIE K. PELL*

THANK YOU. It is a pleasure to participate in this panel discussion[1] of law enforcement access to and use of location data—in my opinion, the most challenging issue Congress will face in any effort to reform the Electronic Communications Privacy Act[2] ("ECPA"). Our moderator, Julia Angwin, has asked me to address the law enforcement perspective on this issue.

Let me start by saying that I come to this issue from both law enforcement and legislative backgrounds. I was a federal prosecutor

* Principal, SKP Strategies, LLC; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, U.S. Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, U.S. Department of Justice; and former Assistant U.S. Attorney, Southern District of Florida. Email: stephanie@stephaniepell.net. I would like to thank Susan Freiwald and the University of San Francisco Law Review for their invitation to participate in the symposium. I would also like to thank Jim Green for his assistance.

1. These written remarks have been adapted from a speech given at the USF Law Review symposium on ECPA reform on February 24, 2012. That speech was based largely on the article I co-authored with Christopher Soghoian entitled, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012). At the time I gave the speech, this article was forthcoming but has since been published.

2. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). I use the term ECPA to describe the first three titles of the Electronic Communications Privacy Act: Title I ("Interception of Communications and Related Matters"), 100 Stat. 1848, which amended the Wiretap Act (commonly referred to as Title III ("Wiretapping and Electronic Surveillance") of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211–25 (codified as amended at 18 U.S.C. §§ 2511–2520 (2010))); Title II ("Stored Wire and Electronic Communications and Transactional Records Access"), commonly referred to as the Stored Communications Act (SCA), Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–68 (codified as amended at 18 U.S.C. §§ 2701–2712 (2010)); and Title III ("Pen Registers and Trap and Trace Devices"), commonly referred to as the Pen/Trap Devices Statute, Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–73 (codified as amended at 18 U.S.C. §§ 3121–27 (2010)).

for almost fifteen years and used ECPA in the course of investigating crimes. Using ECPA—that is, following the rules ECPA prescribes for acquiring information in the course of an investigation—is a very different exercise from considering what those rules *should be* and how they might appropriately balance law enforcement, privacy and industry equities. I first considered the issues involved in balancing these interests when I was detailed from the Department of Justice ("DOJ") to the House Committee on the Judiciary ("Judiciary Committee") during the 111th Congress and became the Committee's lead counsel on ECPA reform. In this role, I developed three ECPA reform hearings for the Judiciary Committee's Subcommittee on the Constitution, Civil Rights and Civil Liberties under the direction of then Chairman Jerrold Nadler (D-NY, 8th Dist.).

One of these hearings focused specifically on law enforcement access to location data.[3] Of the three hearings, I found this one to be the most difficult to develop and execute. The three primary sources of this difficulty were an inconsistent legal landscape, a strong disagreement between two of the three major stakeholders about what the law should be, and the scarcity of reliable information on the subject available for congressional scrutiny.

The first difficulty I faced in developing a hearing on ECPA reform and location data was that the law in this area is, quite frankly, a mess. Locating the proper standard for law enforcement access to prospective or "real time" location data—in ECPA or any other federal statute—is, in some respects, like the quest for the holy grail, the search for the fountain of youth, or (as the women in the audience will appreciate) the hunt for a truly comfortable pair of high-heeled shoes: it is a tale of inexhaustible desire and eternal frustration.

When Congress passed ECPA in 1986, cell phones were the size of small kitchen appliances. As forward-looking a statute as ECPA sought to be—and has, indeed, been—Congress did not foresee the enormous proliferation of mobile devices and the constant "necessity" they would become in our daily lives. Nor could Congress have anticipated the corresponding "benefits" such devices would bestow on law enforcement: they leave a record of almost everywhere we have been,

3. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary,* 111th Cong. 81–85, 93–94 (2010) [hereinafter *Location Hearing*].

allow law enforcement to track us in "real time," and perhaps even aid law enforcement in predicting where we are likely to go.[4]

