

---

# CAN YOU FIND ME NOW?—TRACKING THE LIMITS ON GOVERNMENT ACCESS TO CELLULAR GPS LOCATION DATA

Derek P. Richmond<sup>†</sup>

## I. INTRODUCTION

As cellular<sup>1</sup> telephones have dramatically decreased in size, manufacturers have continued to infuse more and more technology into these devices, some of which are smaller than a deck of cards.<sup>2</sup> In addition to standard voice services, offerings such as text and picture messaging, email, and Web access, photo, and even video cameras are now commonplace.<sup>3</sup> Along with these functions, approximately one hundred million mobile phones in the U.S. contain Global Positioning System (“GPS”) chips,<sup>4</sup> and such phones will continue to proliferate in the future.<sup>5</sup> Partially due to consumer demand for improved technology,<sup>6</sup> and partly a response to a government mandate,<sup>7</sup> this common arrangement allows service providers to offer a host of new options and services.<sup>8</sup> GPS technology, when installed on a cellular phone, allows precise

---

<sup>†</sup> J.D. Candidate, May 2008, The Catholic University of America, Columbus School of Law.

<sup>1</sup> The terms “cellular,” “cell,” “wireless,” and “mobile” are used interchangeably in discussing what the FCC terms “commercial mobile radio service (“CMRS”).” 47 C.F.R. § 20.3 (2006).

<sup>2</sup> Marguerite Reardon, *10 Things Your Phone Will Do in 10 Years*, CNET NEWS, June 1, 2007, [http://www.cnet.com/4520-13387\\_1-6737990-1.html](http://www.cnet.com/4520-13387_1-6737990-1.html).

<sup>3</sup> *Id.*

<sup>4</sup> Melody Joy Kramer, *Somebody’s Watching You—and It’s Your Cell Phone*, NPR, Sept. 18, 2006, <http://www.npr.org/templates/story/story.php?storyId=6097216&sc=emaf>.

<sup>5</sup> Brad Smith, *GPS: The Mobile Way*, WIRELESS WEEK, Nov. 15, 2006, <http://www.wirelessweek.com/article.aspx?id=76952>.

<sup>6</sup> *Id.*

<sup>7</sup> See 911 Service, 47 C.F.R. § 20.18 (2006); see also discussion *infra* Part III.B (discussing the Enhanced 911 System).

<sup>8</sup> Smith, *supra* note 5.

locating and tracking of anyone using such a GPS-enabled phone.<sup>9</sup> Many cell phone manufacturers install these chips regardless of whether the user or service provider explicitly uses it, and many consumers are wholly unaware of the potential, both good and bad, of this combined technology.

GPS technology simplifies tracking. Law enforcement officers need not attach a tracking device to a suspect's car or plant one in his briefcase; they need only know the number of the cell phone in his pocket. Yet as the ease and accuracy of such tracking methods increases, so too does the need for privacy protection. The judiciary and the legislature are at a crossroads. Law enforcement agencies have asked cellular providers to supply cell site data,<sup>10</sup> and those companies have often resisted. Both sides have turned to courts to settle the cell site data dispute,<sup>11</sup> but have yet to present arguments regarding the analogous, more accurate GPS data. Bearing this analogy in mind, this Note will examine court decisions on this issue, including the arguments for and against granting government access to cell site data. In doing so, this Note will illustrate that courts face an equally difficult decision in choosing whether to grant law enforcement access to more accurate GPS location data. This Note will also elucidate flaws in the current statutory protections and argue that Congress must address these flaws before court decisions become too disparate. The promising benefits of GPS-enabled cell phones are as weighty as the potential for its abuse;<sup>12</sup> the promise inherent in the combination of mobile phones and GPS necessitates careful regulation and close scrutiny of government requests for access to the information.<sup>13</sup>

---

<sup>9</sup> See CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 5:26, at 149 (2d ed. Supp. 2006) (“[C]ell phones provide a readily available tracking device that is carried around by a significant portion of the population.”).

<sup>10</sup> Cell site information identifies the physical location of a cellular subscriber by providing “information regarding the strength, angle, and timing of the caller’s signal measured at two or more cell sites” or towers. *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 748–49 (S.D. Tex. 2005) [hereinafter *Texas Pen/Trap Case*]. It functions as the network-based analogue to handset-based GPS tracking technology.

<sup>11</sup> See discussion *infra* Part V.

<sup>12</sup> In an interview on National Public Radio, Matt Richtel, technology correspondent for *The New York Times*, stated that “courts are recognizing that Americans . . . are carrying devices that are at once wonderful communication devices, but also have the potential to let people know where we are at all times, and the courts, just as we as consumers, must figure out a balancing act between these two things.” *Talk of the Nation: Surveillance via Cell Phone* (NPR broadcast Dec. 14, 2005), available at <http://www.npr.org/templates/story/story.php?storyId=5053410>.

<sup>13</sup> Clifford Fishman, Catholic University of America law professor and former New York City Prosecutor, phrased the analysis as involving the “inevitable and invariable and never-ending trade-off between improving police efficiency, which increases their ability to protect us, at the cost of individual privacy and liberty, and here, as in throughout the entire

Part II of this Note considers the regulatory schema limiting government access to cell site data and the government's actions leading to the rise of GPS-enabled cell phones. Part III examines the potential private and commercial uses for applications of this technology focusing on beneficial applications. Part IV considers the judicial uncertainty in applying relevant statutes to protect location data as private and evaluates the government arguments for access to cell site data.<sup>14</sup> Part V analyzes the Fourth Amendment concerns in allowing government access to such information. Finally, this Note concludes that congressional clarification of the standard for government access to both cell site data and GPS tracking information is necessary.

## II. THE RISE AND POTENTIAL OF GLOBAL POSITIONING SYSTEM-ENABLED CELLULAR PHONES

### A. The Global Positioning System

The Global Positioning System consists of twenty-four earth-orbiting satellites, each broadcasting radio signals.<sup>15</sup> When a GPS receiver on Earth picks up these signals, the receiver's location can be calculated based on its distance from each satellite.<sup>16</sup> In a cellular phone, the receiver consists of a chip within the phone.<sup>17</sup> Line-of-sight communication between the receiver and three satellites allows calculation of the receiver's latitude and longitude; if a fourth satellite is available, the altitude of the receiver can also be determined.<sup>18</sup>

Today's GPS technology began as a military initiative to standardize navigation systems and aid in precision weapons delivery.<sup>19</sup> In a coordinated effort

---

spectrum of surveillance, the question is where to draw the line and how to draw the line." *Id.*

<sup>14</sup> As will be further discussed, the use of "cell site data" or "network-based" location techniques constitute one method of determining a cell phone's location; GPS technology or "handset-based" location techniques compose the principal alternative. Readers should bear this distinction in mind. *See* discussion *infra* Part III.B.

<sup>15</sup> The Global Positioning System, <http://www.gps.gov/systems/gps/index.html> (last visited Nov. 7, 2007).

<sup>16</sup> *Id.*

<sup>17</sup> 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).

<sup>18</sup> SCOTT PACE ET AL., *THE GLOBAL POSITIONING SYSTEM* 237–38 app. B (1995), *available at* [http://www.rand.org/pubs/monograph\\_reports/MR614/MR614.appb.pdf](http://www.rand.org/pubs/monograph_reports/MR614/MR614.appb.pdf).

<sup>19</sup> *Id.* at 238.

Beginning in the early 1960s, the U.S. Department of Defense began pursuing the idea of developing a global, all-weather, continuously available, highly accurate positioning and navigation system that could address the needs of a broad spectrum of users and at

among the Army, Air Force, and Navy, the first GPS satellites were launched in 1978.<sup>20</sup> That year, GPS receivers were employed on military craft in the air, sea, and on land, but individual, personal GPS receivers consisted of a twenty-five pound backpack.<sup>21</sup> The system came of age in the early 1990s during the Persian Gulf War. A shortage of military receivers compelled the Armed Forces to order more than ten thousand receivers from commercial producers.<sup>22</sup> The successful demonstration of GPS technology in the Gulf War was a major boon not only to the military, but to the fledgling commercial GPS market as well.<sup>23</sup>

Around that time, GPS also began to appear in commercial vehicles.<sup>24</sup> As GPS and other technologies have developed in the years since, the uses of GPS have multiplied and varied. The advent of high-resolution color displays and browser-enabled cell phones with high-speed wireless capabilities has led to the successful and prolific coupling of cell phones with GPS technology.<sup>25</sup> Indeed, cellular GPS units have certain advantages over their in-car brethren. In addition to providing driving directions, GPS-enabled phones can provide more useful walking directions.<sup>26</sup> Additionally, whereas the maps for in-car systems are often out-of-date by the time the car is sold and can cost hundreds of dollars to update, cellular GPS units rely on Internet servers and are thus constantly updated.<sup>27</sup>

Whether cellular or otherwise, GPS systems do have limitations. Due to their reliance on satellites, GPS receivers are prone to losing reception indoors and in dense cities.<sup>28</sup> In an effort to combat this problem, some cellular manufacturers have begun installing “assisted GPS” systems.<sup>29</sup> Assisted GPS com-

---

the same time save the [Department of Defense] money by limiting the proliferation of specialized equipment that supported only particular mission requirements.

*Id.*

<sup>20</sup> *Id.* at 240–41.

<sup>21</sup> *Id.* at 242.

<sup>22</sup> *Id.* at 245.

<sup>23</sup> *Id.* at 250.

<sup>24</sup> Smith, *supra* note 5.

<sup>25</sup> Kate Norton, *Europe Takes to Location-Based Cell Service*, BUS. WK., Oct. 13, 2006, available at [http://www.businessweek.com/technology/content/oct2006/tc20061013\\_164404.htm](http://www.businessweek.com/technology/content/oct2006/tc20061013_164404.htm).

<sup>26</sup> Michael Kanellos, *Lost? Try Asking Your Cell Phone*, CNET NEWS, Oct. 31, 2006, [http://news.com.com/2100-1039\\_3-6131236.html](http://news.com.com/2100-1039_3-6131236.html).

<sup>27</sup> Smith, *supra* note 5. Despite these advantages, fewer than three percent of cell phone users routinely consult maps or navigation on their cell phones. *Parents Want Child Tracking, Youths Want Social Networking*, GPS WORLD, Aug. 6, 2007, available at <http://lbs.gpsworld.com/gpslbs/article/articleDetail.jsp?id=447414>.

<sup>28</sup> Dan Charles, *GPS is Smartening Up Your Cell Phone*, NPR, Sept. 25, 2006, <http://www.npr.org/templates/story/story.php?storyID=6097216&sc=emaf>.

