Disclosing Stored Communication Data to Fight Crime: The U.S. and EU Approaches to Balancing Competing Privacy and Security Interests

Elise M. Simbro†

"[T]he principle underlying this . . . [is] that law enforcement's investigative intrusions on our private lives, in the interests of social order and safety, should not be unduly hindered, but must be balanced by appropriate degrees of accountability and judicial review."[1]

† Candidate for J.D., Cornell Law School, expected May 2011. B.B.A., The University of Texas at Austin, 2008. I would like to thank U.S. Magistrate Judge Patricia J. Gorence for inciting my curiosity in this issue, the editors of *Cornell International Law Journal* for their valuable feedback throughout the writing process, and my family for their continuous encouragement and support.

1. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Rec. to the Gov't, 534 F. Supp. 2d 585, 587 (W.D. Pa. Feb. 19, 2008) [hereinafter *W.D. Pa. Case*], *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008) [hereinafter *W.D. Pa. Case II*] (citing United States v. U.S. Dist. Ct., 407 U.S. 297, 317 (1972)).

Introduction

Advances in technology permit cellular service providers to create and maintain an indefinite record of a customer's approximate location each time a cellular telephone is used. Location data is becoming increasingly sophisticated and precise, as service providers are required by law to incorporate detailed Global Positioning System (GPS) data into their telephones.[2] The need to accurately locate cellular telephones first arose with respect to the increasing number of calls placed from cellular telephones to 911 emergency operators,[3] but the technology has since transcended these boundaries.

Law enforcement authorities also benefit from accurate location records in the detection, investigation, and prosecution of crime.[4] One prevalent tactic is for law enforcement authorities to seek court-authorized disclosure of a criminal defendant's cellular telephone records to assist in locating the defendant at the time of a charged crime, or to otherwise incriminate the defendant.[5] The ability of law enforcement authorities to obtain this location data increases the tension between public safety and individual privacy interests, prompting federal courts in the United States to reevaluate how to interpret traditional laws in light of emerging location technology.[6] More specifically, federal courts are reevaluating how to apply traditional search and seizure law to the disclosure of historical location data from cellular telephones.[7] This involves reconciling the Fourth Amendment of the U.S. Constitution, which protects citizens' privacy interests,[8] with relevant statutory law, the Stored Wire and Electronic Communications and Transactional Records Access Act (SCA), which details the proper procedure by which law enforcement can access stored communication records.[9]

In a recent decision from the Western District of Pennsylvania (*W.D. Pa. Case*), the court addressed the question of what standard should gov-

2. 47 C.F.R. § 20.18 (2008).

3. *See Who Knows Where You've Been? Privacy Concerns Regarding Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308 (2004) [hereinafter *Privacy Concerns*].

4. *See, e.g.*, *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 749 (S.D. Tex. Oct. 14, 2005) [hereinafter *S.D. Tex. Case 2005*] ("[Using] information regarding the strength, angle, and timing of the caller's signal . . . investigators are often able to locate suspects.").

5. *See id.*

6. *See id.* at 748–49 ("The issue explored here has serious implications for the balance between privacy and law enforcement . . . .").

7. *Privacy Concerns*, *supra* note 3, at 312.

8. *See* U.S. CONST. amend. IV.

9. 18 U.S.C. §§ 2703(c)–(d) (2000).

ern law enforcement's request for a suspect's cell phone records. The Government argued that using cell phone records to determine a suspect's past locations is materially different from real-time tracking, which requires a showing of "probable cause," and therefore, historical location data should be disclosed upon a less stringent showing of "reasonable grounds," the level of suspicion required under the SCA.[10] The court disagreed, finding that historical location data is not materially different merely because it has been stored.[11] The arguments for protecting real-time location information under the traditional probable cause standard also apply to historical location records.[12] Releasing data about past telephone call locations effectively converts the cellular telephone into a tracking device, and infringes upon a suspect's right to privacy in his or her whereabouts.[13] The court's ruling, that a request for a suspect's cellular phone records must be accompanied by a showing of probable cause, was affirmed by the Western District of Pennsylvania,[14] and is pending appeal before the United States Court of Appeals for the Third Circuit.

Not all courts in the United States agree with the decision reached in the *W.D. Pa. Case*. In fact, courts are divided on how to treat requests for stored cell phone records.[15] The case pending before the Third Circuit, which is the first circuit to address whether the standard of probable cause is required to obtain stored location data, carries a lot of weight because other courts will likely look to and follow the Third Circuit's ruling.[16]

This note argues that courts in the United States, and specifically the Third Circuit, can learn from the European Union's approach to dealing with competing privacy and security interests. The European Union issued a Data Retention Directive (2006 EU Directive)[17] following terrorist attacks in New York City, Madrid, and London, with an emphasis on protecting public safety.[18] The goal of the 2006 EU Directive is to preserve communication records and facilitate the cooperation of law enforcement authorities across the European Union in investigating, detecting, and prosecuting serious crime.[19] This does not mean that the European Union ignores privacy interests in a suspect's location, but such interests are less substantial

10. *W.D. Pa. Case*, 534 F. Supp. 2d 585, 585 (W.D. Pa. Feb. 19, 2008).
11. *Id.* at 603.
12. *See id.* at 601.
13. *Id.* at 616.
14. *W.D. Pa. Case II*, 2008 WL 4191511 at *1.
15. *See In re* Application of the U.S. for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F. Supp. 2d 411, 412 (S.D. Tex. 2007) [hereinafter *S.D. Tex. Case 2007*] ("[J]udges have divided over the Government's ability to obtain such data . . . .").
16. *See, e.g.*, *S.D. Tex. Case 2005*, 396 F. Supp. 2d 747, 765 (S.D. Tex. Oct. 14, 2005) ("[This opinion] is written in . . . hope that the government will seek appropriate review by higher courts so that authoritative guidance will be given [to] the magistrate judges who are called upon to rule on these applications on a daily basis.").
17. Council Directive 2006/24, 2006 O.J. (L 105) 54 (EC).
18. Francesca Bignami, *Privacy and Law Enforcement in the EU: The Data Retention Directive*, 8 CHI. J. INT'L L. 233, 238 (2007) [hereinafter *Privacy and Law Enforcement in the EU*].
19. *See* Council Directive 2006/24, art. 1(1), 2006 O.J. (L 105) 54, 56 (EC).

and do not require "rigid legal standards," such as a showing of probable cause, to overcome.[20] Part I sets the stage for tension between security and privacy advocates in the United States by providing background on the evolving location-based technology required by law in cellular phones. Part II refutes the arguments set forth in the *W.D. Pa. Case*—accessing stored cellular phone records effectively converts the telephone into a tracking device, and alternatively, individuals have a protected privacy interest in phone call locations—by considering why the decision is wrong under relevant U.S. constitutional and statutory law. Part III describes the European Union's approach to retaining and providing law enforcement authorities with access to stored communication records. Part IV argues that U.S. courts, in order to reach decisions consistent with U.S. constitutional and statutory law, should adopt the EU approach of advancing public safety at the cost of some, but not much, individual privacy. Specifically, the Third Circuit should overturn the strict probable cause standard required in the *W.D. Pa. Case*, in favor of disclosing stored location data pursuant to a less stringent showing of reasonable grounds under the SCA.

I. The Tension between Privacy and Security Advocates over GPS Enabled Phones

A. Evolving Technology Required by Law in Cellular Phones

The need to accurately locate cellular phone users first arose with respect to the increasing number of calls placed to 911 from cellular phones. One-third of all emergency calls are placed from cellular phones.[21] In 2001, while driving to her Florida home, Karla Gutierrez lost control of her car and skidded into a canal.[22] Ms. Gutierrez managed to call 911 on her cellular phone before the car submerged, but she could not describe her exact location.[23] By the time Miami rescue units located the accident site, Ms. Gutierrez had drowned, trapped inside the sinking car.[24] If Ms. Gutierrez had called 911 from a landline phone, the emergency dispatcher would have received her exact location because landline phones are matched to household addresses stored in emergency-service databases.[25] Emergency calls placed from cellular phones, however, were not as easy to locate because existing technologies could not automatically trace and display the geographic coordinates of the caller to the dispatcher.[26] As a representative from the National Academy of Emergency Medical Dispatchers said, "Cell phones have caused a crisis in the 911

20. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 236.