Because neither ECPA nor any other statute provides a clear standard for law enforcement access to "real time" location data, courts have struggled to discern what the standard might be—that is, what Congress intended it to be.[5] For its part, since at least 2005, DOJ had argued that real time single cell-site location data should be accessible with something called a hybrid order: a combination of an 18 U.S.C. § 2703(d)[6] Order ("D Order") and an Order for a Pen Register/Trap and Trace device[7] ("Pen/Trap").[8] Some courts have adopted this "hybrid theory," while others have refused to authorize "real time" location tracking without a Rule 41[9] probable cause warrant.[10]

4. Researchers are developing algorithms that will predict future movements of mobile device users through the analysis of location data in the possession of law enforcement. *See* Parmy Olson, *Algorithm Aims to Predict Crime by Tracking Mobile Phones*, FORBES (Aug. 6, 2012), http://www.forbes.com/sites/parmyolson/2012/08/06/algorithm-aims-to-predict-crime-by-tracking-mobile-phones/.

5. Consider the congressional testimony of Judge Smith describing the difficulty he and other Magistrate Judges have faced in determining the proper standard for law enforcement access to real-time location information:

> Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA. The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of "electronic communication" specifically excludes information from a tracking device; and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring.

Location Hearing, *supra* note 3, at 82–83 (footnotes omitted).

6. 18 U.S.C. § 2703(d) (2006). To obtain an order under 18 U.S.C. § 2703(d), law enforcement must provide "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[ ] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2006).

7. *Id.* § 3123(a)(1) (directing that a court "shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device . . . if the court finds that the attorney for the Government [in an application pursuant to 18 U.S.C. § 3122(a)(1)] has certified to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation.").

8. Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance,* 41 U.S.F. L. REV. 589, 609–12 (2007) (describing the first publicly known case where the DOJ articulated the "hybrid theory" in applying for a court order authorizing access to real-time cell site information). A DOJ Manual contains DOJ guidance about the use of "hybrid" orders. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 159–60 (3d ed. 2009), *available at* http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

9. FED. R. CRIM. P. 41(d)(1) ("After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

Even magistrate judges within the same district do not always agree: there are districts where some judges will approve real time tracking with hybrid orders while others require a probable cause warrant.[11] Perhaps the most "cogent expression"[12] of a court approving a hybrid order (to use Judge Smith's words) is Magistrate Judge Gorenstein's 2005 decision from the Southern District of New York.[13] While approving the government's hybrid theory in that case, Judge Gorenstein's analysis of the relevant issues compelled him literally to examine a map of cell towers to determine the relative precision of location data that could be generated by a specific geographical portion of a cellular network.[14] He explained that his analysis was addressing the technology currently available to the government in the district in question at that time.[15] Thus, if the technology changed over time, his analysis might have to change with it.

Consider the legal instability that results when court decisions must depend upon the relative precision of location data generated by technology that is continuously and rapidly becoming more accurate. Indeed, in 2012, we all have the ability, in order to prevent "dropped calls," to place picocells, microcells or femtocells in our homes, which can, in some cases, generate location data that will identify individual floors or rooms within buildings.[16] It is almost comical

10. *See Location Hearing*, *supra* note 3, at 83–85 (written statement of Judge Stephen Wm. Smith discussing Magistrate and District Court decisions where courts have authorized the law enforcement access of prospective cell site data with hybrid orders and Rule 41 search warrants). *Id.* at 93–94 (Exhibit B cataloguing the Magistrate and District Court decisions).

11. *Compare In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC. 01, 2006 WL 468300 (S.D.N.Y. Feb. 28 2006) (denying application for limited single tower data), *with In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (granting application for limited single tower data).

12. *See Location Hearing*, *supra* note 3, at 83 (written statement of Judge Stephen Wm. Smith).

13. *In re* Application of the U.S. for an Order for Disclosure of Telecomm. Records and Authorizing the Use of Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 450 (S.D.N.Y. 2005).

14. *Id.* at 437.

15. *Id.* at 450.