<sup>29</sup> Elena Malykhina, *Nokia Wants Your Cell Phone to Tell You Where You Are*, INFO.

bines cell tower triangulation techniques with location information from satellites.<sup>30</sup> Whether standard or assisted, GPS provides location information more accurately than traditional cell site triangulation methods.<sup>31</sup>

The commercialization of GPS has led to a plethora of not only goods, namely a wide variety of GPS receivers, but also services allowing navigation, location, and tracking.<sup>32</sup> Similarly, the internationalization of the system has allowed foreign companies to create devices and services designed to meet the demands of an array of distinct societies.<sup>33</sup> The inclusion of GPS technology in cell phones has allowed, and in fact driven, industry to find new ways to use this technology. This technology comes in forms including so-called location-based services (“LBS”), and services allowing the tracking of employees and children.<sup>34</sup>

## B. Location-Based Services

LBS operate on the principle that a person’s exact position “at a fine level of granularity (much finer than zip code), via global positioning systems [sic] (GPS), will be a datum that can be known automatically . . . and constantly utilized.”<sup>35</sup> Using such location data, LBS allow cellular subscribers to receive information about the people and places around them. LBS have already gained a substantial following in Japan and South Korea.<sup>36</sup>

---

Wk., Oct. 9, 2006, available at <http://www.informationweek.com/story/showArticle.jhtml?articleID=193105219>.

<sup>30</sup> Smith, *supra* note 5.

<sup>31</sup> See discussion *infra* Part III.B.

<sup>32</sup> The U.S. first offered GPS for civilian use in 1983. Even before the system was fully operational, it gained significant popularity among surveyors. Indeed, “[s]atellite surveying also helped sustain the commercial market for GPS equipment after the Challenger disaster shut down operations and delayed satellite launches for several years.” PACE ET AL., *supra* note 18, at 247–49.

<sup>33</sup> International use of the U.S.-created system was granted by President Reagan in the same announcement that opened GPS up for commercial use. PACE ET AL., *supra* note 18, at 247–48. As will be discussed later, internationalizing GPS has also led to a diversity of regulatory schema protecting to various degrees the rights and privacy of a society’s citizens—and furnishing a comparison and model for U.S. regulations. See *infra* notes 99–104 and accompanying text.

<sup>34</sup> *Parents Want Child Tracking, Youths Want Social Networking*, *supra* note 27.

<sup>35</sup> Jerry Kang & Dana Cuff, *Pervasive Computing: Embedding the Public Sphere*, 62 WASH. & LEE L. REV. 93, 103–04 (2005).

<sup>36</sup> Hiawatha Bray, *Cellphone GPS Services Find Their Way Into Market*, BOSTON GLOBE, Apr. 19, 2006, available at [http://www.boston.com/business/globe/articles/2006/04/19/cellphone\\_gps\\_services\\_find\\_their\\_way\\_into\\_market](http://www.boston.com/business/globe/articles/2006/04/19/cellphone_gps_services_find_their_way_into_market); see also Press Release, Frost & Sullivan, Value-Added Offerings to Spur Growth of Location-Based Services (July 3, 2007) available at <http://www.frost.com/prod/servlet/press-en-press.pag> (search “spur growth”; then follow

One such location-based application is the so-called friend-finder service, which alerts cellular subscribers when contacts are nearby.<sup>37</sup> As one commentator predicted, “GPS intelligence that we carry on our person will notify contacts in our vicinity of our precise location. This could lead to spontaneous gatherings, as people quickly find one another in real time and real places.”<sup>38</sup> In some places, such prophecies have come to fruition. In South Korea, for instance, friend-finder services already comprised more than four million members in 2005, with subscriptions growing at seventy-four percent per year.<sup>39</sup> One South Korean LBS sends text messages to friends who are within a block of one another.<sup>40</sup> Another similar service periodically texts a subscriber’s location to specified people while that subscriber is traveling.<sup>41</sup>

While social LBS took off quickly in South Korea and Japan, in America they remained in their infancy and have only recently begun to gain momentum and a strong following.<sup>42</sup> Even as MySpace<sup>43</sup> and Facebook<sup>44</sup> become commonplace online social networking sites, only twenty-six percent of American cell phone owners between ages eighteen and twenty-four want the mobile equivalent.<sup>45</sup> For those who do, however, the options for mobile social networking LBS grow daily. For instance, Boost Mobile, a subsidiary of Sprint

---

hyperlink to article). (“Japan and South Korea are by far the most developed LBS markets accounting for nearly 92 percent of the total revenues in Asia-Pacific.”).

<sup>37</sup> Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 19 (2007); see also Kang & Cuff, *supra* note 35, at 104 (“[W]hen you enter the shopping mall, all friends in your social network who are nearby can be buzzed.”).

<sup>38</sup> Zick, *supra* note 37, at 19–20.

<sup>39</sup> *Id.* South Korea makes for an interesting comparison to the United States in terms of the way its people and its government have handled the wealth of information provided by GPS. As will be seen, South Koreans have embraced this tracking technology while Americans remain generally apprehensive. See *infra* notes 99–104 and accompanying text. On the other hand, the South Korean government has regulated the use of tracking technologies in ways some American scholars advocate the U.S. government should. Jill Yung, *Big Brother is Watching: How Employee Monitoring in 2004 Brought Orwell’s 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 212–18 (2005). Interestingly, President Reagan’s decision to allow international civil use of the Global Positioning System came on the heels of the downing of Korean Airlines Flight 007 over the Soviet Union. PACE ET AL., *supra* note 18, at 247–48.

<sup>40</sup> Moon Ihlwan & Andy Reinhardt, “Working Late” Won’t Work Anymore, BUS. WK., Oct. 31, 2005, available at [http://www.businessweek.com/magazine/content/05\\_44/b3957069.htm](http://www.businessweek.com/magazine/content/05_44/b3957069.htm).

<sup>41</sup> *Id.*

<sup>42</sup> Press Release, ABIresearch, GPS-Enabled Location-Based Services (LBS) Subscribers Will Total 315 Million in Five Years (Sept. 27, 2006), available at <http://www.abiresearch.com/abiprdisplay.jsp?pressid=731>.

<sup>43</sup> MySpace, <http://www.myspace.com> (last visited Nov. 7, 2007).

<sup>44</sup> Facebook, <http://www.facebook.com> (last visited Nov. 7, 2007).

<sup>45</sup> *Parents Want Child Tracking, Youths Want Social Networking*, *supra* note 27.



asts, the company's AllSportGPS line serves a different function: it provides users with workout data and is geared toward runners and cyclists.<sup>55</sup> AllSportGPS uses GPS networks to measure distance and speed, and to record users' routes and elevations.<sup>56</sup> Both services are compatible with a number of GPS-enabled phone models from a variety of service providers.<sup>57</sup>

More importantly to businesses, GPS-enabled cell phones allow for targeted advertising. In Japan, for example, cell users can choose to receive text messages advertising sales at nearby stores.<sup>58</sup> In another variation, a subscriber's location and direction would determine the "points of interest," such as stores and restaurants on the route, displayed by the GPS unit.<sup>59</sup> MINI USA recently announced a program where drivers with a radio frequency identification ("RFID") chip on their keychain will have billboards display messages personalized for each driver.<sup>60</sup> One could easily imagine the same being done by using GPS-enabled cell phones rather than RFID chips.

The trend for such personalized advertising services is unclear.<sup>61</sup> At least one scholar believes its impact on consumers will be minor, arguing that "new forms of targeted advertising or spamming that rely upon the GPS features in personal devices will bombard an already advertising-saturated public."<sup>62</sup> On the other hand, several studies indicate that the use and popularity of such services is on the rise. Early estimates predicted that South Korean consumer spending on such services would triple to \$1.54 billion in 2007.<sup>63</sup> In thirteen

---

<sup>55</sup> Press Release, Trimble, Trimble Launches AllSport GPS for its Trimble Outdoors Product Line (Aug. 28, 2006), *available at* <http://investor.trimble.com/releasedetail.cfm?ReleaseID=209076>.

<sup>56</sup> *Id.*

<sup>57</sup> *See* Phones Supported by Trimble Outdoors, <http://www.trimbleoutdoors.com/SupportedPhones.aspx> (last visited Nov. 7, 2007); *see also* AllSportGPS Supported Devices, <http://www.allsportgps.com/phones/howtobuy.aspx> (click on carriers to see phones offered) (last visited Nov. 7, 2007).

<sup>58</sup> Ihlwan & Reinhardt, *supra* note 40.

<sup>59</sup> Kang & Cuff, *supra* note 35, at 104.

<sup>60</sup> Press Release, MiniUSA, First-Ever "Talking" Billboards Revealed to Mini Motorists; Smiles Expected as Drivers "Motorby" (Jan. 31, 2007), *available at* [http://www.miniusa.com/#/learn/awards\\_news\\_events/news](http://www.miniusa.com/#/learn/awards_news_events/news) (follow "Talking Billboards Revealed" hyperlink).

<sup>61</sup> Social and commercial location-based services are only the beginning of the LBS that are offered or that may be imagined. Weather and yellow page services, which are specific to a user's location, are at the simpler end of the spectrum; at the other end, services such as Smarter Agent provide information to realtors about recent transactions and average property values near the user's location. Charles, *supra* note 28. Indeed, Nextel has allowed access to geographic coordinates calculated by the chips in its phones. This has allowed private programmers to develop software that utilizes this information. Some of these programs are downloadable via the internet. *Id.*

<sup>62</sup> Zick, *supra* note 37, at 26.

<sup>63</sup> Ihlwan & Reinhardt, *supra*, note 40. Such growth would mark a threefold increase

other major Asian markets, spending is projected to rise at about fifteen percent per year, to a total of \$447 million by the end of 2009.<sup>64</sup> European LBS are projected to climb from just over \$180 million in 2005 to \$780 million by 2010.<sup>65</sup> Worldwide, only about 12 million cellular customers pay for LBS, but that number could increase to 315 million in five years, by one estimate.<sup>66</sup> Another report expects LBS to become an \$8.5 billion business by 2010.<sup>67</sup> In the U.S., LBS represent a \$750 million market, which is expected to double in the next two years.<sup>68</sup> Likewise, location-based functions top the list of features consumers want in their phones.<sup>69</sup> One market survey showed that, aside from talking, U.S. consumers' top three desired uses for their cell phones were "calling up maps and directions, finding friends and family members, and avoiding traffic jams."<sup>70</sup>

### C. Cellular Tracking Services

While forecasters are optimistic about the growth of LBS, the outlook is less optimistic for GPS tracking services, a second major innovation created by incorporating GPS technology into cell phones. American consumers have thus far been wary of anyone tracking their movements, at least in part due to privacy concerns. Still, forty-two percent of parents with children under thirteen report that they are willing to pay for LBS that will track their children's cell phones;<sup>71</sup> and this figure does not take into account the rising number of businesses using GPS-based tracking services to keep an electronic eye on their employees.<sup>72</sup>

---

over revenues of \$500 million in 2004. *Id.*

<sup>64</sup> Press Release, Frost & Sullivan, *supra* note 36.

<sup>65</sup> Norton, *supra* note 25. These figures include only revenues received by the cellular service providers, not those received by the stores, companies, and services offered to consumers via LBS advertising. *Id.*

<sup>66</sup> Smith, *supra*, note 5; see also Press Release, ABIresearch, *supra* note 42. In 2006, less than half a percent of wireless users subscribed to LBS; the projection of 315 million subscribers would represent a nine percent market presence. *Id.*

<sup>67</sup> Malykhina, *supra* note 29.