21. GENERAL ACCOUNTING OFFICE, UNEVEN IMPLEMENTATION OF WIRELESS ENHANCED 911 RAISES PROSPECT OF PIECEMEAL AVAILABILITY FOR YEARS TO COME, GAO-04-55, (2003), *available at* http://www.gao.gov/new.items/d0455.pdf [hereinafter GAO REPORT].

22. *Dateline NBC* (NBC television broadcast Jan. 27, 2001), *available at* http://www.911dispatch.com/video/dateline/datelinenbc_qt.html.

23. *Id.*

24. *Id.*

25. GAO REPORT, *supra* note 21, at 1.

26. *Id.*

community."[27] To deal with the difficulties presented by emergency calls placed from cellular phones, the Federal Communications Commission (FCC) set deadlines for cellular service providers to implement more precise location technology by the end of 2005. Ultimately, cellular service providers must be able to locate callers within 50–300 meters, depending on how the technology is used.[28] Countries besides the United States have embraced this location technology even beyond its use in emergencies.[29]

While the FCC does not require cellular service providers to use a specific technology, providers typically implement either GPS technology or signal triangulation to locate customers through their cellular phones, which are the two most accurate methods.[30] GPS technology works by measuring the amount of time it takes for a signal to travel between space-based satellites and a GPS chip embedded in a cellular phone.[31] "When the GPS chip receives four synchronized signals from GPS satellites, it can calculate a [subscriber's] three-dimensional location that is accurate to within twenty meters."[32] GPS technology is dependent on information transmitted via signals between satellites and a cellular phone's GPS chip.[33] Locating cellular phones by means of signal triangulation relies not on signals from a satellite, but rather on radio signals sent between a cellular phone and a nearby cellular tower.[34] The cellular tower (or towers) supporting the phone call registers the subscriber's general location by calculating the distance between the phone and the tower using the "known speed of radio signals."[35] A phone that is turned on continuously sends out signals to nearby cellular towers, scanning for the best reception, and switches towers automatically as the subscriber moves.[36] If three nearby cellular towers simultaneously receive signals from a cellular phone, the towers compare signals and triangulate a more precise location in one of two ways.[37] The Time Difference of Arrival (TDOA) method measures the

27. *Dateline NBC*, *supra* note 22.

28. 47 C.F.R. § 20.18(g)(1)(v), (h)(1)-(2) (2008) ("[Providers shall b]y December 31, 2005, achieve 95 percent penetration of location-capable handsets among its subscribers.").

29. *See, e.g.*, Moon Ihlwan & Andy Reinhardt, *"Working Late" Won't Work Anymore*, BUSINESSWEEK, Oct. 31, 2005, at 40 (describing how millions of Koreans pay for a service that sends a message if a subscriber is not where he or she should be at a specific time and permits the tracker to see the subscriber's movements over the past five hours, and how in Britain, parents are willing to pay $52 a year to track children's cell phones).

30. *See Privacy Concerns*, *supra* note 3, at 308.

31. James E. Holloway et al., *Regulation and Public Policy in the Full Deployment of the Enhanced Emergency Call System (E-911) and their Influence on Wireless Cellular and Other Technologies*, 12 B.U. J. SCI. & TECH. L. 93, 103 (2006) ("GPS is a space-based radio navigation system consisting of twenty-four earth-orbiting satellites that broadcast information used by the receiver, a chip embedded in the wireless phone, to calculate the receiver's latitude, longitude, and—when more than three satellites are available—altitude").

32. *Privacy Concerns*, *supra* note 3, at 308.

33. *See id.*

34. Holloway, *supra* note 31, at 103.

35. *Id.*

36. *W.D. Pa. Case*, 534 F. Supp. 2d 585, 587 (W.D. Pa. Feb. 19, 2008).

37. *See id.* at 590.

amount of time it takes for a signal to travel from a cellular phone to the nearby cellular towers or vice-versa.[38] The Angle of Arrival (AOA) method measures the angle at which a signal sent from a phone reaches the nearby cellular towers.[39] The only way a subscriber can prevent a cellular phone from sending out signals and registering its current location is to turn the phone off.[40]

As people depend on their cellular phones instead of traditional landline phones, service providers continue to upgrade cellular tower locations, especially in densely populated areas, sometimes placing towers only hundreds of feet apart.[41] The close proximity of cellular towers in densely populated areas allows service providers to record more precise location information, often placing a phone within 200 feet,[42] and "creating a virtual map of [a subscriber's] movements."[43] In rural areas, however, fewer cellular towers exist.[44] A single tower often covers several hundred square miles and is the sole provider of reception, preventing the use of TDOA and AOA to triangulate a subscriber's location.[45] Therefore, the accuracy of location information depends a great deal on whether the subscriber is in an urban or rural setting.

B. Conflicting Viewpoints—Security and Privacy Advocates in the United States

Beyond providing emergency operators with pertinent location data, cellular technology is also a valuable tool for law enforcement authorities.[46] In 2004, police successfully located a stolen car with a kidnapped child inside within a half-hour, by repeatedly calling the cellular phone that the child's mother had left inside the vehicle.[47] People undoubtedly recognize the importance of location data to law enforcement authorities in such a situation, or to an emergency operator when callers are unaware of their exact location.[48] However, not everyone welcomes the idea of a cellular phone being used as a locating device, considering it instead an invitation to invade individual privacy.[49] Some even describe the cellular phone as a modern tracking device, putting Justice Brandeis ahead of his time

38. *Id.* at 590 n.19.
39. *Id.*
40. *See Privacy Concerns*, *supra* note 3, at 309.
41. *See In re* Application of U.S. for an Order for Disclosure of Telecomm. Records, 405 F.Supp.2d 435, 437 (S.D.N.Y. 2005) [hereinafter *S.D.N.Y. Case 2005*].
42. *W.D. Pa. Case*, 534 F. Supp. 2d at 590.
43. *Privacy Concerns*, *supra* note 3 at 309.
44. *Id.*
45. *Id.* at 309–10.
46. *See In re* Applications of U.S. for Orders Pursuant to 18 U.S.C. § 2703(d), 509 F. Supp. 2d 76, 78 (D. Mass. 2007) [hereinafter *D. Mass. Case*] ("[C]lose proximity of cell towers . . . makes it possible to identify with reasonable certainty the location from which a call was made.").
47. *See Girl, 5, Found Safe as Man Steals Car*, ROCKY MTN. NEWS, Apr. 22, 2004, at A18.
48. GAO REPORT, *supra* note 21, at 1.
49. *See Privacy Concerns*, *supra* note 3, at 312.

when he predicted in 1928 that "[s]ubtler and more far-reaching means of invading privacy have become available to the government. . . . The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping."[50] Few could have imagined the technological advances that have occurred since 1928, but law enforcement authorities continue to use new technologies to assist in their investigations.

It is difficult to reconcile the tension that exists between the interest in public safety and the right to individual privacy. Citizens' concerns about the government tracking their movements without cause conflict with law enforcement's concern that it may lose an effective tool if rules are made too restrictive. Tension lies in the premise that usefulness of an investigation tool is "roughly proportional to its intrusiveness."[51] This leaves courts with the "prospect of balancing legitimate law enforcement goals against deeply ensconced privacy interests of American citizens."[52]

II. U.S. Law Does Not Protect Cellular Telephone Records

One particular area of tension between security and privacy interests arises when the government seeks court-authorized disclosure of the defendant's cellular telephone records to assist in locating the defendant at the time of the charged crime. This tension has prompted U.S. federal courts to evaluate which standard the government is required to establish—probable cause or reasonable cause—before a court will order disclosure of a defendant's cellular phone records.[53] Courts have to rely on and interpret sections of the U.S. Constitution that were promulgated before location technologies existed, and statutory laws that do not develop as quickly as the technology itself.[54] As a result of cellular technology challenging the law faster than legislatures can respond and provide guidance, courts are divided on the correct approach.[55]

---

50. Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

51. Ian Samuel, Note, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, 1325 (2008).

52. Derek P. Richmond, Comment, *Can You Find Me now? Tracking the Limits on Government Access to Cellular GPS Location Data*, 16 COMMLAW CONSPECTUS 283, 309 (2007).