16. In order to assist with the coverage of "dead spots," wireless carriers in recent years have been:

> deploy[ing] . . . the latest generation of smaller and smaller-scale cellular base stations (called, variously, 'microcells,' 'picocells' and 'femtocells') designed to serve very small areas, such as particular floors of buildings or even individual homes and offices. The effect of this trend toward smaller sectors is that knowing the identity of the base station (or sector ID) that handled a call is tantamount to

to think about magistrate judges, each time they are presented with a new government request for a hybrid order, examining new cell tower maps or consulting industry network experts[17] to determine the implications of the addition of a new cell tower or femtocell to a particular area. Such instability in the law does not benefit law enforcement, industry or consumer privacy interests, and this example illustrates only one of several problems that serve to make this area of the law such a mess.

The second issue that burdened the effort to execute a location data hearing was that, even though there is general agreement among the major stakeholders (law enforcement, industry and privacy advocates) that a lack of clarity in the law harms everyone, finding a clear standard everyone can agree upon—particularly, finding the legislative formula that will reconcile the interests of law enforcement with privacy advocates—is an exceedingly difficult task.

The policy position advocated by the Digital Due Process Coalition (a coalition of civil liberties organizations and companies which together proposed several principles to guide congressional consideration of ECPA reform),[18] which Jim Dempsey discussed earlier, would require a probable cause warrant for access to any location data generated by a cell phone—from a single point of historical location data indicating where someone was at a particular place and time, to "real time" tracking for several days or weeks.[19] Given my background as a prosecutor, I knew this blanket standard would be a "non-starter" for law enforcement.

---

knowing a phone's location to within a relatively small geographic area. In relatively unpopulated areas with open terrain, this may be an area miles in diameter. But in urban areas and other environments that use microcells, this area can be quite small indeed, sometimes effectively identifying individual floors and rooms within buildings.

Location Hearing, s*upra* note 3 at 25 (written statement of Professor Matt Blaze).

17. *See In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register, 415 F. Supp. 2d 211, 213 n.3 (W.D.N.Y. 2006) (reviewing a letter from Verizon's Court Order Compliance Manager "which states that the information sought will only 'identify the general area that the target mobile phone number is located at the time of a specific call' and that it 'cannot pinpoint the exact location of the mobile phone'").

18. *See About the Issue*, DIGITAL DUE PROCESS COALITION (May 5, 2010), http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163; *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 7, 12 (2010) (written statement of James X. Dempsey).

19. *See Our Principles*, DIGITAL DUE PROCESS COALITION (May 5, 2010), http://www.digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163.

Why would law enforcement oppose this blanket probable cause standard that treated historical and prospective location data identically? To begin with, investigations proceed over time, in something like a narrative. As such, once begun, they are simultaneously prospective and retrospective, with each new fact both refining the direction of the investigation's forward course and correcting previous erroneous assumptions. Particularly at the beginning of an investigation, then, agents must have the ability to acquire certain types of information in order to focus the inquiry in the right direction and on the correct person or people who might have committed the crime. Imagine, for example, if you were asked to write a book report on *Moby Dick*, but you were only allowed to read the first sentence, "Call me Ishmael."[20] How would you summarize the plot or talk about characters and themes without more information? Law enforcement, in my opinion, can make a credible argument that a probable cause standard for all location data—historical and prospective—will unduly hamper their activities at the early stages of an investigation. That is, it will prohibit investigators from reading far enough ahead to learn who Ahab is—and that there might just be a white whale involved, too—before they are able to develop the probable cause necessary for a valid warrant.[21] Excessively constraining law enforcement's vision at the beginning of an investigation is a genuine public safety concern. In our post-9/11 world, it could also prove to be a particularly difficult political stance.

Moreover, when we talk about a probable cause standard for all location data, we are generally referring to the notion of probable cause articulated in Rule 41 of the Federal Rules of Criminal Procedure.[22] Under Rule 41, the government would need to demonstrate that there is probable cause to believe that the location information *itself* is evidence of a crime. The government may often be able to make this showing insofar as a suspect's location (and thus her phone's location) would be evidence of a crime: Location information can rebut a defendant's alibi, place a defendant at the scene of a crime, or show that her movements are consistent with actions alleged in furtherance of a criminal conspiracy.