<sup>68</sup> Dan Costa, *Yes, I Spy on My Kid*, PC MAGAZINE, July 17, 2007, available at <http://www.pcmag.com/article2/0,1895,2145504,00.asp>.

<sup>69</sup> Ricadela, *supra* note 47.

<sup>70</sup> *Id.* (citing a study conducted in April 2006 by market research firm In-Stat, polling 1,363 "tech-savvy consumers."). One might question whether a similar study polling average cell phone users would reveal the same results, especially when many cell phone users are blissfully unaware that their cell phone contains a GPS chip.

<sup>71</sup> *Parents Want Child Tracking, Youths Want Social Networking*, *supra* note 27.

<sup>72</sup> Diane Cadrain, *GPS On Rise: Workers' Complaints May Follow*, HR MAG., Apr. 2005, available at [http://www.findarticles.com/p/articles/mi\\_m3495/is\\_4\\_50/ai\\_n13629523](http://www.findarticles.com/p/articles/mi_m3495/is_4_50/ai_n13629523).

*1. The Maternal Eye: Monitoring Children via Global Positioning System-Enabled Cell Phones*

Several companies offer services allowing parents to track their children's GPS-enabled cell phones. The uLocate service, launched in 2003, allows parents to obtain a child's last known location, as well as the direction and speed at which the child is traveling, and download the information either on their own compatible phone or via an Internet connection.<sup>73</sup> Additionally, parents can program the system to alert them when a child reaches a preset location or travels outside of a pre-defined area.<sup>74</sup>

In June 2006, the Walt Disney Company launched Disney Mobile, promoting the system as "the first national wireless phone service specifically designed for families."<sup>75</sup> The system combined voice and text services with the entertainment content one might expect from Disney, while allowing parents to closely monitor children's cell phone usage and restrict when and with whom children may use the phones.<sup>76</sup> Additionally, Disney Mobile provided a Family Locator function similar to the uLocate system. Using either their own Disney Mobile cell phone or an Internet connection, parents could locate their children's GPS-enabled Disney Mobile cell phone.<sup>77</sup> Parents could then view both a map and accuracy indicator, appearing as a red circle on the map covering the accuracy range of the phone's GPS chip.<sup>78</sup> Accessing the Family Locator function required a personal identification number set by parents.<sup>79</sup> Priced comparably to similar GPS locator services, the Disney Mobile service plan included five locates per month, with each additional locate costing forty-nine cents; or users could opt for Family Locator Unlimited, which cost about thirteen dollars per month.<sup>80</sup>

---

<sup>73</sup> Press Release, uLocate Commc'ns, Inc., New Service Enables Parents to Pinpoint Kids' Whereabouts Using Cell Phones (Oct. 6, 2003), <http://www.ulocate.com/10-6-03.php>.

<sup>74</sup> *Id.*

<sup>75</sup> Press Release, Disney Corp., Mobile Magic for Families (Apr. 5, 2006), [http://corporate.disney.go.com/news/corporate/2006/2006\\_0405\\_mobile\\_magic\\_for\\_families.html](http://corporate.disney.go.com/news/corporate/2006/2006_0405_mobile_magic_for_families.html).

<sup>76</sup> *Id.*

<sup>77</sup> See Disney Mobile, <http://disneymobile.go.com> (follow "family locator" hyperlink) (last visited Aug. 7, 2007).

<sup>78</sup> See *id.* (demonstrating the Disney Mobile Family Locator service).

<sup>79</sup> Disney Mobile, <http://www.disneymobile.go.com/disneymobile/home> (click on "Family locator"; then "View Demo"; then "Start Demo") (last visited Nov. 9, 2007).

<sup>80</sup> Disney Mobile, <http://disneymobile.go.com/disneymobile/includedServicesandFeatures.do?method=viewincludedservicesfeatures> (last visited Sept. 21, 2007); Disney Mobile Optional Services & Features, <http://disneymobile.go.com/disneymobile/browseShop.do?method=viewServicesFeatures> (last visited Sept. 22, 2007).

Perhaps responding to reservations American consumers have expressed about other such plans, Disney attempted to market the service without implicating privacy considerations. For instance, one television commercial for Disney Mobile depicted a child bragging about how “cool” his mom is for letting him have a cell phone with voice, text and Disney entertainment functions; the next scene showed his mother demonstrating functions including the Family Locator service for her adult friends, who also rave that she must be “the coolest mom ever.” Additionally, Disney promoted the GPS service as a “family locator,” when in fact adult phones on the plan could not be used to locate other adults’ phones, nor could children’s phones locate those of adults.<sup>81</sup>

The Disney Company never owned its own cell towers or equipment; rather, Disney Mobile acted as a mobile virtual network operator (“MVNO”),<sup>82</sup> having joined with Sprint, to offer cellular service using that provider’s equipment.<sup>83</sup> Shortly after launching Disney Mobile MVNO in the United States, Disney scrapped plans to offer the service in the United Kingdom,<sup>84</sup> possibly due to the disappointing performances of its two MVNOs offered in the United States.<sup>85</sup> Indeed, Disney Mobile’s domestic sales were so disappointing that in September, 2007, the company announced that it would cease operation at the

---

<sup>81</sup> Disney Mobile FAQs, <http://disneymobile.go.com/disneymobile/faq.do> (last visited Sept. 21, 2007) (Under Family Locator section see questions: “Will anyone be able to locate adult phones on my plan with Family Locator?” and “Will my child be able to locate other family members’ phones with Family Locator?”).

<sup>82</sup> A MVNO is defined as “an organization that buys minutes and services wholesale from an existing cell phone carrier (or carriers) and resells them under its own brand. . . . A MVNO is basically a reseller. It does not have radio frequency (spectrum).” NEWTON’S TELECOM DICTIONARY 624 (23 ed. 2007).

<sup>83</sup> Press Release, Disney Corp., Disney Teams with Sprint to Offer National Wireless Service for Families (July 6, 2005), available at [http://corporate.disney.go.com/news/corporate/2005/2005\\_0706\\_disneyteamsprint.html](http://corporate.disney.go.com/news/corporate/2005/2005_0706_disneyteamsprint.html).

<sup>84</sup> Jo Best, *Disney Cancels U.K. Mobile Kid-Tracking*, CNET NEWS, Aug. 14, 2006, [http://news.com.com/Disney+cancels+U.K.+mobile+kid-tracking/2100-1039\\_3-6105149.html](http://news.com.com/Disney+cancels+U.K.+mobile+kid-tracking/2100-1039_3-6105149.html); see also Bill Ray, *Disney Scraps UK Mobile Plan*, THE REGISTER, Aug. 16, 2006, [http://www.theregister.co.uk/2006/08/16/disney\\_mvno\\_pulled](http://www.theregister.co.uk/2006/08/16/disney_mvno_pulled).

<sup>85</sup> See Roger Cheng, *Mobile ESPN’s Struggle Illustrates Hardships Serving Niche Markets*, WALL ST. J., Oct. 4, 2006, at A12A (stating that the Walt Disney Company, which owned both Mobile ESPN and the Disney Mobile MVNOs, decided to end the Mobile ESPN service in September 2006 because of disappointing numbers, but kept Disney Mobile despite the possibility that it “could run into the same problem.”); see also Gene J. Koprowski, *Promising MVNO Market Fails to Meet Expectations*, E-COMMERCE TIMES, Aug. 15, 2006, <http://www.ecommercetimes.com/story/52396.html> (stating both Disney Mobile and Mobile ESPN were not competitive in market share); cf. Andrew Wallenstein, *ESPN Back in Mobile Game After Costly Flop*, REUTERS, Feb. 9, 2007, <http://www.reuters.com/article/televisionNews/idUSN0920849920070212?pageNumber=1> (announcing agreement between ESPN and both Verizon Wireless and MediaFlo USA to offer Mobile ESPN as content over carriers’ networks).

end of that year, after just 15 months of operation.<sup>86</sup> At least one factor in Disney Mobile's shutdown was intense competition among MVNOs and traditional cellular service providers.<sup>87</sup> For instance, Verizon Wireless offers the Chaperone Service, with features strikingly similar to those formerly offered by Disney Mobile.<sup>88</sup> Despite American reservations regarding cellular tracking—even of family members—companies seem likely to continue offering such services for the foreseeable future.

## 2. Paternalism in Business: Using Cellular GPS to Track Employees

Parents are not the only users of GPS cell phone tracking technology. An increasing number of employers are utilizing this technology to keep a paternalistic eye on their employees in the field.<sup>89</sup> In some cases, employers may have legitimate purposes in monitoring employee actions while on the job.<sup>90</sup> For example, several companies offer so-called “fleet management” systems.<sup>91</sup> These systems track the location of a GPS unit, and many “tout their ability to prevent theft of company assets, verify employee productivity, and reduce insurance premiums by providing carriers with evidence that drivers comply with traffic laws.”<sup>92</sup> Services such as Cingular's Work Order Manager provide dispatchers with exact locations of technicians, so the one closest to the job site can be sent.<sup>93</sup> In South Korea, at least one company uses a similar service to

---

<sup>86</sup> Press Release, Disney Corporate, Disney to End U.S.-Based MVNO Operations; Explore New Business Model for Popular Family Centric Suite of Services and Content for Mobile (Sept. 27, 2007), available at [http://corporate.disney.go.com/news/corporate/2007/2007\\_0927\\_mobile.html](http://corporate.disney.go.com/news/corporate/2007/2007_0927_mobile.html); see also *Signal Fades for Disney Mobile*, THE STREET, Sept. 27, 2007, <http://www.thestreet.com/newsanalysis/techtelecom/10381822.html>.

<sup>87</sup> Press Release, Disney Corporate, Disney to End U.S.-Based MVNO Operations; Explore New Business Model for Popular Family Centric Suite of Services and Content for Mobile (Sept. 27, 2007), available at [http://corporate.disney.go.com/news/corporate/2007/2007\\_0927\\_mobile.html](http://corporate.disney.go.com/news/corporate/2007/2007_0927_mobile.html).

<sup>88</sup> <http://www.verizonwireless.com/b2c/splash/chaperone/index.jsp>.

<sup>89</sup> Cadrain, *supra* note 72 (“[E]mployer use of global positioning system (GPS)-based employee monitoring is a wave that hasn't even begun to crest.”). Employer use of GPS technology to monitor employees provides an interesting comparison for government use of the same technology to monitor its citizens, and is discussed here for that purpose. For an in-depth analysis of the problems created by employer use of GPS tracking, and at least one proposed solution, see Yung, *supra* note 39.

<sup>90</sup> Yung, *supra* note 39, at 176–77. GPS tracking allows employers to observe any employees that are breaking the law. It may also help an employer to obtain lower insurance rates, recover lost or stolen property, and increase efficiency. *Id.*

<sup>91</sup> See, e.g., GPS Fleet Solutions, <http://www.gpsfleetsolutions.com> (last visited Nov. 7, 2007).

<sup>92</sup> Yung, *supra* note 39, at 172.