53. *See, e.g.*, *D. Mass. Case*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007) (analyzing "whether the Fourth Amendment's probable cause requirement . . . preempts the more relaxed [reasonable cause] provisions of the SCA . . . .").

54. *See* U.S. CONST. amend. IV.; Stored Wire & Electronic Communication & Transactional Records Access Statute (SCA), 18 U.S.C. § 2703 (2000); Richmond, *supra* note 52, at 309.

55. *Compare D. Mass. Case*, 509 F. Supp. 2d at 80, *and S.D. Tex. Case 2007*, 622 F. Supp. 2d 411, 418 (granting access to historical cell phone records on showing of less than probable cause), *with W.D. Pa. Case*, 534 F. Supp. 2d 585 (W.D. Pa. Feb. 19, 2008), *and In re* Application of the U.S. for an Order (1) Authorizing Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Info; and (3) Authorizing Disclosure of Location-Based Serv., 2006 WL 1876847, at * 1 (N.D. Ind. July 5, 2006) [hereinafter *N.D. Ind. Case*] (denying access to historical cell phone records absent showing of probable cause).

A. The Fourth Amendment Does Not Protect Privacy Interests in Historical Call Locations

One issue before U.S. courts is whether government requests for cellular phone records implicate defendants' privacy protections under the Fourth Amendment of the U.S. Constitution.[56] The Fourth Amendment specifically protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, . . . and no warrants shall issue, but upon probable cause, . . . particularly describing the place to be searched, and the persons or things to be seized."[57] Courts struggle with how to apply this privacy right to the context of location data obtained from cellular phones.

Although cellular technology is a recent development, courts have interpreted law enforcement use of location information in light of Fourth Amendment protections. In *Katz v. United States*, law enforcement authorities attached a listening device to the outside of a public telephone booth to intercept the defendant's telephone conversations.[58] The United States Supreme Court held that monitoring a closed telephone booth—which went so far as to reveal the content of the defendant's conversations—constituted an unreasonable search and violated the defendant's right to privacy.[59] While this case does not provide much guidance on applying the Fourth Amendment to historical location data obtained from a cellular phone, it was the first case to suggest a now widely used two-part test to determine whether a person's Fourth Amendment rights have been violated.[60] Under this test, a defendant must demonstrate (1) an actual expectation of privacy that (2) society is willing to recognize as reasonable.[61]

In *Smith v. Maryland*, the Supreme Court adopted the two-part test originally expressed in Justice Harlan's concurrence in *Katz*.[62] Law enforcement authorities, acting through a telephone company and without a warrant, installed a pen register at the telephone company's central offices to record the numbers dialed by the defendant from his landline phone.[63] Using the two-part test, the Court concluded that law enforcement authorities did not violate the defendant's Fourth Amendment rights because it is unlikely that telephone users have a right to privacy in the phone numbers that they dial.[64] The defendant did not demonstrate an actual expectation of privacy because telephone users voluntarily convey numerical information to the telephone company in order to connect their phone calls.[65] Even if the defendant had an actual expectation of privacy, it was in the content of his communications, which a pen register is unable

56. U.S. CONST. amend. IV.
57. *Id.*
58. 389 U.S. 347, 348 (1967).
59. *Id.* at 353.
60. *See id.* at 361 (Harlan, J., concurring).
61. *Id.*
62. 442 U.S. 735, 740 (1979).
63. *Id.* at 737.
64. *Id.* at 745.
65. *Id.* at 742.

to record.[66] The Court refused to recognize a privacy interest in phone numbers dialed.[67]

United States v. Knotts addressed the legality of law enforcement use of tracking devices.[68] The Court specifically considered whether a beeper secretly placed inside the defendant's vehicle, allowing law enforcement to use signals emitted by the beeper to monitor the defendant's location without a warrant, violated the defendant's Fourth Amendment rights.[69] The Court found that the defendant had no reasonable expectation of privacy in his movements as he traveled on public roads because anyone traveling on the same roads could have visually observed the same information obtained from the beeper.[70] The beeper was merely "a more effective means of observing what [was] already public."[71] The Court distinguished between tracking what is already public and tracking inside the "private sphere," such as inside a person's home, where there is a recognized privacy interest under the Fourth Amendment.[72]

Considering privacy interests with respect to personal, mobile communication devices, the Sixth Circuit Court of Appeals found that there is no expectation of privacy in a message sent to a pager.[73] The confidentiality of a message is uncertain when sent to a pager over which the sender has no control.[74] The sender takes the risk that an unintended recipient in possession of the pager may intercept the message, or that the person receiving the message may disclose its content.[75] The defendant failed the first part of the two-part test—demonstrating an actual expectation of privacy—by relying on a "misplaced trust that the message would actually reach the intended recipient."[76]

United States v. Forest was one of the first cases to discuss the limits of intercepting cellular phone data to reveal a defendant's general location.[77] To monitor suspected cocaine traffickers, law enforcement authorities obtained court authorization to intercept conversations from the defendants' cellular phones.[78] Intercepted communications revealed "the imminent arrival of a large shipment of cocaine."[79] Drug Enforcement Administration (DEA) agents attempted to keep visual surveillance of the defendants in anticipation of the shipment, but were unable to maintain

66. *Id.* at 741.
67. *Id.* at 745.
68. 460 U.S. 276, 277 (1983).
69. *Id.*
70. *Id.* at 281–82.
71. *Id.* at 284. "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." *Id.* at 282.
72. *See id.* at 282.
73. United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990).
74. *Id.*
75. *Id.*
76. *Id.*
77. 355 F.3d 942 (6th Cir. 2004).
78. *Id.* at 947.
79. *Id.*

constant watch.[80] In an effort to re-establish visual contact, the agents dialed one defendant's cellular phone, hanging up before the phone had a chance to ring, but after the phone sent out signals to the nearest cellular towers.[81] Agents identified the location of the cellular phone towers being hit and therefore, the general location of the defendant.[82] While searching the general area, agents spotted the defendants in their vehicle and were able to continue visual surveillance.[83] Following the reasoning set forth in *Knotts*, the court found no violation of the defendant's privacy because the DEA agents could have obtained the same information from the defendant's visually observable location.[84] While the Sixth Circuit in *Forest* purports to follow controlling Supreme Court decisions, it actually expands law enforcement's ability to obtain information from a cellular phone without a warrant. Rather than using information conveyed when the defendant voluntarily made or received calls, the DEA agents dialed the defendant's phone, inducing the phone to send out signals and register the defendant's current location.[85] Law enforcement authorities, however, cannot infer from this case that there are no limits when manipulating a defendant's personal property.

A more recent case that applies traditional Fourth Amendment principles to emerging technologies directly addresses whether the government must demonstrate probable cause to obtain cellular phone records.[86] The court in *United States v. Suarez-Blanca* concluded that probable cause is not necessary because cell phone users do not have a reasonable expectation of privacy in the information stored by service providers.[87] The court held that "there is no privacy interest in records kept in the [ordinary] course of a business."[88] The court analogized to an individual's lack of privacy in bank records or credit card statements,[89] the latter of which records a customer's location each time a purchase is made. Similarly, the location of a subscriber's cellular phone is a record kept in the ordinary course of business, as it is a record identifying the cellular towers through which a subscriber's calls are directed.[90] By voluntarily using the service provider's equipment and conveying information to the service provider in order to connect telephone calls, a subscriber assumes the risk that records concerning the call will be retained and possibly disclosed.[91]

---

80. *Id.*
81. *Id.*
82. *Id.*
83. *Forest*, 355 F.3d at 947.
84. *Id.* at 951 (obtaining location data from a cellular phone is "simply a proxy for [defendant's] visually observable location.").
85. *Id.*
86. United States v. Suarez-Blanca, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008).
87. *See id.*
88. *Id.*
89. *Id.*
90. *Id.*
91. *See id.* (recognizing no right to privacy if information is in hands of third party).