20. HERMAN MELVILLE, MOBY DICK: OR, THE WHALE 3 (Harrison Hayford et al. eds. 1988).

21. *See supra* note 9.

22. *See* FED. R. CRIM. P. 41(c) (listing categories of probable cause: "(1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained").

What if, however, law enforcement has a legitimate reason to find a suspect but the location information itself is *not* evidence of a crime? Consider, for example, a situation where law enforcement has an arrest warrant for a suspect. Agents go to his house and he is not there. They contact relatives and associates, and no one knows or, perhaps, no one is willing to tell them where he is. Investigators decide to seek a probable cause warrant from a magistrate judge in order to require the suspect's cell phone company to "ping" his phone[23] and track his location in real time. What if the arrest warrant is based on the suspect's alleged involvement in a health care fraud scheme and law enforcement has no reason to believe that his current location is in any way relevant to the crimes that led a judge to issue an arrest warrant? Could law enforcement acquire a Rule 41 probable cause warrant to track the suspect's current location via his cell phone? Arguably not. Indeed, Maryland Magistrate Judge Susan K. Gauvey concluded that a probable cause search warrant does not permit law enforcement to acquire GPS location data solely to execute an arrest warrant.[24] Her analysis focused on the fact that the government's probable cause theory was that the "evidence sought will aid in a particular apprehension," not that location data was evidence of a crime itself.[25] While the government was able to locate the subject of the arrest warrant by other means in this case,[26] a probable cause standard tied directly to the language of Rule 41 can, ironically, limit law enforcement's ability to find someone when a court has already found there is probable cause to arrest them. Professor Orin Kerr has labeled this the "probable cause of what" problem.[27]

What if law enforcement requests historical location data in order to exclude someone from an investigation? Under this scenario, the location information would likely not be evidence of a crime but, rather, would allow law enforcement to clear someone suspected of criminal activity and thus focus investigative resources upon appre-

23. Carriers can locate a cell phone by covertly "pinging" it. Such pings can "reveal the nearest cell site [tower] to the subscriber, or more accurate GPS or triangulated data if requested." Pell & Soghoian, *supra* note 1, at 131 (footnote omitted). For a general discussion of how mobile devices generate location data, *see* Pell & Soghoian, *supra* note 1, at 126–33.

24. *In re* Application of the U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 530 (D. Md. 2011).

25. *Id.* at 559.

26. *Id.* at 531-32.

27. *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 39 (2010) (written statement of Prof. Orin S. Kerr, George Washington Univ. Law School).

hension of the actual perpetrator. Under these circumstances, unduly limiting law enforcement's access to location data might, ironically, serve not only to impede important investigative functions, but also to compromise important interests of innocent third parties who otherwise could have been spared the anxiety and possible expense of being the erroneous object of a criminal investigation.

Third and finally, building a location data hearing was challenging because acquiring facts that could aid Congress in making good policy proved difficult. As I indicated before, the legal landscape governing law enforcement access of location data is messy and inconsistent. Moreover, the recent Supreme Court opinions in *Jones*[28] did not clarify the issues pertaining to law enforcement access to cell phone location data. If anything, the *Jones* decision only added additional layers of complexity and uncertainty.[29] In this particularly difficult and intricate area of the law, Congress needs information from all of the major stakeholders—law enforcement, industry and privacy advocacy groups—in order to judge the necessity for legislative action and the specific direction the law should take.