<sup>93</sup> Smith, *supra* note 5.

locate and dispatch the cab closest to a customer.<sup>94</sup> However, in the U.S., such systems have met with limited success as taxi cab drivers in New York City<sup>95</sup> and Philadelphia<sup>96</sup> have vocally opposed their installation. Trucker unions have been equally critical of such tracking measures, which they consider invasive.<sup>97</sup> One cause of criticism is that, when employed on GPS-enabled cell phones, such systems enable employers to monitor much more than their equipment; it also allows monitoring of the location and activities of employees, in some cases both on the job and in their own time.<sup>98</sup>

Nonetheless, in South Korea, sales of business-related tracking services continue to flourish.<sup>99</sup> This may be due in part to the South Korean government's willingness to regulate employer tracking. In late 2004, the National Assembly passed a law requiring a government license to gather location information on employees.<sup>100</sup> Under the law, only designated people can view the tracking information, and the tracked individual can inspect records of tracking requests.<sup>101</sup> In the United States, on the other hand, the Fourth Amendment does not apply to the private sector.<sup>102</sup> In fact, in most cases, companies providing cell phones to employees do not need to disclose that those phones can be tracked by the employer using GPS.<sup>103</sup> Only Connecticut mandates disclosure of such information.<sup>104</sup> If parents can so easily track their children using GPS-enabled cellular technology, and companies can so paternalistically monitor the actions of their employees, it bears asking whether anything stops the government from surveilling the average citizen using the same methods.

#### D. Turning it Off

Of course, one method of avoiding parental, employer, or governmental tracking via a GPS-enabled cell phone would be to simply turn off the phone's

---

<sup>94</sup> Ihlwan & Reinhardt, *supra* note 40.

<sup>95</sup> K.C. Jones, *Cabbies Say 'No' to GPS*, INFO. WK., Oct. 3, 2005, <http://www.informationweek.com/story/showArticle.jhtml?articleID=171202670>.

<sup>96</sup> Steve Inskeep, *Taxi Drivers Wary of GPS Tracking Plan*, NPR, Aug. 17, 2006, <http://www.npr.org/templates/story/story.php?storyId=5662500>.

<sup>97</sup> Rachel King, *Tracking Trucks the Telematics Way*, BUS. WK., Oct. 9, 2006, available at [http://www.businessweek.com/technology/content/oct2006/tc20061009\\_055494.htm](http://www.businessweek.com/technology/content/oct2006/tc20061009_055494.htm).

<sup>98</sup> See Yung, *supra* note 39, at 172–75.

<sup>99</sup> Ihlwan & Reinhardt, *supra* note 40.

<sup>100</sup> *Id.*

<sup>101</sup> *Id.*

<sup>102</sup> See *United States v. Jacobsen*, 466 U.S. 109 (1984) (noting that the Court has “consistently construed [Fourth Amendment] protection as proscribing only governmental action”).

<sup>103</sup> Kramer, *supra* note 4.

<sup>104</sup> Cadrain, *supra* note 72.

internal GPS receiver.<sup>105</sup> Some phones equipped with GPS enable the user to partially disable the GPS by opting for a 911-only setting.<sup>106</sup> Not all phones, however, give the user such an option, and because of the E-911 mandate, consumers cannot entirely disable the GPS chip.<sup>107</sup> Cellular service providers and third parties offering LBS via cellular GPS argue that, except for E-911, all other location-based services require the user to sign up; thus cellular subscribers will receive only the services they want and affirmatively request.<sup>108</sup> Still, just because a cell phone user does not opt for a family tracking plan or a friend-finder service does not make his phone immune to GPS tracking. Whether through GPS or tower triangulation, an active phone can be tracked.<sup>109</sup>

Employees wary of having their work phones tracked while off the clock have found some inventive ways to allegedly thwart the GPS signals. Because GPS relies on a line-of-sight connection with satellites, placing a GPS-enabled cell phone under a vehicle seat or in a glove box, or taking it inside a building may cause the signal to be lost.<sup>110</sup> More creatively, some Web sites suggest wrapping the phone in tin foil to disrupt the signal.<sup>111</sup> However, many of these techniques would also cut off the network signal, rendering the phone essentially useless.

Another method of thwarting GPS tracking, which is perhaps more practical, is to simply turn the phone off. However, this too is an uncertain solution. Even when the user presses the power button, some cell phones “can’t be fully powered down without removing the battery.”<sup>112</sup> Additionally, there is some

---

<sup>105</sup> The simplest solution, of course, would be to carry no cell phone at all. However, the ubiquity of the cell phone and the important (or vital) role it has come to play in society almost makes this not an option. Likewise, using a cell phone that is not GPS-enabled is becoming increasingly a non-option, and even those can be tracked, albeit with less accuracy, via cell tower triangulation. *See infra* Part III.B.

<sup>106</sup> Privacy Rights Clearinghouse, Fact Sheet 2(b): Cell Phone Technology (Oct. 2006), <http://www.privacyrights.org/fs/fs2b-cellprivacy.htm>.

<sup>107</sup> *See id.*

<sup>108</sup> Jay Wroldstad, *Sprint Claims First with E911-Capable Phone*, NEWSFACTOR NETWORK, Oct. 4, 2001, <http://www.newsfactor.com/perl/story/13952.html>.

<sup>109</sup> *See Talk of the Nation: Surveillance via Cell Phone*, *supra* note 12 (interview of Matt Richtel, technology correspondent for *The New York Times*). “[A]ny time you’re hooked into the network, by definition, your carrier knows where you are. Think of it this way. They need to know if you’re roaming in order to bill you extra.” *Id.*

<sup>110</sup> The GPS Primer, GPS Pitfalls, [http://gpsprimer.net/gps\\_pitfalls.html](http://gpsprimer.net/gps_pitfalls.html) (last visited Nov. 7, 2007). Taking a phone into a building to impede GPS tracking still allows anyone collecting the data to determine at least roughly which building the phone is in, and the signal will return when the phone is brought back outside.

<sup>111</sup> Global Tracking Communications Inc., GPS Tracking FAQ, <http://www.gpstrackit.com/faq.html> (last visited Nov. 7, 2007).

<sup>112</sup> Declan McCullagh, *FBI Taps Cell Phone Mic as Eavesdropping Tool*, CNET NEWS, Dec. 4, 2006,

evidence indicating that at least certain parts of a cell phone, including the microphone, can be remotely activated even when the user has turned the phone off.<sup>113</sup> If a cell phone's microphone can be remotely activated, it is entirely possible that its GPS chip, or the entire phone, could likewise be remotely activated. Even if this is not the case, powering down one's cell phone and removing the battery to avoid the possibility of GPS tracking renders the device useless. In short, there is no certain way to prevent GPS tracking of an enabled cell phone. Thus, the judiciary and the legislature must determine who may access GPS tracking data from cell phones and under what circumstances.<sup>114</sup>

### III. LEGISLATIVE CONTROL OF CELLULAR TRACKING INFORMATION

The integration of GPS into cell phones adds a new wrinkle to an area of law constantly besieged by technological advances. Although the combination of GPS and cellular technology is relatively new, scholars already have expressed concern about the Fourth Amendment issues it implicates.<sup>115</sup> Such apprehension will only increase as the technology becomes more prevalent and both private and governmental parties introduce new applications for its use.<sup>116</sup> Courts have evinced similar concerns,<sup>117</sup> but absent any precedent or legislative directive, they have been unsure how to balance privacy concerns against a legitimate need for cellular location information derived from either network-based or handset-based GPS technologies.<sup>118</sup> The state of the law is in flux,<sup>119</sup>

---

[http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029\\_3-6140191.html](http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029_3-6140191.html).

<sup>113</sup> See *United States v. Tomero*, 462 F. Supp. 2d 565, 567 (S.D.N.Y. 2006) (noting that in using a cellular phone's microphone as a bug, "[t]he device functioned whether the phone was powered on or off.>").

<sup>114</sup> *Talk of the Nation: Surveillance via Cell Phone*, *supra* note 12 (interview of Clifford Fishman, law professor at The Catholic University of America, Columbus School of Law) ("[I]f the technology exists, the capacity is there, it's a question of what the law allows, who the law allows to use the information or the technology and under what circumstances.>").

<sup>115</sup> See, e.g., *Zick*, *supra* note 37, at 3 (noting that scholarly concerns exist and will only become more relevant and prevalent "as the technologies of communication and surveillance become more widespread and more sophisticated.>").

<sup>116</sup> *Id.*

<sup>117</sup> See, e.g., *Texas Pen/Trap Case*, *supra* note 10, at 748–49 (stating that the arguments before the court have "serious implications for the balance between privacy and law enforcement"); *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 464 (D.C. Cir. 2000) (citing *In re Communications Assistance for Law Enforcement Act, Third Report and Order*, 14 F.C.C.R. 16,794, ¶ 46 (Aug. 26, 1999), for the proposition that "such a capability . . . poses difficulties that could undermine individual privacy.>").

<sup>118</sup> See *infra* Part III.B, for a discussion of network-based and handset-based location

and courts have haphazardly applied a number of statutes in deciding the types of location information to which the government should have access.<sup>120</sup> In determining the manner by which courts should protect this information, a review of the various sections of federal legislation on which the government has relied—and courts have struggled to interpret—is a crucial first step.

At the outset, it bears noting that wireless telecommunications carriers have a general duty to keep customer information private.<sup>121</sup> Wireless carriers may only divulge such “proprietary network information . . . [when] required by law or with the approval of the customer.”<sup>122</sup> Despite this general ban on disclosure, the government has made a case for access to such information based primarily on three sections of the Electronic Communications Privacy Act (“ECPA”).

#### A. The Electronic Communications Privacy Act

In 1986, Congress passed the ECPA<sup>123</sup> with the belief that it struck “a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.”<sup>124</sup> The ECPA defines the criteria that the government must meet before it can monitor electronic communications in various ways. Specifically, the statute enumerates four methods for the government to gain information from electronic communications: wiretaps,<sup>125</sup> tracking devices,<sup>126</sup> pen registers and trap and trace devices,<sup>127</sup> and stored electronic communications.<sup>128</sup>

---

technologies.

<sup>119</sup> Yung, *supra* note 39 at 196.

<sup>120</sup> See *infra* Part V (discussing the various standards courts have required before granting access to cell phone tracking information and the assortment of arguments posed by the government that courts have accepted and rejected).

<sup>121</sup> Wireless Communications and Public Safety Act of 1999, 47 U.S.C. § 222(a) (2000) (discussing a duty “to protect the confidentiality of proprietary information of, and relating to . . . customers”).

<sup>122</sup> *Id.* § 222(c)(1). “Proprietary network information” includes “information that relates to the . . . location . . . of a telecommunications service subscribed to by any customer of a telecommunications carrier.” *Id.* § 222(h)(1)(A). Indeed, “without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—(1) call location information concerning the user of a commercial mobile service.” *Id.* § 222(f).

<sup>123</sup> Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

<sup>124</sup> S. REP. NO. 99-541, at 5 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3559.

<sup>125</sup> See 18 U.S.C. § 2516 (2000). Wiretaps, governed by 18 U.S.C. §§ 2510–22, are not relevant to this discussion.