The court in *Suarez-Blanca* did recognize limits on law enforcement's use of location information. Monitoring a subscriber's movements in a private location, such as inside a home where the information is unobtainable by visual surveillance, would infringe upon the subscriber's Fourth Amendment rights.[92] Cellular phone records, however, are only specific enough to reveal the location of cellular towers used to support a phone call, and are unable to pinpoint the exact location of a subscriber or definitively place a subscriber within a private location.[93] When historical information is neither precise in its locating nor revealing in its details, the court is not willing to afford much privacy to the customer.[94]

This progression of cases suggests that cellular telephone customers do not have a reasonable expectation of privacy in historical location data. Records kept in the ordinary course of business fall outside Fourth Amendment protections, and cellular phone records should be no exception. It would be difficult to defend privacy protections afforded to cellular phone records when past credit card transactions "place a person at a given location at a specific time, yet under established Fourth Amendment law . . . enjoy no Fourth Amendment protection."[95] Subscribers do not control the data contained in transactional records or its disclosure.[96] To the contrary, subscribers voluntarily turn over the rights to such information each time they use a provider's cellular equipment and services.[97]

It would also be contradictory to require a showing of probable cause to obtain cellular phone records considering the ruling in *Smith* provides law enforcement authorities with access to landline phone records on a lesser showing,[98] even though these records pinpoint customers inside a home, a place where it is undisputed that individuals have a right to privacy. Cellular phone records are not precise enough to definitively place a customer inside a protected space, as they reveal only the location of cellular towers used to support a call; however,[99] if courts require a showing of probable cause before granting access, they effectively recognize these records as more intrusive on people's privacy rights. There is no reason to expect a higher level of privacy simply because a cellular phone moves.

---

92. *Suarez-Blanca*, 2008 WL 4200156, at *9.

93. *Id.* at *10; *see In re* Application of U.S. for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info, 411 F. Supp. 2d 678, 682 (W.D. La. 2006) [hereinafter *W.D. La. Case*] (finding no Fourth Amendment violation because cell phone records only locate the cellular towers used to support a phone call).

94. *See id.*

95. Ellen Nakashima, *Judge Limits Searches Using Cellphone Data*, THE WASHINGTON POST, Sept. 12, 2008, at A02 (quoting U.S. Attorney Mary Beth Buchanan involved in *W.D. Pa. Case*).

96. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

97. *See id.* at 743–44.

98. *See id.* at 746.

99. *See W.D. La. Case*, 411 F. Supp. 2d at 682.

B. Cellular Phones Not Converted into Tracking Devices

The U.S. Constitution, and specifically the Fourth Amendment, provides the framework within which to develop statutory law regarding the proper standard for disclosing cellular phone records. Defendants often challenge the disclosure of cellular phone records not only on constitutional but also on statutory grounds.[100] One issue of statutory interpretation before U.S. courts is whether the government can obtain cellular phone records under the Stored Wire and Electronic Communications and Transactional Records Access Act (SCA) and its more lenient standard of reasonable cause. Courts must first consider whether cellular phone records fall outside the scope of the SCA, and its permissive use of the reasonable cause standard, by virtue of the statute's express exclusion of communications from a device "which permits the *tracking* of the movement of a person or object," i.e. a tracking device.[101] To resolve this, courts look at whether 18 U.S.C. § 3117—the Mobile Tracking Device Statute—is meant to cover cellular phones.[102] The statute vaguely and circularly defines a "mobile tracking device" as an "electronic or mechanical device which permits the tracking of the movement of a person or object."[103] A court may only authorize "installation of a mobile tracking device" if the government demonstrates probable cause.[104] Some courts interpret "*installation*" narrowly and limit the reach of § 3117 to devices physically and often secretly installed by the government in personal property, excluding a cellular phone that is knowingly possessed and used.[105] "The existence of a true 'tracking device' is unknown to, and cannot be disabled or turned off by, the person being tracked."[106] Courts that interpret § 3117 in this way broadly distinguish between a cellular phone and a device installed by the government when defining a tracking device.

Rather than entirely exclude cellular phones from the scope of § 3117, some courts differentiate between records of a subscriber's past locations and real-time monitoring, finding that only real-time monitoring converts a telephone into an imprecise tracking device.[107] By using vague language in the text of § 3117(b), Congress anticipated future advances in technology and left open the possibility that devices not originally intended or designed to track movements, such as cellular phones, could be treated as

100. *See, e.g.*, *D. Mass. Case*, 509 F. Supp. 2d 76, 79 (D. Mass. 2007) (challenging the court's refusal to disclose cell phone records on a more lenient showing of reasonable grounds, the standard set out in SCA, 18 U.S.C. § 2703).

101. *W.D. Pa. Case*, 534 F. Supp. 2d 585, 601 (W.D. Pa. Feb. 19, 2008).

102. *See id.* at 602.

103. 18 U.S.C. § 3117(b) (1986).

104. *Id.* § 3117(a).

105. *See D. Mass. Case*, 509 F. Supp. 2d at 81 n.11 ("I am not . . . persuaded of the relevance of the mobile device tracking statute, 18 U.S.C. § 3117, to the issue. The statute governs the 'installation' of tracking devices. The 'tracking' of a cell phone does not require the installation of any sort of device. The telephone does the job by itself.").

106. *W.D. La. Case*, 411 F. Supp. 2d 678, 681 (W.D. La. 2006).

107. *See In re* Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 949 (E.D. Wis. 2006), [hereinafter *E.D. Wis. Case*], *aff'd*, 2006 WL 2871743, at *5-6 (E.D. Wis. Oct. 6, 2006).

tracking devices in some situations.[108] Courts that adopt this position require the government to demonstrate probable cause before monitoring a defendant's cellular phone in real-time.[109] However, the same courts suggest that historical cellular phone records are outside § 3117 and its strict requirement that the government show probable cause to obtain them.[110]

Assuming historical cellular phone data is not tracking information—§ 3117 does not provide the authority to access it—the government may be entitled to such data under the SCA standard.[111] 18 U.S.C. § 2703, a provision within the SCA, sets forth the procedure that the government must follow in order to obtain customer records regarding "electronic communication service[s]," so long as the records do not contain the contents of the communications.[112] Because the SCA does not regulate the disclosure of content information, the contents of communications are only accessible upon establishing a probable cause suspicion.[113] A court, however, may order a cellular service provider to disclose information about a subscriber's name, address, phone number, call records, payments, and length and types of service[114] on a comparatively lenient standard of "specific and articulable facts showing . . . reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation."[115] The government does not even need to provide notice to the subscriber when requesting his or her records.[116] It is no surprise that the government relies upon the argument that the SCA applies to cellular phone records.

In response to the government's assertion that a reasonable grounds standard is sufficient, one court—among others—agreed that it "ha[s] no doubt that the SCA authorizes a service provider's disclosure to law enforcement of historical cell [phone] information."[117] This certainty arises from the plain language of the statute itself. § 2703 applies to requests for stored electronic communications,[118] and provides courts with the authority to compel service providers to disclose communication records that are in their possession and that pertain to a subscriber of their

108. *See S.D. Tex. Case 2005*, 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005).

109. *See E.D. Wis. Case*, 2006 WL 2871743, at *5.

110. *See In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294, 307 n.10 (E.D.N.Y. 2005) [hereinafter *E.D.N.Y. Case 2005*].

111. *See* SCA, 18 U.S.C. § 2703 (2000).

112. *Id.* § 2703(c)(1) (excluding the content of communications from its scope).

113. *See id.* §§ 2703(a)–(b) (providing requirements to compel disclosure of the contents of communications).

114. *See id.* § 2703(c)(2).

115. *Id.* § 2703(d).

116. *See id.* § 2703(c)(3).

117. *E.D.N.Y. Case 2005*, 396 F. Supp. 2d 294, 307 n.10 (E.D.N.Y. 2005).