Compared with the hearing I developed on ECPA reform and cloud computing,[30] which drew significant industry participation, not one wireless carrier agreed to testify on location data access. Law enforcement was equally reluctant to discuss publicly how location data is used in investigations. While some details would likely reveal law enforcement sources and methods or industry proprietary information, I think there is a way to have a more public discussion about these issues. One mechanism that would promote this discussion and provide Congress with important facts concerning law enforcement access to location data would be reporting requirements similar to those mandated by Congress for law enforcement use of Wiretap[31]

28. United States v. Jones, 132 S. Ct. 945 (2012).

29. *See* Pell & Soghoian, *supra* note 1 at 148-50 (discussing the *Jones* majority opinion's failure to address GPS tracking, like cell phone tracking, that does not involve physical trespass and the Alito concurrence's failure to provide specific guidance about when Fourth Amendment concerns materialize and quoting *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.")).

30. *See generally ECPA Reform and the Revolution in Cloud Based Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary,* 111th Cong. (2010).

31. *See* 18 U.S.C. § 2519(2)-(3) (2006) (outlining what the intercepted communications report issued by the Administrative Office of the United States Courts must contain). These reports are detailed, revealing for each wiretap the city or county where it was executed, the type of interception (phone, computer, pager, fax), the number of individuals whose communications were intercepted, the number of intercepted messages, the num-

and Pen/Trap[32] authorities. No such reporting requirements currently exist for location data. As Senator Patrick Leahy has explained in a different context, reporting requirements are a "far more reliable basis than anecdotal evidence on which to access law enforcement needs and make sensible policy in this area."[33]

When I left the House Judiciary Committee at the end of the 111th Congress in 2010, I did not have a satisfactory recommendation to make to the members I worked for about how Congress should regulate law enforcement access to location data. So I decided to take a more academic route by joining forces with a technologist and diehard privacy advocate named Christopher Soghoian in order to try and develop a legislative framework for law enforcement access to location data that would improve the relative positions of each of the major stakeholders,[34] understanding that no individual group would be completely happy with the result. Ideally, we thought our dialogue from two different representative positions would serve both to replicate and expedite the dynamics and products of the legislative process. Our collaboration resulted in an article that is forthcoming in the *Berkeley Technology Law Journal*.[35]

Julia Angwin, our moderator, makes the point that not sharing the details of our framework at this point would be tantamount to our own version of trying to ignore the whale in *Moby Dick*—ignoring the sixty-ton whale in the room, so to speak—so I'll summarize them briefly.

The framework we propose in our article includes both a set of standards for law enforcement access to location data and a series of what we call "downstream" privacy protections to address aspects of consumer privacy that access standards alone cannot. The downstream protections we recommend are reporting requirements, minimization of data, and notice. Given the time constraints of this panel, I will focus the remainder of my remarks on our proposed standards. I do want to stress, however, that we take the position that standards

ber of arrests and convictions that resulted from interception, as well as the financial cost of the wiretap. *Id.*

32. *See id.* § 3126 (outlining what the Pen/Trap report issued by the Attorney General must contain). Similar to the intercepted communications report, *supra* note 31, the Pen/Trap report requires information about numbers of Pen/Trap orders applied for by law enforcement agencies to include, among other things, the offense specified in each order and the identity, including district, of the law enforcement agency making the application. § 3126.

33. 145 CONG. REC. 31,312 (1999) (statement of Sen. Patrick Leahy).

34. *See* Pell & Soghoian, *supra* note 1.

35. *Id.*

alone, in the absence of minimization and other protections, will not achieve the type of privacy protections and oversight needed to balance the major stakeholder equities.

Taking into account some of the issues I have discussed about the problems that a blanket probable cause standard would pose for legitimate law enforcement investigative activities, along with how a lower standard might result in the unnecessary over-collection of data (which includes the location data of innocent people), we came up with two access standards, one for historical location data and one for prospective data.[36]

For historical location data, we kept the current D Order standard—"specific and articulable facts showing that there are reasonable grounds to believe" that the information sought is "relevant and material to an ongoing criminal investigation"[37]—but added an additional element to § 2703(d). This new element would require the government to establish specific and articulable facts that a reasonable and sufficient *nexus* exists between the scope of the information requested and the alleged or suspected criminal activity being investigated.