<sup>126</sup> See *id.* 18 U.S.C. § 3117. At least one commentator suggests that no part of the ECPA is applicable to GPS tracking. Yung, *supra* note 39, at 195. The government, however, has relied on the ECPA in its three main arguments for getting location information based on

### 1. Tracking Devices under the Electronic Communications Privacy Act

A “tracking device” is defined as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”<sup>129</sup> Under this definition, the ECPA does not require that the device be designed specifically as a tracking device. Rather, any device that allows tracking, whether or not that was the purpose of the device, is governed by the ECPA.<sup>130</sup> Thus, this language left open the possibility that a cell phone could be a tracking device, even if this possibility was not foreseeable when the law was passed.<sup>131</sup> Indeed, because the ECPA allowed for this possibility, cell phones are used as tracking devices today.<sup>132</sup> Accordingly, the issue the courts must determine is under what circumstances and with what evidentiary standard the government should be granted access to real-time cell site tracking information.<sup>133</sup>

### 2. The Stored Communications Act

In addition to the access granted under the ECPA’s tracking device section, the government has argued in a number of cases<sup>134</sup> that it is entitled to real-time tracking data based on another section of the ECPA, the Stored Communications Act (“SCA”).<sup>135</sup> The SCA allows the government to obtain the contents of a wire or electronic communication being stored in either electronic storage or a remote computing service.<sup>136</sup> More specifically, section 2703(c) grants the

---

tower triangulation. See discussion *infra* Part V. It is well within the realm of possibilities that the ECPA may be relied on to argue for tracking data from GPS-enabled cell phones as well.

<sup>127</sup> See *id.* 18 U.S.C. §§ 3121–26.

<sup>128</sup> See *id.* 18 U.S.C. §§ 2701–10.

<sup>129</sup> *Id.* § 3117(b).

<sup>130</sup> FISHMAN & MCKENNA, *supra* note 9, at 150; see also *Texas Pen/Trap Case*, *supra* note 10, at 753 (“Aside from its welcome brevity, the definition is striking for its breadth.”).

<sup>131</sup> *Texas Pen/Trap Case*, *supra* note 10, at 754.

<sup>132</sup> FISHMAN & MCKENNA, *supra* note 9, at 153 (“Given that current cellular technology permits, and the Federal Communications Commission requires, that cellular phones be able to be tracked in real time to within 100 meters of the phone’s exact location, cellular phones are for all intent and purposes, tracking devices.”).

<sup>133</sup> See discussion *infra* Part V.

<sup>134</sup> See, e.g., *Texas Pen/Trap Case*, *supra* note 10, at 765; *In re Application of the United States for Orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices on Tel. Nos. [Sealed] and [Sealed]*, 416 F. Supp. 2d 390 (D. Md. 2006) [hereinafter *Maryland Pen/Trap Case*].

<sup>135</sup> Stored Communications Act, 18 U.S.C. §§ 2701–11 (2000).

<sup>136</sup> *Id.* § 2703(a)–(b). The term “electronic storage” means “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” *Id.* § 2510(17). The term “re-

government access to “records concerning electronic communication service.”<sup>137</sup> Unlike other parts of the ECPA, the SCA allows disclosure of this information with a comparatively low standard of “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.”<sup>138</sup> The higher probable cause standard is not required—and the Fourth Amendment is not implicated—because the information the cell service provider gathered for its “own legitimate business purposes,” belongs to the carrier, and not the subscriber.<sup>139</sup>

### 3. *The Communications Assistance to Law Enforcement Act and the “Pen/Trap Statute”*

Pen/Trap orders are among the most frequently employed criminal law enforcement mechanisms.<sup>140</sup> The use of pen registers,<sup>141</sup> or trap and trace devices,<sup>142</sup> is governed by the “Pen/Trap Statute.”<sup>143</sup> This statute grants the gov-

mote computing service” is defined as “the provision to the public of computer storage or processing services by means of an electronic communications system.” *Id.* § 2711(2).

<sup>137</sup> *Id.* § 2703(c). This information includes the name, address, phone number, length, and types of service. *Id.* § 2703(c)(1)(C).

<sup>138</sup> *Id.* § 2703(d).

<sup>139</sup> *People v. Hall*, 823 N.Y.S.2d 334, 343 (N.Y. Sup. Ct. 2006).

<sup>140</sup> *Texas Pen/Trap Case*, *supra* note 10, at 749.

<sup>141</sup> Pen registers collect certain information about calls placed from a particular telephone line and are defined as:

[A] device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

18 U.S.C. § 3127(3).

<sup>142</sup> Trap and trace devices collect certain information about calls coming in to a particular telephone number and are defined as:

[A] device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.

*Id.* § 3127(4).

<sup>143</sup> The Pen/Trap Statute refers to 18 U.S.C. §§ 3122–27. FISHMAN & MCKENNA, *supra* note 9, at 146. Because they are governed by the same statute, pen registers and trap and

ernment access to information related to the processing and transmission of wire or electronic communications, but not the contents of those communications.<sup>144</sup> The government has argued in a number of cases that this includes location information for calls made from cell phones.<sup>145</sup>

The government's advantage from obtaining tracking location information via the Pen/Trap Statute, as opposed to other portions of the ECPA, is the statute's relatively low standard of proof.<sup>146</sup> An order authorizing the use of a pen/trap device requires only that the government show that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."<sup>147</sup> Such little protection stems from the Supreme Court's holding in *Smith v. Maryland* that no reasonable expectation of privacy exists as to the phone numbers a person dials.<sup>148</sup> Compared to the SCA's specific and articulable facts standard or a probable cause requirement, this standard is relatively low and easier for the government to meet.<sup>149</sup> Thus, this lower threshold, if accepted by the courts, would permit access to invaluable information while severely encroaching on Fourth Amendment protections.

The Communications Assistance to Law Enforcement Act ("CALEA"),<sup>150</sup> however, makes clear why the ECPA's Pen/Trap Statute is not applicable to GPS phones. CALEA was enacted in 1994 "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes."<sup>151</sup> It provides that a communications carrier may not provide, and

---

trace devices will hereinafter be referred to as "pen/trap devices."

<sup>144</sup> 18 U.S.C. § 3121(c) (Supp. IV 2004).

<sup>145</sup> See, e.g., *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Data*, 412 F. Supp. 2d 947 (E.D. Wis. 2006) [hereinafter *Wisconsin Pen/Trap Case*]; *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) [hereinafter *New York Pen/Trap Case*]; *Texas Pen/Trap Case*, *supra* note 10.

<sup>146</sup> See FISHMAN & MCKENNA, *supra* note 9, at 147.

<sup>147</sup> 18 U.S.C. § 3123(a)(1) (Supp. IV 2004).

<sup>148</sup> *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979).

<sup>149</sup> Police need not demonstrate probable cause, nor even provide "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d) (2000).

<sup>150</sup> Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279.

<sup>151</sup> H.R. REP. NO. 103-827, at 9 (1994), as reprinted in 1994 U.S.C.C.A.N. 3489, 3489; see also, Stephanie Lockwood, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J. L. & TECH. 307, 312 (2004) (stating that CALEA was enacted "to enumerate the obligations of telecommunications carriers to aid in intercepting digital communications.").

the government may not obtain, “any information that may disclose the physical location of the subscriber” when the government’s access is “acquired solely pursuant to the authority for pen registers and trap and trace devices.”<sup>152</sup> Nonetheless, the government has attempted to argue the Pen/Trap Statute as a basis for obtaining such information.<sup>153</sup>

## B. The Enhanced 911 System

Of course, if the location of a particular cell phone could not be determined, any argument that the government was entitled to such information would be moot. However, technological advances coupled with a federal statute have not only made such cell location possible but have mandated it.<sup>154</sup> Cell location information is already available and being utilized in myriad ways. This availability is due at least in part to the enhanced 911 (“E-911”) program: a Federal Communications Commission (“FCC”) initiative created to aid emergency response services.<sup>155</sup>

Since 1996, the FCC has promulgated a series of orders that have collectively implemented the E-911 system.<sup>156</sup> These E-911 regulations<sup>157</sup> are “aimed at improving the reliability of wireless 911 services and identifying the location of wireless 911 callers to enable emergency response personnel to provide assistance to them much more quickly.”<sup>158</sup> Prior to the E-911 regulations, the location of a 911 caller using a traditional landline was determined through a reverse telephone directory.<sup>159</sup> A dispatcher then provided directions to emergency personnel based on the address associated with that telephone number.<sup>160</sup> This system, however, did not comport with the rapid expansion of cellular telephone use. Thus, the FCC established the E-911 system to ensure that 911

---

<sup>152</sup> 47 U.S.C. § 1002(a)(2) (2000).

<sup>153</sup> See discussion *infra* Part V.B.

<sup>154</sup> Reardon, *supra* note 2.

<sup>155</sup> FCC Enhanced 911, <http://www.fcc.gov/pshs/911/enhanced911/Welcome.html> (last visited Nov. 7, 2007).

<sup>156</sup> See *In re* Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Report and Order and Further Notice of Proposed Rulemaking*, 11 F.C.C.R. 18,676 (June 12, 1996); *In re* Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Third Report and Order*, 14 F.C.C.R. 17,388 (Sept. 15, 1999).

<sup>157</sup> 47 C.F.R. § 20.18 (2006).

<sup>158</sup> FCC CONSUMER FACTS: WIRELESS 911 SERVICES 2 (2006), <http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.pdf>.

<sup>159</sup> FCC CONSUMER FACTS: COMMUNICATING DURING EMERGENCIES 1–2 (2005), <http://www.fcc.gov/cgb/consumerfacts/emergencies.pdf>.

<sup>160</sup> *Id.* at 2.

callers using cell phones could be located with almost the same ease and accuracy as locating a land-based 911 caller.<sup>161</sup>

The FCC implemented this system in two phases. Phase I required that cellular service providers be able to provide to emergency dispatchers the cell phone number and the location of the cell.<sup>162</sup> Under Phase II, cellular service providers must provide more accurate location information geographically by latitude and longitude.<sup>163</sup> The compliance and accuracy standards for Phase II depend on the method chosen by the cellular service provider to comply with those requirements.<sup>164</sup>

Current technology presents providers with two primary methods by which to obtain the location of a 911 caller in compliance with phase II.<sup>165</sup> The first option involves network-based location technologies.<sup>166</sup> These techniques use triangulation of cell phone signals picked up by three or more non-linear cell towers.<sup>167</sup> The location of a cellular phone is calculated based on “the known speed of radio signals.”<sup>168</sup> The E-911 regulations required service providers choosing this route to comply with the Phase II requirements by October 2002, i.e., that such services must be accurate to within three hundred meters for ninety-five percent of calls, and to within one hundred meters for two-thirds of 911 calls.<sup>169</sup> Unfortunately, three hundred feet (approximately ninety-one meters) is the limit of accuracy for such triangulation techniques,<sup>170</sup> thus limiting the aid such techniques can provide to emergency responders in locating 911 callers. Indeed, the FCC has notified a number of wireless service providers

---

<sup>161</sup> *Id.*; see also *In re* Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, *Third Report and Order*, 14 F.C.C.R. 17,388, ¶¶1–8 (Sept. 15, 1999) (noting the importance of locating emergency callers in a timely manner).