118. *See In re* Application of U.S. for an Order Authorizing the Installation and Use of a Pen Register Device, 497 F. Supp. 2d 301, 309 (D.P.R. 2007) [hereinafter *D.P.R. Case 2007*].

service.[119] Stored cellular location data appears to fall within the scope of § 2703 because a cellular service provider keeps records of a subscriber's past phone call locations, and such locations pertain to the subscriber's cellular phone service, but do not fall within the express exclusion of content communications.[120]

The *D. Mass. Case* was the first published opinion to thoroughly assess § 2703 and conclude that cellular phone records meet all the requirements.[121] The court specifically concluded that cell phone companies provide *electronic communications*, data revealing a subscriber's location when using the cell phone is a *record* pertaining to a subscriber of such service, and location information is not *content* information because it discloses nothing about a call's substance.[122] Other courts followed the lead and ordered service providers to disclose cellular phone records pursuant to a more lenient standard of reasonable cause.[123] These courts emphasized the limited scope of the information requested; law enforcement authorities were not seeking to activate GPS capabilities on the target's phone in order to track the target in real-time or track the location of the phone when it was not being used.[124] Courts appear more willing to grant access to cellular phone records if the government only seeks limited information under § 2703.[125] Where a court requires the government to provide evidence of the relevancy of cellular phone records and restricts access to the confines of a limited request, it effectively balances interests in security and privacy. Courts should read the SCA, as many courts already do, to cover requests for cellular phone records and provide authority for their disclosure, pursuant to a more lenient standard of judicial oversight as compared to that afforded to requests to monitor or track a target in real-time.

C. The *W.D. Pa.* Strikes an Incorrect Balance Between Privacy and Security

The *W.D. Pa. Case* rejected the conclusions that many courts reach—the Fourth Amendment does not protect cellular phone records and access to such records does not convert the phone into a tracking device—in favor of requiring a strict probable cause standard to obtain cellular phone records.[126] Magistrate Judge Lenihan denied the Government's request for a subscriber's cellular phone records pursuant to § 2703 and accompanied by a reasonable suspicion that the target of a drug trafficking investigation

119. *See* 18 U.S.C. § 2703(c)(1); *In re* Application of U.S. for an Order for Prospective Cell Site Location Info., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) [hereinafter *S.D.N.Y. Case 2006*].
120. *See D. Mass. Case*, 509 F. Supp. 2d 76, 79–80 (D. Mass. 2007).
121. *See id.*
122. *Id.*
123. *See, e.g.*, *S.D. Tex. Case 2007*, 622 F. Supp. 2d 411, 418 (S.D. Tex. 2007).
124. *See id.* at 417–18.
125. *See id.* at 418.
126. *See W.D. Pa. Case*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008).

was using the subscriber's phone.[127] It was not enough for the Government to assert that the phone records would provide valuable evidence as to the suspect's past, and likely future, whereabouts, as well as provide the suspect's "sources of supply, 'stash sites,' and distribution networks."[128] The court concluded that a cellular phone used to register location operates in the same way and for the same purpose as a tracking device[129] because it is an "electronic . . . device which permits the tracking of the movement of a person or object."[130] By maintaining records of a cellular phone's location, the service provider effectively records the movement of the person in possession. Whether a service provider releases information about a subscriber's movements in real-time, or retains it and releases it later in the form of historical records, it nevertheless remains information from a device that permits tracking.[131] In other words, mere storage does not alter the source or character of the information.[132]

The Government argued that regardless of whether a cellular phone has the ability to track an individual's movements, cellular phone records are no different than other transactional records kept in the ordinary course of business.[133] These records should be accessible under § 2703(c)'s reasonable relevancy standard as records "pertaining to a subscriber['s]" cellular phone service.[134] To the contrary, the court found that historical records of a subscriber's movements do not in any way pertain to the service provided.[135] Customers pay for content services (voice or text), not to have their changes in location recorded.[136]

According to the court in the *W.D. Pa. Case*, even if historical cellular location data falls within the scope of § 2703, it remains information that traditionally requires a showing of probable cause.[137] Individuals have a reasonable expectation of privacy as to their physical movements and locations under Fourth Amendment protections.[138] "People place a certain privacy value on their movements. . . . Whether it's their movements yesterday or their movements today, it's the same."[139] Using the two-part test first stated in *Katz*, (1) individuals have an actual expectation of privacy, not knowing that service providers create and retain a record of their move-

127. *See id.* at 587 ("[SCA] does not authorize access to an individual's cell-phone derived 'location information,' either past or prospective, on a simple showing of articulable relevance to an ongoing investigation . . . .").
128. *Id.* at 588 n.12.
129. *See id.* at 602 n.44 (noting that 18 U.S.C. § 3117 does not require a "particular degree of precision").
130. 18 U.S.C. § 3117(b).
131. *See W.D. Pa. Case*, 534 F. Supp. 2d at 603.
132. *See id.*
133. *See id.* at 588–89.
134. 18 U.S.C. § 2703(c)(1); *W.D. Pa. Case*, 534 F. Supp. 2d at 588–89.
135. *See W.D. Pa. Case*, 534 F. Supp. 2d at 606 n.54.
136. *See id.*
137. *See id.* at 607.
138. *See id.* at 610–11.
139. Nakashima, *supra* note 95, at A02 (quoting Catherine Crump, a lawyer with the American Civil Liberties Union, explaining why the Government's position in the *W.D. Pa. Case* was flawed).

ments each time they use a cellular phone; and (2) this expectation is reasonable because the record has the potential to locate individuals within private property.[140] The imprecision of such records—only revealing a subscriber's location to within a few hundred yards and unable to definitively place a cellular phone within private property or detail the interior of such private property—is overcome by the very nature of the records.[141] Location information is extremely personal and susceptible to abuse by reason of the possible breadth of information that the Government could request and the low cost and undetectable process of obtaining it.[142]

The Sixth Circuit Court of Appeals, in *Warshak v. United States*, made it clear that a customer can waive a reasonable expectation of privacy by voluntarily conveying information to a service provider that will be accessed for business purposes.[143] Applying this standard, the court in the *W.D. Pa. Case* found that cellular phone customers do not voluntarily convey location information because the information is automatically registered, possibly without customer knowledge.[144] Also, retaining records of customers' locations serves no business purpose other than to satisfy government regulations.[145]

The *W.D. Pa. Case* used two lines of reasoning—first, individuals have a reasonable expectation of privacy under the Fourth Amendment in movements or locations; and second, cellular phones are tracking devices excluded from the scope of § 2703—to reach the conclusion that the Government must show probable cause to obtain a suspect's cellular phone records.[146] There are, however, problems specific to the case that may have unduly influenced the court's decision. Courts are more likely to compel disclosure of cellular phone records when the government seeks limited information.[147] The Government in this case broadly sought the subscriber's location records without narrowing the scope of its request.[148] Also, the Government requested the subscriber's records not because there was reason to believe that the subscriber was directly involved in illegal activity, but because there was reasonable suspicion that the suspect of a drug investigation was using the subscriber's phone.[149] In other words, the Government attempted to obtain the personal records of someone other than the suspect in question. This indirect connection is too tenuous to link the subscriber to the suspect or the suspect to the cellular phone.[150] If

140. *See W.D. Pa. Case*, 534 F. Supp. 2d at 611–12.
141. *See* Nakashima, *supra* note 95, at A02.
142. *See W.D. Pa. Case*, 534 F. Supp. 2d at 586.
143. *Id.* at 615 (citing Warshak v. United States, 490 F.3d 455, 476 (6th Cir. 2007)).
144. *Id.*
145. *Id.* (pointing out that it is not enough for the location data to be accessible; location data must actually be used by employees in the course of providing cellular phone services).
146. *Id.* at 591, 607.
147. *See supra* text accompanying notes 124–25.
148. *See W.D. Pa. Case*, 534 F. Supp. 2d at 588.
149. *Id.* at 588 n.11.
150. *Id.*

these reasons influenced the court's decision to deny the Government's request for disclosure, the Third Circuit should make this clear.

Because the Third Circuit is the first circuit court in the United States to address whether government requests for historical location data are subject to the reasonable grounds standard of the SCA or the traditional probable cause standard, this case carries a lot of weight. This note argues that the Third Circuit should overturn the strict probable cause standard in favor of reasonable cause because the weight of the evidence under U.S. law, in light of EU policy, demonstrates that security interests can be advanced without significant costs to individual privacy.