This new "scope" element is specifically meant to address the potential for unnecessary over-collection of data. While the government often needs to cast a wide net at early stages in an investigation, the new element requires the government to demonstrate that the scope of the information requested is *reasonable* in light of the criminal activity being investigated. The current D Order standard may not adequately limit an over-collection of data. Indeed, the DOJ has argued that the word "material" in the D Order standard "does not transform the standard into one that requires a showing that the records requested are 'vital,' 'highly relevant,' or 'essential.'"[38] Thus, the scope of § 2703(d) may be "appropriate even if it compels disclosure of some unhelpful information" as "§ 2703(d) is routinely used to com-

36. Our proposed standards would not change the voluntary disclosure provisions in ECPA, which include exceptions for emergencies. *See* § 2702(b), (c).

37. 18 U.S.C. § 2703(d) (2006).

38. Government's Response to Objections of Three Twitter Subscribers to Magistrate Judge's March 11, 2011 Opinion Denying Motion To Vacate and Denying in Part Motion To Unseal at 9, *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114 (E.D. Va. 2011) (Misc. No. 1:11-DM-3) (quoting Subscribers' Objections), *available at* http://files.cloudprivacy.net/goverment_opp.pdf.

pel disclosure of records, only some of which are later determined to be essential to the government's case."[39]

So, in a murder investigation where police do not know the identity of the perpetrator, they may want to know every cell phone that was in the vicinity of the murder scene. Under the current practices in many jurisdictions, the police would use a D Order to obtain numbers of all cell phones that identified themselves to the closest cell towers. In this scenario, the new scope element we propose would require law enforcement to articulate and justify, for example, a timeframe for the data requested. If the police believe that the murder happened in or around 12:00 a.m. after the victim stepped out of a local nightclub when her shift was over, it might be reasonable for investigators to request the relevant cell site data from 11:00 p.m. to 1:00 a.m. Based on these limited facts, it may not be reasonable for the police to request data outside of that timeframe. But if the police developed information to suggest, for example, that the perpetrator was in the vicinity of the crime a week before the murder in order to watch the victim leave her place of work, it might be reasonable to request location data for that timeframe, as well. The magistrate judge would evaluate the scope of the government's request, which may involve a timeframe or other elements of scope like the number of people whose data was requested, in light of what is reasonable for the particular investigation.

With respect to prospective location data, we propose a probable cause standard for all "real time" location data, but we expand the categories of probable cause. In addition to "evidence of a crime,"[40] law enforcement could compel "real time" location data if there was probable cause to believe a person is committing, has committed, or is about to commit a felony offense, or is a victim of that offense, and the location information sought to be obtained concerns the location of the person believed to have committed, be committing, or about to commit that offense, or a victim of that offense. These expanded categories of probable cause will address the "probable cause of what problem" insofar as the focus of the probable cause standard is on the individual believed to be committing the crime, rather than exclusively on whether the location data *itself* is evidence of a crime.

We believe that the combination of these standards—maintaining the D Order standard for historical location with the addition of a

39. *Id.* at 8 (quoting *In re* § 2703(d) Order; 10GJ3793, 787 F. Supp. 2d 430, 437 (E.D. Va. 2011)).

40. *See* FED. R. CRIM. P. 41(c).

scope element and requiring a probable cause standard for "real time" data with expanded categories of probable cause—improves the relative positions of all major stakeholders. Everyone benefits from a greater degree of clarity in the law. Among other things, privacy advocates gain standards providing a higher degree of judicial oversight of law enforcement access to location data. Even with greater judicial involvement and standards that may require a more robust showing by law enforcement, these standards should not unduly inhibit their investigative activities. Moreover, law enforcement's participation in a system that features tighter, more rigorous access standards may promote increased public trust in the integrity of the system and, perhaps, a corresponding increase in law enforcement's own credibility.

I hope that I have given some insight into why law enforcement would oppose a blanket warrant standard for access to all location data, as well as some sense of the legal, substantive and political complexities that burden the very necessary effort to develop coherent policy in this area. Thank you, and I would be happy to answer any questions you may have.