<sup>162</sup> 47 C.F.R. § 20.18(d)(1). “As of April 1, 1998 . . . licensees subject to this section must provide the telephone number of the originator of a 911 call and the location of the cell site or base station receiving a 911 call from any mobile handset accessing their systems to the designated Public Safety Answering Point.” *Id.* “The term ‘public safety answering point’ means a facility that has been designated to receive emergency calls and route them to emergency service personnel.” 47 U.S.C. § 222(h)(4) (2000).

<sup>163</sup> 47 C.F.R. § 20.18(e).

<sup>164</sup> See *id.* § 20.18(h).

<sup>165</sup> A third, hybrid option called “assisted GPS” also exists. See *supra* notes 29–31 and accompanying text.

<sup>166</sup> 47 C.F.R. § 20.18(f). As of early 2007, only about seventy percent of emergency call centers had become E-911 compliant, covering approximately eighty percent of the population. Marguerite Reardon, *Homing in on a Plan for Cellular 911*, ZDNET NEWS, June 4, 2007, [http://news.zdnet.com/2100-1035\\_22-6188332.html](http://news.zdnet.com/2100-1035_22-6188332.html).

<sup>167</sup> Holloway et al., *supra* note 17, at 103.

<sup>168</sup> *Id.*

<sup>169</sup> 47 C.F.R. § 20.18(h)(1).

<sup>170</sup> Norton, *supra* note 25.

that such network-based technology “does not provide an adequate level of public safety for callers.”<sup>171</sup>

While some cellular providers still use these network-based technologies, others have adopted handset-based location technologies to meet the Phase II requirements of the E-911 regulations.<sup>172</sup> Handset-based location technologies operate using GPS information to locate a phone.<sup>173</sup> Unlike network-based technologies, GPS has an accuracy of approximately thirty feet.<sup>174</sup> This accuracy depends on the number of line-of-sight connections satellites can make with a phone.<sup>175</sup> The FCC took into account the greater accuracy of GPS-reliant handset-based systems when it set Phase II requirements for such technology.<sup>176</sup> Cellular service providers choosing the handset-based option must be able to provide an accurate location to within fifty meters for two-thirds of calls, and to within one hundred fifty meters for ninety-five percent of calls.<sup>177</sup>

Integration of GPS technology has accelerated as a result of FCC regulations. The FCC’s E-911 regulations have encouraged rapid growth in the development of cellular phones incorporating GPS systems.<sup>178</sup> Sprint introduced the first GPS-enabled phone: the Samsung SPH-300, which hit the market just prior to the FCC’s October 1, 2001 deadline for Phase II introduction of handset-based technologies.<sup>179</sup> With the introduction of the SPH-300, Sprint became the only cell service provider to meet the FCC’s deadline, while other providers requested extensions.<sup>180</sup> Since then, dozens of other GPS-enabled cell phones have entered the market, allowing other cell service providers to com-

---

<sup>171</sup> Holloway et al., *supra* note 17, at 104.

<sup>172</sup> Charles, *supra* note 28 (“Some companies, such as Cingular, adopted technology that locates a cell phone by analyzing how its signal is picked up by different cell towers. Others, including Verizon, Sprint and Nextel, decided to install a GPS receiver in every cell phone. This generally determines location more accurately . . .”).

<sup>173</sup> Holloway et al., *supra* note 17, at 103. For an overview of the Global Positioning System, see *supra* Part II.A.

<sup>174</sup> Norton, *supra* note 25. If the accuracy is increased by a factor of ten, then the area in which the phone may be located is decreased by a factor of one hundred, thereby providing greater accuracy to firemen, police officers, EMTs, and indeed to the 911 caller. *Id.*

<sup>175</sup> Holloway et al., *supra* note 17, at 103.

<sup>176</sup> Compare 47 C.F.R. § 20.18(h)(1) (2006) (setting forth network-based accuracy requirements), with *id.* § 20.18(h)(2) (setting forth handset-based accuracy requirements).

<sup>177</sup> *Id.* § 20.18(h)(2).

<sup>178</sup> See Charles, *supra* note 28.

<sup>179</sup> Press Release, Sprint, Sprint and Samsung Telecommunications America Launch America’s First GPS-Enabled Wireless Phone, The Sprint PCS SPH-N300 (Oct. 1, 2001), available at <http://spatialnews.geocomm.com/dailynews/2001/oct/01/news8.html>.

<sup>180</sup> *Id.*

ply with Phase II of the E-911 regulations.<sup>181</sup> In turn, this has led to more accurate information for first responders, and increased public safety.<sup>182</sup>

#### IV. FOURTH AMENDMENT IMPLICATIONS OF CELL PHONE TRACKING

As cellular phones proliferate and evolve, the privacy considerations implicated by their use follow a similar trend. The technology of cellular phones is most implicated in the Fourth Amendment prohibition of unreasonable searches and seizures. Likewise, the solution to these privacy concerns lies within the Fourth Amendment's requirement of probable cause to demonstrate the reasonableness of a search or seizure. Specifically, the Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."<sup>183</sup> The exact application of this text to electronic communications, in general, and to cellular tracking, in particular, has proven a struggle for the courts.

##### A. *Katz* and *Smith*: Foundations of Fourth Amendment Protections

In *Katz v. United States*, the Supreme Court held that electronic recording by the government of a conversation made from a public telephone booth violated the caller's Fourth Amendment right to be free from unreasonable searches.<sup>184</sup> The decision hinged on the fact that although the call was placed in public, the caller took steps to isolate himself and maintain the privacy of his conversation.<sup>185</sup> While important for the premise that the Fourth Amendment protects what one seeks to keep private, and society agrees is private, *Katz* gives little guidance regarding the application of the Fourth Amendment to cell site or GPS tracking data obtained from a cell phone. In fact, the case's main contribution to Fourth Amendment construction comes from Justice Harlan's con-

---

<sup>181</sup> *Id.*

<sup>182</sup> See FCC CONSUMER FACTS: WIRELESS 911 SERVICES, *supra* note 158, at 2.

<sup>183</sup> U.S. CONST. amend. IV.

<sup>184</sup> *Katz v. United States*, 389 U.S. 347, 353 (1967).

<sup>185</sup> *Id.* at 351–52. The Majority noted:

No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

*Id.* at 352.

currence, which provided a two-part test to determine whether the information is protected: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”<sup>186</sup>

More than a decade later, the Supreme Court adopted Justice Harlan’s two-fold requirement in *Smith v. Maryland*.<sup>187</sup> In *Smith*, law enforcement, acting without a warrant, installed a pen register device to record numbers dialed from the defendant’s phone.<sup>188</sup> Applying the twofold analysis, the Court held that the Fourth Amendment did not apply. In doing so, the Court first found it doubtful that telephone users have any expectation of privacy regarding the numbers they dial.<sup>189</sup> Nor did the defendant manifest any such expectation through his actions.<sup>190</sup> The defendant “voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business.”<sup>191</sup> The Court further explained that while the defendant’s actions of placing the calls from his home phone may have been calculated to keep the contents of the conversation private, a pen register is unable to record the contents of electronic communications, merely the numbers dialed by a phone.<sup>192</sup> Therefore, applying Justice Harlan’s test, the Court stated that even if the defendant had manifested such an expectation of privacy, society was not prepared to regard that expectation as reasonable.<sup>193</sup>

Applying the two-part analysis, the Court held that the use of a pen register to record outgoing calls from the defendant’s phone did not constitute a search.<sup>194</sup> Thus, no Fourth Amendment protection existed, and the device could be installed and used without a warrant.<sup>195</sup> Congress responded by enacting the ECPA, particularly the Pen/Trap Statute, which codifies the holding in *Smith*, at least insofar as it establishes that something less than probable cause is required for the installation and use of a pen/trap device.<sup>196</sup>

---

<sup>186</sup> *Id.* at 361 (Harlan, J., concurring).

<sup>187</sup> *Smith v. Maryland*, 442 U.S. 735, 740 (1979).

<sup>188</sup> *Id.* at 737. For a description of pen register devices, see *supra* Part III.A.3.

<sup>189</sup> *Smith*, 442 U.S. at 742.

<sup>190</sup> *Id.* at 743 (observing that the use of a home phone may have been calculated to keep the contents of the conversation private, similar to the use of an enclosed public telephone in *Katz*, but that nothing he did preserved the privacy of the numbers dialed by the defendant).

<sup>191</sup> *Id.* at 744.

<sup>192</sup> *Id.* at 741, 743.

<sup>193</sup> *Id.* at 745.

<sup>194</sup> *Id.* at 745–46.

<sup>195</sup> *Id.*

<sup>196</sup> See discussion *supra* Part III.A.3.

### B. *Knotts* and *Karo*: The Tracking Device Cases

In addition to codifying the standard for pen/trap devices, the ECPA defines tracking devices and establishes that probable cause must be demonstrated before law enforcement may use a tracking device.<sup>197</sup> Prior to the passage of the ECPA, any Fourth Amendment protection from tracking devices came solely from case law.<sup>198</sup>

In 1983, the Supreme Court ruled in *United States v. Knotts* that a tracking device placed in the defendant's vehicle and used to follow the car when it was out of visual surveillance constituted neither a search nor seizure, and therefore was not subject to the probable cause requirement of the Fourth Amendment.<sup>199</sup> The *Knotts* decision turned on the fact that the canister that the defendant was transporting was being tracked on public roads.<sup>200</sup> In applying the *Smith* analysis, the Court found that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."<sup>201</sup> Anyone who happened to be on the same roads, and cared to look, could have obtained the information acquired by the tracking device.<sup>202</sup> In arriving at its decision, the Court noted that such tracking devices serve only to effectuate observation of already public occurrences, relying heavily on the fact that the device was not used to track the defendant inside private spheres such as a residence, which is clearly protected by the Fourth Amendment.<sup>203</sup> The importance of this distinction was realized the following year, when the Supreme Court confronted the issue of a tracking device's use in a private residence in *United States v. Karo*.<sup>204</sup>

In *Karo*, law enforcement officials used a tracking device to track certain drug-related chemicals through a series of private residences and storage lockers.<sup>205</sup> The defendant challenged such use of a tracking device, claiming that surveillance inside private residences violated the Fourth Amendment.<sup>206</sup> The Court stated, "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justi-

---

<sup>197</sup> *See id.*

<sup>198</sup> *See* S. REP. NO. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

<sup>199</sup> *United States v. Knotts*, 460 U.S. 276, 285 (1983).

<sup>200</sup> *Id.*

<sup>201</sup> *Id.* at 281.

<sup>202</sup> *Id.* at 285.

<sup>203</sup> *Id.* at 284–85.

<sup>204</sup> *See United States v. Karo*, 468 U.S. 705 (1984).

<sup>205</sup> *Id.* at 708–09.