III. The EU Approach to Using Stored Communication Data to Fight Crime

Following terrorist attacks in New York City, Madrid, and London, the European Union put more emphasis on the security of its citizens over privacy.[151] In particular, the European Union passed the 2006 Data Retention Directive, compelling member states to retain mobile phone records for a period of not less than six months and not more than twenty-four months from the date of communication.[152] The intent was to promote law enforcement cooperation across borders and accelerate the exchange of personal communication records to prevent, investigate, and punish criminal acts.[153]

A. The 1995 EU Data Protection Directive

The European Union has not always followed an approach that promotes member states exercising their security and law enforcement powers. One reason behind this is the European Union's recognition of a fundamental right to privacy.[154] All EU member states are signatories of the European Convention on Human Rights (ECHR), under which a "right to respect for . . . private and family life" is recognized, subject to some limitations.[155] This right to a private life is a broad term that courts have interpreted to protect "important elements of the personal sphere" including a person's name, gender, and sexual orientation,[156] as well as a person's right to information privacy.[157] Within this framework, one of the oldest policies in the European Union was the protection of data privacy.[158]

---

151. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 238.
152. Council Directive 2006/24, art. 6, 2006 O.J. (L 105) 54, 58 (EC).
153. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 238.
154. *See* Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].
155. *Id.*
156. P.G. v. United Kingdom, App. No. 44787/98, Eur. Ct. H.R. para. 56 (2001).
157. This right to privacy under the ECHR has "been interpreted to include a right to information privacy." *See* Francesca Bignami, *Towards a Right to Privacy in Transnational Intelligence Networks*, 28 MICH. J. INT'L L. 663, 672 (2007) [hereinafter *Towards a Right to Privacy*].
158. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 233.

The European Union Data Protection Directive of 1995 (1995 EU Directive) addressed concerns that liberalizing the European market would conflict with the protection of individual privacy rights.[159] In an integrated European market, one way to encourage the free flow of information was to set an "equally high privacy level in all EU Member States"[160] with regard to the processing and movement of personal data.[161] The 1995 EU Directive established common guidelines for collecting personal data throughout the European Union in order to protect individuals from privacy abuses by market actors.[162] While the privacy protections under the 1995 EU Directive were very broad,[163] the Directive only regulated market actors, and therefore, data collected for law enforcement and public safety purposes was outside of its scope.[164] Beyond reasons of public safety, EU member states could not process personal data unless they provided notice to the data subject,[165] collected the personal data for a legitimate purpose,[166] and refrained from collecting personal data that was excessive in relation to that purpose.[167] The 1995 EU Directive left open the possibility of collecting personal data only in limited circumstances.

B. The 2006 EU Data Retention Directive

Following the terrorist attacks in New York City in 2001, Madrid in 2004, and London in 2005, the idea of preserving communication records to fight crime gained support and shifted the focus in the European Union from data protection to data retention.[168] The European Parliament and the Council of the European Union passed the 2006 Data Retention Directive (2006 EU Directive), which requires the storage of data generated in connection with providing electronic communication services, such as landline telephone, mobile telephone, e-mail, or other Internet services.[169] The 2006 EU Directive facilitates European cooperation in the "investigation, detection and prosecution of serious crime" by improving, as well as

159. *See* Council Directive 95/46, art. 1, 1995 O.J. (L 281) 31, 38 (EC); *Privacy and Law Enforcement in the EU*, *supra* note 18, at 233.

160. DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 900 (2d ed. 2006).

161. *See* Council Directive 2006/24, para. 1, 2006 O.J. (L 105) 54, 54 (EC).

162. *Privacy and Law Enforcement in the EU*, *supra* note 18, at 234.

163. *See* Council Directive 95/46, art. 1(1), 1995 O.J. (L 281) 31, 38 (EC) ("Member states shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.").

164. *Id.* art. 3(2), at 39; *Privacy and Law Enforcement in the EU*, *supra* note 18, at 237.

165. Council Directive 95/46, arts. 10–12, 1995 O.J. (L 281) 31, 41–42 (EC) (providing data subject with the right to receive notice when personal data is processed, access all personal data, and seek rectification, deletion, or blocking of incomplete or inaccurate data).

166. *Id.* art. 6(1)(b), at 40 ("[P]ersonal data must be . . . collected for specified, explicit and legitimate purposes . . . .").

167. *Id.* art. 6(1)(c), at 40 ("[P]ersonal data must be . . . adequate, relevant, and not excessive in relation to the purposes for which [it is] collected and/or further processed . . . .").

168. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 238.

169. Council Directive 2006/24, art. 1(1), 2006 O.J. (L 105) 54, 56 (EC).

standardizing, the information available to national authorities.[170] EU member states must retain data regarding the location of a mobile phone throughout the duration of a call, excluding any data that reveals the content of the call.[171] This is similar to 18 U.S.C. § 2703 that, as mentioned in Part II.B, distinguishes between the level of privacy afforded to a phone call's location and content.[172] EU member states must retain location data for a period of at least six months, but no longer than twenty-four months, from the date of communication.[173] After two years, the value of the data to law enforcement authorities diminishes too much to justify continued interference with an individual's right to privacy.[174]

C. EU Member States Implement 2006 EU Data Retention Directive

EU member states were required to implement the 2006 EU Directive within eighteen months of its passing, or no later than September 15, 2007.[175] However, member states had an option to postpone application of the 2006 EU Directive for an additional eighteen months.[176] The United Kingdom exercised this option, declaring its intention pursuant to Article 15(3) of the 2006 EU Directive to postpone its application to Internet communications data, but not to mobile telephones.[177] Therefore, on October 1, 2007, the UK's Data Retention Regulations (2007 UK Regulations) put the 2006 EU Directive into effect with respect to mobile telephones.[178] The 2007 UK Regulations impose an obligation on service providers to retain data generated in the process of supplying mobile telephone services for a period of twelve months.[179] Data identifying the telephone number from which a call is made, the telephone number dialed, the date and time of the start and end of the call, the telephone service used, and the location of the telephone during the call must be retained.[180] Service providers must also retain data relating to a dialed, but unsuccessful call attempt.[181]

There are similarities between the effects on privacy under UK and U.S. law. The 2007 UK Regulations require service providers to retain personal data generated in the process of supplying mobile communica-

170. *Id.*; *Privacy and Law Enforcement in the EU*, *supra* note 18, at 239.
171. Council Directive 2006/24, art. 5(f), 2006 O.J. (L 105) 54, 58 (EC).
172. *See supra* note 112 and accompanying text.
173. Council Directive 2006/24, art. 6, 2006 O.J. (L 105) 54, 58 (EC).
174. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 250 (arguing that communication data more than two years old is not useful because individuals planning a serious crime would communicate in the two years immediately preceding the crime).
175. Council Directive 2006/24, art. 15(1), 2006 O.J. (L 105) 54, 60 (EC).
176. *Id.* art. 15(3), at 60. The majority of EU countries postponed application of the 2006 EU Directive including the Netherlands, Austria, Estonia, the United Kingdom, the Republic of Cyprus, the Hellenic Republic, the Grand Duchy of Luxembourg, Slovenia, Sweden, the Republic of Lithuania, the Republic of Latvia, the Czech Republic, Belgium, Poland, Finland, and Germany. *Id.* at 61–63.
177. The Data Retention (EC Directive) Regulations, 2007, S.I. 2007/2199 (U.K.) (explanatory note) [hereinafter UK Directive].
178. *Id.* art. 1.
179. *Id.* arts. 4(1)–(2).
180. *Id.* art. 5.
181. *Id.* art. 4(3).

tions.[182] Likewise, there is no protected privacy interest in records kept in the "ordinary course of business" under the Fourth Amendment of the U.S. Constitution.[183] Whether location data qualifies as data produced in the course of business and therefore, is excluded from extensive privacy protections, varies between the two countries. As noted in the *W.D. Pa. Case*, U.S. courts have not definitively decided whether a cell phone customer's location records pertain to the services provided.[184] In contrast, the United Kingdom characterizes a customer's location records as data generated in the process of supplying mobile communication services.[185] While both countries exempt records kept in the course of business from privacy protections, they disagree as to what is considered a business record.

IV. Evaluation of the EU Approach

Although the European Union and the United States have different approaches to data protection, the United States could learn from the EU approach of advancing law enforcement and security efforts at the cost of some, but not much, individual privacy. The 2006 EU Directive demonstrates how the EU member states cooperate in order to prevent serious crime, while still complying with the fundamental right to "private life" under the ECHR.[186] Put differently, the 2006 EU Directive effectively addresses the fear in the *W.D. Pa. Case* of sacrificing too much in the way of individual privacy.

A. Recognizing Different Conceptions of Privacy

The U.S. and EU ideas of data protection differ in many respects.[187] This stems from two different conceptions of privacy, which lead to differences in privacy laws.[188] The U.S. conception of privacy is a right of freedom from government intrusion.[189] There is no affirmative duty to put legislation in place to protect individual privacy rights because the rights themselves shield against unlawful interference.[190] Privacy in the United States is a narrow concept, focusing on the "physical places and personal

182. *Id.* arts. 4(1), 5.

183. *See, e.g.*, United States v. Suarez-Blanca, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) ("[N]o privacy interest in records kept in the [ordinary] course of a business . . . .").

184. *See W.D. Pa. Case*, 534 F.Supp.2d 585, 605–06 (W.D. Pa. 2008), *aff'd*, No. 07–524M, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008).

185. *See* UK Directive, 2007, S.I. 2007/2199, arts. 4(1), 5(2)(e) (U.K.).

186. *See Privacy and Law Enforcement in the EU*, *supra* note 18, at 249.

187. *See* Francesca Bignami, *Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network*, 26 MICH. J. INT'L L. 807, 815 (2005) [hereinafter *Transgovernmental Networks vs. Democracy*] ("European and American concepts of privacy differ in important respects, a fact that has far-reaching consequences for their information privacy regulation.").

188. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151, 1160 (2004).

189. *Transgovernmental Networks vs. Democracy*, *supra* note 187, at 817; Whitman, *supra* note 188, at 1161.

190. *Transgovernmental Networks vs. Democracy*, *supra* note 187, at 817.

facts which, if invaded or disclosed, would offend common expectations of privacy."[191]

In contrast, the EU conception of privacy is based not upon a right to be free *from* intrusion, but rather upon a right *to* personal dignity.[192] This positive right imposes a duty on the state to safeguard informational privacy.[193] For example, German privacy laws protect the "*rights to one's image, name, and reputation*."[194] A privacy right based upon personal dignity provides individuals with more access to and control over the personal information that is disclosed.[195] This is reflected in the 1995 EU Directive where, absent concerns for public safety,[196] there are general requirements to provide notice to the data subject,[197] collect accurate data,[198] and allow a subject to access personal information that is being processed.[199] Individuals in the European Union have more "rights to control [their] public image" and the way that others view them.[200] While EU privacy protections broadly apply to all types of personal information,[201] the European Union carves out exceptions, limiting privacy protections in circumstances where public safety is at issue.[202]

Different conceptions of privacy in the European Union and United States lead to different legal standards to obtain location data. In the European Union, the law of data protection, rather than the law of criminal procedure as used in the United States, governs access to personal location data.[203] There are some similarities between the two approaches. For example, data protection law, much like U.S. criminal procedure, limits the amount and type of personal information available to law enforcement authorities.[204] However, the legal standards to obtain personal data in the European Union, including location data, are more flexible.[205] Authorities can obtain location data without a strict showing of probable cause—as advocated in the *W.D. Pa. Case*—so long as the data is relevant, used for purposes related to the criminal investigation, and expunged or made anonymous once it is no longer needed.[206] Even before the European Par-

191. *Id.* at 816.
192. Whitman, *supra* note 188, at 1161.
193. *Transgovernmental Networks vs. Democracy*, *supra* note 187, at 816–17.
194. Whitman, *supra* note 188, at 1161.
195. *Id.* (describing German privacy law as a "*right to informational self-determination*—the right to control the sorts of information disclosed about oneself."); *see also Transgovernmental Networks vs. Democracy*, *supra* note 187, at 816.
196. *See* Council Directive 95/46, art. 13(1), 1995 O.J. (L 281) 31, 42 (EC) (allowing government to restrict the scope of privacy protections when necessary to safeguard national security, defense, and domestic law enforcement).
197. *See id.* arts. 10–11, at 41–42.
198. *See id.* art. 6(1)(d), at 40.
199. *See id.* art. 12, at 42.
200. Whitman, *supra* note 188, at 1161.
201. *See Towards a Right to Privacy*, *supra* note 157, at 672.
202. *See* ECHR, art. 8(2).
203. *Privacy and Law Enforcement in the EU*, *supra* note 18, at 236.
204. *See id.*
205. *Id.*
206. *Id.*

liament and the Council of the European Union passed the 2006 EU Directive, national authorities only prevented the transfer of personal data from one EU member state to another three times as a result of privacy concerns.[207] The European Union's flexible approach to storing and transferring personal location data lends itself as a valuable option for fighting serious crimes.

Another crucial difference between U.S. and EU perceptions of privacy and resulting legal standards to obtain location data is whether the right to privacy is balanced against government interests. The European Court of Human Rights interprets Article Eight of the ECHR as prohibiting authorities from storing personal data because it interferes with an individual's right to a private life,[208] unless three conditions are met.[209] One of the three conditions—all of which will be discussed in greater detail[210]—requires a proportional interference with an individual's private life.[211] Proportionality under EU law implies balancing the importance of the privacy right against the importance of the public purpose and searching for a less intrusive way to accomplish the same purpose.[212] Law enforcement authorities carry the burden of establishing that the interference is proportional, and the burden will vary with the privacy right at stake and the public purpose pursued.[213] The European Union recognizes a fundamental right to privacy, but permits balancing where the purpose is investigating, detecting, and prosecuting serious crimes. Conversely, the U.S. court in the *W.D. Pa. Case* requires the Government to demonstrate probable cause in order to obtain personal location data relevant to the criminal investigation,[214] with no hint of balancing the importance of the privacy right at stake against the public purpose. The court appears to treat the fundamental right to privacy as a trump card.

B. Exploring Reasons to Adopt the EU Approach

The 2006 EU Directive strikes a delicate balance between retaining location data to facilitate cooperation in fighting serious crime,[215] and complying with the right to private life under Article Eight of the ECHR,

---

207. *Transgovernmental Networks vs. Democracy*, *supra* note 187, at 843–44 (noting that all three cases involved transfers of data to countries lacking any type of legislation on information privacy).

208. *See e.g.*, Rotaru v. Romania, App. No. 28341/95, Eur. Ct. H.R. paras. 44, 46 (2000).

209. *Privacy and Law Enforcement in the EU*, *supra* note 18, at 242 (describing the three conditions that justify storing personal data as interferences that are (1) authorized by law, (2) in pursuit of a legitimate purpose, and (3) proportional).

210. *See* discussion *infra* Part IV.B.

211. *Privacy and Law Enforcement in the EU*, *supra* note 18, at 242.

212. *Id.* ("If the [privacy] right is sufficiently important and there are alternative means of accomplishing the public purpose, proportionality is breached.").

213. *Id.* at 246.

214. *W.D. Pa. Case*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008).

215. Council Directive 2006/24, art. 1(1), 2006 O.J. (L 105) 54, 56 (EC).

which cautions against storing personal data.[216] As mentioned in Part IV.A, the European Court of Human Rights interprets Article Eight to permit authorities to interfere with the right to privacy and store personal data for the purpose of fighting crime, only if three conditions are met.[217] The interference must be "in accordance with the law,"[218] in pursuit of a legitimate purpose,[219] and proportional and no more than necessary to achieve that purpose.[220]

The 2006 EU Directive meets all three conditions to permit a public authority to interfere with private life. To retain and use location data, it must first be "authorized by a law, [that is] accessible to the public, with precise enough provisions to curb arbitrary government action and to put citizens on notice of possible incursions into their private sphere."[221] In other words, individuals must know the basis for an intrusion into their private life, as set out in law, to justify such an intrusion by a public authority.[222] The 2006 EU Directive fulfills this first condition by authorizing member states to store and use personal data regarding the location of calls made from mobile phones.[223] Second, the purpose for storing location data must fit one of the legitimate purposes listed in Article Eight of the ECHR, which includes preventing crime, and because it does not specify what type of crime, arguably to prevent *any* crime.[224] Although the 2006 EU Directive could broadly permit member states to retain location data to prevent all crimes, it instead has a narrow scope that permits member states to retain location data for the purpose of investigating, detecting, and prosecuting *only serious* crimes.[225]

Using personal data only in connection with serious crimes also applies to the third condition—interference with the right to privacy must be proportional and no more than necessary to pursue the legitimate aim.