<sup>206</sup> *Id.* at 713–14.

fiable.”<sup>207</sup> Ultimately, the Court held that a search of a private residence, even when conducted with a tracking device, must be conducted pursuant to a warrant obtained after demonstrating probable cause.<sup>208</sup> Following the *Karo* decision, the ECPA amended the section governing tracking devices to require a warrant based on probable cause.<sup>209</sup>

### C. The Probable Cause Requirement and Rule 41 Warrants

Following the *Knotts* decision and the enactment of the ECPA, a demonstration of probable cause is required before a warrant may issue allowing the search or seizure of a person, place, or effect protected by the Fourth Amendment. Rule 41 of the Federal Rules of Criminal Procedure governs the issuance of such probable cause warrants.<sup>210</sup> This rule provides that a magistrate or other 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.”<sup>211</sup> The rule also lays out what the warrant must contain<sup>212</sup> and what types of people and property may be searched and seized pursuant to such a warrant.<sup>213</sup> Likewise, it lays out the requirements for a warrant authorizing the installation and use of a tracking device.<sup>214</sup> Specifically, a warrant for a tracking device must “identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used.”<sup>215</sup> Rule 41 relies on the ECPA’s definition of tracking device.<sup>216</sup>

Thus, if the courts or Congress determine that a GPS-enabled cell phone can be used as a tracking device under this definition, a warrant based on probable cause must be required to authorize law enforcement to use it. Only such a warrant sufficiently protects the Fourth Amendment considerations implicated by law enforcement use of cell phones to determine location. This is especially true in light of the *Karo* decision because cell phones are frequently carried into private residences and other locations where a reasonable expectation of privacy may exist.

---

<sup>207</sup> *Id.* at 714.

<sup>208</sup> *Id.* at 718.

<sup>209</sup> See 18 U.S.C. § 3117 (2000).

<sup>210</sup> FED. R. CRIM. P. 41.

<sup>211</sup> FED. R. CRIM. P. 41(d)(1).

<sup>212</sup> Fed. R. Crim. P.41(e)(2).

<sup>213</sup> FED. R. CRIM. P. 41(c).

<sup>214</sup> FED. R. CRIM. P. 41(e)(2)(B).

<sup>215</sup> *Id.*

<sup>216</sup> FED. R. CRIM. P. 41(a)(2)(E) (stating that “[t]racking device’ has the meaning set out in 18 U.S.C. § 3117(b)”); see also discussion *supra* Part III.A.1.

## V. JUDICIAL INDECISION REGARDING THE CLASSIFICATION OF CELLULAR TRACKING DATA

Justice Brandeis prophetically stated 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.”<sup>217</sup> When Justice Brandeis so opined in 1928, nobody could have imagined the technological leaps that have allowed for cellular telephones and GPS satellites. The technology that has brought together families and friends, sellers and consumers, simultaneously provides almost boundless potential for domestic spying through real-time tracking data collected via cellular GPS signals. In an age when terrorism prevention is used to justify preemptive government intrusion into the private sphere while watch lists and biometrics aid the cause,<sup>218</sup> cellular tracking is just one of dozens of threats to personal privacy interests and the Fourth Amendment. Courts face the prospect of balancing legitimate law enforcement goals against deeply enscorced privacy interests of American citizens, and these concerns must be balanced with regard to traditional implements, new innovations, and technologies not yet even on the drawing board.<sup>219</sup>

Several courts have been asked to give the government access to real-time cell phone tracking information. Thus far, while a few federal district courts have tried to tackle the issue, no circuit court has taken up the question.<sup>220</sup> Among the courts that have examined the issue, no clear consensus has developed as to whether the government should be allowed access to this data, and if so, what burden of proof is required to get it.<sup>221</sup> Notably, so far, these courts have only been asked to deal with network-based technologies, those less-accurate methods of cellular location based on tower triangulation.<sup>222</sup> It seems that no court has specifically been asked to grant government access to real-time cellular GPS tracking information. However, the two systems are quite similar,<sup>223</sup> and by analogizing GPS methods to these network-based cases, it

---

<sup>217</sup> *Olmstead v. United States*, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

<sup>218</sup> See Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy*, 13 MICH. TELECOM. & TECH. L. REV. 541, 546 (2007); Karen DeYoung, *U.S. Watch Lists Are Drawn From Massive Clearinghouse*, WASH. POST, Mar. 25, 2007, at A01.

<sup>219</sup> *Talk of the Nation: Surveillance via Cell Phone*, *supra* note 12 (interview of Matt Richtel, technology correspondent for *The New York Times*) (“[T]his debate happens each time there are technological advances, and the law has to catch up to them.”).

<sup>220</sup> FISHMAN & MCKENNA, *supra* note 9, at 149.

<sup>221</sup> *Id.* at 147.

<sup>222</sup> See *id.*

<sup>223</sup> See discussion *supra* Part III.B.

should be obvious that courts will face the same and perhaps even greater problems when asked to grant the government access to more accurate real-time tracking information possible through the GPS.

The primary issue for the courts to resolve in these cases has been to determine what standard the government must meet under the ECPA to obtain real-time cell site tracking data. Specifically, the issue focuses on whether such data is properly classified as: (1) “[r]ecords concerning electronic communication service”<sup>224</sup> under the SCA, and therefore obtainable upon the intermediate standard of “specific and articulable facts;”<sup>225</sup> or (2) information collected by Pen/Trap devices, which requires only proof of relevance to an ongoing criminal investigation;<sup>226</sup> or finally, (3) information collected by cell phones which should be considered “tracking devices” and their real-time location available only with a probable cause warrant, the strictest standard.<sup>227</sup> The government has made several innovative, if not always persuasive, arguments in trying to obtain cell site information based on a standard lower than probable cause.<sup>228</sup> By advocating these lower standards, “the government seeks to avail itself of the easiest, least stringent means possible to obtain that information under the current statutory scheme.”<sup>229</sup>

#### A. Tracking Information Does Not Fit Within the Stored Communication Act

A logical first step in categorizing cell site information, and, thus, determining what standard must be met before law enforcement may obtain such data, is to look at the government’s claim that cell site data falls within the SCA and is obtainable with proof of “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.”<sup>230</sup> That there is no mention of cell site data in the plain language of the statute is the first strike against this argument. While the laundry list of subscriber information obtainable under

---

<sup>224</sup> 18 U.S.C. § 2703(c) (Supp. IV 2004). This information includes the name, address, phone number, length and types of service, and means of payment for such services. *Id.* § 2703(c)(2).

<sup>225</sup> *Id.* § 2703(d).

<sup>226</sup> *Id.* § 3123(a)(1)–(2).

<sup>227</sup> See *Texas Pen/Trap Case*, *supra* note 10, at 753 (setting out the hierarchy of burdens the government must meet to obtain authority to interfere with private electronic communications).

<sup>228</sup> FISHMAN & MCKENNA, *supra* note 9, at 153.

<sup>229</sup> *Id.* at 151.

<sup>230</sup> 18 U.S.C. § 2703(d).

this section does include “address,”<sup>231</sup> “this plainly refers to the subscriber’s nominal residence for billing or contact purposes, rather than the physical location(s) where the mobile phone is used.”<sup>232</sup>

A second strike against the SCA argument is the fact that the SCA does not contemplate providing law enforcement with the ability to conduct real-time prospective surveillance. The statute’s language shows that it was not enacted with the purpose of allowing such real-time tracking.<sup>233</sup> The SCA grants access to “stored” communications; it does not regulate access to real-time data.<sup>234</sup>

Finally, the government resorts to an argument based on the SCA’s language that law enforcement “may require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service.”<sup>235</sup> The legislative history of the SCA indicates that the information contemplated in the statute is “information about the customer’s use of the service not the content of the customer’s communications.”<sup>236</sup> The government has argued that cell site data falls within the ambit of this allowance and is thus obtainable under the SCA.<sup>237</sup> At least one court has rejected this argument by looking at the statutory definition of “electronic communication.”<sup>238</sup> This definition excepts all communications from a tracking device.<sup>239</sup> Thus, after deciding that a cell phone constituted a tracking device, one court reached the conclusion that “[t]racking device information such as cell site data is plainly not a form of electronic communication at all.”<sup>240</sup> It then follows that such information is not obtainable under the SCA and its concomitant lower standard.

Writing for the U.S. District Court for the Southern District of Texas, Judge Smith made a troubling observation related to the SCA. In discounting any argument for cell-site information, he noted that because a cell user “does not use the phone to track his own movements in real time, prospective cell site data appears to be unrelated to any *customer* (as opposed to law enforcement) use of the provider’s services.”<sup>241</sup> Were real-time cell site data used by the customer, however, the implication is that such data might be obtainable under the SCA. With GPS-enabled cell phones, customers may very well use the phone

---

<sup>231</sup> *Id.* § 2703(c)(2).

<sup>232</sup> *Texas Pen/Trap Case*, *supra* note 10, at 758.

<sup>233</sup> *Maryland Pen/Trap Case*, *supra* note 134, at 395.

<sup>234</sup> FISHMAN & MCKENNA, *supra* note 9, at 152.

<sup>235</sup> 18 U.S.C. § 2703(c)(1).

<sup>236</sup> S. REP. NO. 99-541, at 38 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3592.

<sup>237</sup> *See discussion supra* Part III.A.2.

<sup>238</sup> *Texas Pen/Trap Case*, *supra* note 10, at 758–59.

<sup>239</sup> 18 U.S.C. § 2510(12)(C) (2000).

<sup>240</sup> *Texas Pen/Trap Case*, *supra* note 10, at 759.

<sup>241</sup> *Id.* (emphasis in original).

to track their own movements (or more accurately, to map exactly where they want to go just before or as they go there). By Judge Smith's reasoning, then, GPS location data could be considered customer information, thereby falling under Congress' understanding of the information available through resort to the SCA. On the other hand, this argument may still be rejected by recalling that information from a tracking device has traditionally been held unobtainable under the SCA. Still, this counter-argument demonstrates the need for Congressional clarification of what standard must be met before cell site data (and its analogue, GPS tracking data) may be obtained by the government. Because the SCA does not allow the government to obtain real-time cell site data, the next logical place to look for such an allowance is within the ECPA's Pen/Trap Statute.

#### B. The Pen/Trap Statute Does Not Grant Access to Tracking Data

Even though such arguments still require a mere demonstration of relevance, courts have put more stock in, or at least had a more difficult time refuting, government arguments based on the Pen/Trap Statute. Two cases in particular have provided analyses of the Pen/Trap Statute as a mechanism for granting government access to cell site location data.<sup>242</sup> The U.S. District Court for the Southern District of Texas was willing to throw out the Pen/Trap Statute with minimal analysis stating that "[t]he minimal pen/trap standard does not authorize access to cell site data; Congress made that much clear in the Communications Assistance to Law Enforcement Act of 1994 ("CALEA")."<sup>243</sup> Indeed, the legislative history of CALEA appears to support this conclusion. In enacting CALEA, Congress intended to remedy the privacy concerns caused by the fact that "in some cellular systems, transactional data that could be obtained by a pen register may include location information."<sup>244</sup> Through its plain language and legislative history, CALEA clearly shows the Pen/Trap Statute to be an insufficient basis for obtaining cell site data.

The U.S. District Court for the Southern District of New York held that the Pen/Trap Statute is at least in part an acceptable instrument through which the government may obtain cell site data.<sup>245</sup> In its analysis, the court first noted that the USA PATRIOT Act amended the Pen/Trap Statute, adding "signaling information" to the laundry list of information obtainable through a pen regis-

---

<sup>242</sup> See *New York Pen/Trap Case*, *supra* note 145; *Texas Pen/Trap Case*, *supra* note 10.