---

216. *See* Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC, para. 9, 2005 O.J. (C 298) 1, 2 (EC) [hereinafter Opinion of the European Data Protection Supervisor].

217. *See e.g.*, Amann v. Switzerland, App. No. 27798/95, Eur. Ct. H.R. paras. 45–46 (2000) (intercepting and recording a phone call is "'interference by a public authority', within the meaning of Article 8(2)" and is a breach of the right to private life under Article 8(1) unless the justification for the interference satisfies three conditions).

218. *Id.* para. 46.

219. ECHR, art. 8(2) ("[N]o interference by a public authority with the exercise of this [privacy] right except . . . in the interests of national security, public safety or the economic well-being of the country, . . . prevention of disorder or crime, . . . protection of health or morals, or . . . protection of the rights and freedoms of others.").

220. *Amann*, App. No. 27798/95, Eur. Ct. H.R. para. 46.

221. *Privacy and Law Enforcement in the EU*, *supra* note 18, at 242.

222. *See e.g.*, Sunday Times v. United Kingdom, App. No. 6538/74, Eur. Ct. H.R. para. 49 (1979) ("[T]he law must be adequately accessible: the citizen must . . . have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct . . . .").

223. Council Directive 2006/24, art. 5(1)(f), 2006 O.J. (L 105) 54, 58 (EC).

224. ECHR, art. 8(2); *Privacy and Law Enforcement in the EU*, *supra* note 18, at 245.

225. Council Directive 2006/24, art. 1(1), 2006 O.J. (L 105) 54, 56 (EC).

Pursuit of a legitimate aim, such as preventing crime, will not alone justify violating an individual's right to privacy if the approach used to prevent crime is excessive. "[T]he state cannot use a sledgehammer to crack a nut."[226] To comply with the requirement of a proportionate interference, the 2006 EU Directive prohibits member states from retaining data for more than twenty-four months,[227] or storing the content of telephone conversations at all.[228] The 2006 EU Directive "retain[s] less data for a shorter time,"[229] and complies with the idea that the privacy interest in when, where, and to whom cellular phone calls are made is less substantial than the privacy interest in the content of the calls.[230] Also, the 2006 EU Directive does not allow law enforcement authorities to make broad requests for information, requiring them to complete thorough requests for information with respect to specific telephone numbers linked to suspected criminal activity.[231]

Not only does the 2006 EU Directive comply with the right to privacy on its own, but in 2008, the European Union issued a Protection of Personal Data Framework Decision (2008 EU Framework Decision) to ensure that personal data used in the "fields of police and judicial cooperation in criminal matters" is protected.[232] The 2008 EU Framework Decision reiterates the three principles of lawfulness, legitimate purpose, and proportionality when collecting and processing data,[233] requires member states to verify the quality and accuracy of personal data,[234] limits the situations in which authorities may transmit data across borders as well as the people who may receive the data,[235] requires member states to inform the data subject about the collection of personal data,[236] and obliges member states to implement measures designed to protect data against "destruction[,] . . . loss, alteration, [and] unauthori[z]ed disclosure or access."[237]

The 2008 EU Framework Decision should not be viewed in isolation to indicate that the European Union is taking a step away from its emphasis on security, but rather, it should be interpreted in connection with the 2006 EU Directive. Together, they represent the European Union's balance of two competing ideals—protecting the right to privacy while also enhancing public safety. One way to understand the 2008 EU Framework Decision is to view it as developing mutual trust between member states' law enforcement authorities. Putting guidelines in place to protect personal

226. PHILIP PLOWDEN & KEVIN KERRIGAN, ADVOCACY AND HUMAN RIGHTS: USING THE CONVENTION IN COURTS AND TRIBUNALS 39 (2002).
227. Council Directive 2006/24, art. 6, 2006 O.J. (L 105) 54, 58 (EC).
228. *Id.* art. 5(2), at 58.
229. *Privacy and Law Enforcement in the EU*, *supra* note 18, at 249.
230. *Id.* at 236.
231. *Id.* at 252.
232. Council Framework Decision 2008/977, art. 1(1), 2008 O.J. (L 350) 60, 64 (EC).
233. *Id.* art. 3(1), at 65.
234. *Id.* art. 8, at 66.
235. *Id.* arts. 13–14, at 67–68.
236. *Id.* art. 16(1), at 68.
237. *Id.* art. 22(1), at 69.

communication records exchanged across borders prevents a barrier to state cooperation. States are more likely to cooperate in an initiative if it simultaneously respects their citizens' privacy rights. The 2006 EU Directive permits authorities to store and use personal communication records to prevent serious crime, but in connection with the protections of the 2008 EU Framework Decision, it does not require member states to sacrifice too much in the way of individual privacy. The fears of U.S. privacy advocates—that providing access to personal location data will encourage "twenty-four hour surveillance of any citizen of this country"[238] and eventually undermine privacy rights completely—have not come true in the European Union.

Conclusion

Until the Third Circuit, and ultimately, the Supreme Court, consider the issue of what standard is required to obtain stored location data, the protection afforded this data remains uncertain, and lower U.S. courts will continue to reach conflicting results. This note narrowly focuses on the decision reached in the *W.D. Pa. Case*—requiring probable cause to obtain records of the defendant's cellular phone call locations—and why it should be overturned under existing U.S. law and with reference to EU law. If the *W.D. Pa. Case* involved tracking a defendant's location through a cellular phone in real-time or disclosing the content of a past phone call without a showing of probable cause, the analysis and conclusions in this note would likely be different.

The Fourth Amendment of the U.S. Constitution does not protect privacy interests in historical call locations. There is no reasonable expectation of privacy because the documented location is imprecise, unable to definitively place a person within a constitutionally protected space, and is part of a record kept by service providers in the ordinary course of business. Without Fourth Amendment protection, § 2703 of the SCA allows the government to obtain cellular phone records absent a probable cause warrant. The standard of access under § 2703 is, and should be, a showing of reasonable grounds to believe that the information is relevant to an ongoing criminal investigation.

The United States can also learn from how the European Union balances competing privacy and security interests. The devastating impact of terrorist attacks in New York City, London, and Madrid was the driving force behind the 2006 EU Directive, put in place to encourage member states to cooperate in the prevention of serious crime. It directs EU member states to retain and share mobile communication data, including the location of customers' past phone calls. The proper authorities may obtain location data without probable cause, so long as the data is relevant and used for purposes related to the criminal investigation. This flexible approach allows the European Union to emphasize public safety without

238. United States v. Knotts, 460 U.S. 276, 283–84 (1983).

sacrificing too much in the way of individual privacy. The interests of public safety and consistency in lower court decisions require that the United States take a similar approach. The Third Circuit overturning the decision in the *W.D. Pa. Case* would be a step in the right direction toward implementing the EU approach and ruling consistently with U.S. law.

Considering that U.S. courts have yet to reach a consensus about how to treat stored location data, another approach is for Congress to step in and clarify the judiciary's role under the SCA—the statutory scheme in place for electronic communications—and pass legislation to fill in the gaps. The problem is formulating legislation specific enough so that courts know how to treat existing technologies, but not too specific as to be out-of-date each time there is a technological advancement.[239] Vague legislation is a "necessary and inevitable evil" where the technology in question rapidly evolves, but it can still provide guidelines for regulating existing, as well as future, technology.[240] Going forward, the stage is set for either Congress or the Third Circuit to address the correct standard for access to stored location data and in effect, the appropriate balance for competing privacy and security interests in a post-9/11 world.

---

239. Richmond, *supra* note 52, at 318–19.
240. *Id.* at 319.