<sup>243</sup> *Texas Pen/Trap Case*, *supra* note 10, at 757.

<sup>244</sup> H. REP. NO. 103-827, at 17 (1994), as reprinted in 1994 U.S.C.C.A.N. 3489, 3497.

<sup>245</sup> *New York Pen/Trap Case*, *supra* note 145, at 449.

ter.<sup>246</sup> The court then accepted the proposition that the term “signaling information” includes location information related to the towers used by a particular cell phone.<sup>247</sup> In interpreting this term to include cell site data, the court held that the Pen/Trap Statute would have allowed the government to access such data.<sup>248</sup> However, by excepting location data from call-identifying information available to law enforcement, CALEA “plainly reflects an underlying assumption that physical location data *would* have been obtainable under the Pen Register Statute in the absence of the exception clause [of CALEA].”<sup>249</sup> Thus, because of CALEA’s exception clause, cell site information is not obtainable under the Pen/Trap Statute of the ECPA.

Regardless of this apparent clarity, the U.S. District Court for the Southern District of New York went on to scrutinize the language of CALEA, finding what it interpreted as a loophole that allowed government access to cell site information. Rather than forbidding cell site information “pursuant” to the Pen/Trap Statute, the text of CALEA includes the phrase “solely pursuant.”<sup>250</sup> This language left the court “with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination of the Pen Register Statute with some other unspecified mechanism.”<sup>251</sup>

This idea of combining the Pen/Trap Statute with other statutory authority is known as the hybrid theory.<sup>252</sup> The government’s most common hybrid argument is that the combination of the Pen/Trap Statute and the SCA permit it to

---

<sup>246</sup> *New York Pen/Trap Case*, *supra* note 145, at 438–39 (citing USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 216(c)(2), 115 Stat. 272, 290). The Pen/Trap Statute defines “pen register” as a “device or process which records or decodes dialing, routing, addressing, or *signaling information* transmitted by an instrument or facility from which a wire or electronic communication is transmitted.” 18 U.S.C. § 3127(3) (Supp. IV 2004) (emphasis added).

<sup>247</sup> *New York Pen/Trap Case*, *supra* note 145, at 439 (citing U.S. Telecom Ass’n. v. FCC, 227 F.3d 450, 463–64 (D.C. Cir. 2000)).

<sup>248</sup> *Id.* at 440. The court did not, however, reach the issue of whether “signaling information” would allow the government, to continuously track a cell phone regardless of call activity. *Id.* at 439 n.2.

<sup>249</sup> *New York Pen/Trap Case*, *supra* note 145, at 440 (emphasis in original).

<sup>250</sup> 47 U.S.C. § 1002(a)(2)(2000).

<sup>251</sup> *New York Pen/Trap Case*, *supra* note 145, at 442; *see also In re Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services*, No. 1:06-MC-6, 2006 WL 1876847, at \*3 (N.D. Ind. July 5, 2006) [hereinafter *Indiana Pen/Trap Case*] (“The use of the word solely in the exception provision of the CALEA has created considerable dubiety in the courts concerning the appropriate application of the exception to cell site location information.”).

<sup>252</sup> *See FISHMAN & MCKENNA*, *supra* note 9, at 152.

obtain real-time cell site tracking data without resort to a probable cause warrant.<sup>253</sup> A dozen courts have analyzed hybrid arguments, and more than half have rejected them.<sup>254</sup> Those courts that have rejected the hybrid argument and denied access to cell site data under a Pen/Trap-SCA combination have done so based on the plain language of CALEA's exception clause, and on legislative history. For example, one court reasoned that if the legislature "intended to allow prospective cell site information to be obtained by means of the combined authority of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the statutes themselves. Indeed . . . the legislative history of CALEA would suggest Congress's intent to be otherwise."<sup>255</sup> While some courts have accepted hybrid arguments, the prior examination of the flaws inherent in both the Pen/Trap Statute argument<sup>256</sup> and the SCA argument<sup>257</sup> should make clear that such a hybrid argument suffers the same deficiencies.

### C. Cell Site Data Must Be Classified as Data Obtained From a Tracking Device

After examining the accuracy of cellular locating techniques and their various uses, whether or not GPS-enabled cell phones are invasive of privacy, it is hard to escape the conclusion that real-time cell site data falls squarely within the ambit of tracking device information under the ECPA.<sup>258</sup> Of the three sections of the ECPA arguably applicable to cell phone tracking methods, the tracking device category provides the best fit.<sup>259</sup> Defined as "an electronic or

---

<sup>253</sup> *Id.*

<sup>254</sup> See, e.g., *Indiana Pen/Trap Case*, *supra* note 251, at \*4; *In re Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, No. 06 Crim. Misc. 01., 2006 WL 468300, at \*1 (S.D.N.Y. Feb. 28, 2006); *Maryland Pen/Trap Case*, *supra* note 134; *In re the Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification No. (585) 111-1111 and the Disclosure of Subscriber and Activity Info. under 18 U.S.C. § 2703*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *Wisconsin Pen/Trap Case*, *supra* note 145; *In re the Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 132 (D. D.C. 2005); *In re an Application of the United States for an Order (1) Authorizing the Installation of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *Texas Pen/Trap Case*, *supra* note 10.

<sup>255</sup> *Wisconsin Pen/Trap Case*, *supra* note 145, at 958 (setting out the reasoning relied upon by many of the courts that have rejected the hybrid argument).

<sup>256</sup> See *supra* Part V.B.

<sup>257</sup> See *supra* Part V.A.

<sup>258</sup> *Texas Pen/Trap Case*, *supra* note 10, at 757.

<sup>259</sup> *Texas Pen/Trap Case*, *supra* note 10, at 753. The phrase "arguably applicable" is used here to denote the fact that the government has based arguments on these other sections of the ECPA. As previous sections have shown, however, logical and statutory flaws exist in

mechanical device which permits the tracking of the movement of a person or object,”<sup>260</sup> the term “tracking devices” is broad enough to encompass cell phones. Despite the breadth of the ECPA’s definition, some courts have held that a cell phone does not fit within its meaning, or was not contemplated under Congress’s statutory definition. For example, the U.S. District Court for the Eastern District of California determined that because cell phones could not be used as tracking devices when the ECPA was passed in 1986, Congress did not contemplate their inclusion within that term.<sup>261</sup>

This argument is improper. It limits law enforcement to using tracking devices that existed when the ECPA was passed in 1986, despite technical and technological advancements. Although the exact form of future tracking advancements was not contemplated, the potential for advancements forced Congress to leave the statute broad.<sup>262</sup> Far from excluding new technologies, the sheer breadth of the definition indicates that Congress recognized that there could be unforeseeable advances.<sup>263</sup> Moreover, it is doubtful that, when used to track the location of a cellular subscriber, cell phones are so drastically different from the tracking devices that existed in 1986 or that exist now. Indeed, the information that can be gleaned from a traditional tracking device is not much different from that obtained from a cell phone through cell site data.<sup>264</sup> In some cases, the devices are so similar that they rely on the same cell towers for operation.<sup>265</sup> Still, the government has attempted to argue that cell phones are not tracking devices and therefore not subject to the higher probable cause burden concomitant with that classification.

Another government argument against classifying cell phones as tracking devices is that the location information derived from real-time cell site information is not sufficiently detailed to qualify the device as a tracking device.<sup>266</sup> Courts and commentators alike have rejected this argument.<sup>267</sup> First, the ECPA

---

these arguments. *See* discussion *supra* Parts V.A and V.B.

<sup>260</sup> 18 U.S.C. § 3117(b) (2000).

<sup>261</sup> *In re Application for an Order Authorizing the Extension and Use of a Pen Register Device*, No. 07-SW-034 GGH, 2007 WL 397129, at \*2 (E.D. Cal. Feb. 1, 2007) (“[O]ne must look at the meaning of electronic or mechanical device in 1986, the date of passage of § 3117(b), and the legislative history which indicates that the device contemplated was only of the ‘beeper’ variety.”).

<sup>262</sup> *See Texas Pen/Trap Case*, *supra* note 10, at 753–54 (“By adopting the broader language, Congress may simply have been anticipating future advances in tracking technology. Such advances have indeed come to pass.”).

<sup>263</sup> *Id.*

<sup>264</sup> *See id.* at 754 (“[T]he distinction between cell site data and information gathered by a tracking device has practically vanished.”).

<sup>265</sup> FISHMAN & MCKENNA, *supra* note 9, at 149.

<sup>266</sup> *Texas Pen/Trap Case*, *supra* note 10, at 755.

<sup>267</sup> *See, e.g., id.* at 751–52, 757; *see also* FISHMAN & MCKENNA, *supra* note 9, at 152

definition of tracking device does not include any accuracy requirements.<sup>268</sup> Additionally, the inclusion of GPS chips in cell phones has greatly increased the accuracy of location compared to network-based location technologies.<sup>269</sup> Despite government arguments to the contrary, “the ability to pinpoint in real time the location of a cell phone to within meters challenges the notion that the information is not ‘detailed.’”<sup>270</sup> Cell phone tracking creates the potential for a map detailing the movements of a cell user.<sup>271</sup> Such detailed accuracy is both required by the E-911 mandate<sup>272</sup> and available to private consumers using parental or employee tracking systems.<sup>273</sup> Faced with these counter-arguments, it seems an exercise in futility to argue that a cell phone does not fit the definition of a tracking device.<sup>274</sup> At least some courts have reached the same conclusion, and in so doing have required a probable cause warrant to authorize the use of a tracking device.<sup>275</sup>

In perhaps a final effort to obtain tracking information under some burden lower than probable cause, the government has argued that the Fourth Amendment does not apply because there is no reasonable expectation of privacy in cell site information.<sup>276</sup> This claim stems from the argument that, like the numbers dialed by a caller, there is no expectation of privacy in the location information transferred to the cell service provider.<sup>277</sup> The flaw in this contention is that, unlike the numbers dialed, cell site information is not voluntarily conveyed by the cellular user to the service provider.<sup>278</sup> Similarly, location information is unlike numbers dialed; while customers may reasonably

---

(“[T]he ability to pinpoint in real time the location of a cell phone to within meters challenges the notion that the information is not ‘detailed.’”).

<sup>268</sup> 18 U.S.C. § 3117(b) (2000); see also *Texas Pen/Trap Case*, *supra* note 10, at 753.

<sup>269</sup> See discussion *supra* Part III.B. Indeed, as of May 2000, the government ended Selective Availability, the intentional degradation of GPS signals available to commercial GPS devices. President Clinton stated that “[t]his will mean that civilian users of GPS will be able to pinpoint locations up to ten times more accurately” than when Selective Availability was active. Press Release, The White House, Statement by the President Regarding the United States’ Decision to Stop Degrading Global Positioning System Accuracy (May 1, 2000), available at [http://www.navcen.uscg.gov/gps/selective\\_availability.htm](http://www.navcen.uscg.gov/gps/selective_availability.htm).

<sup>270</sup> FISHMAN & MCKENNA, *supra* note 9, at 152.

<sup>271</sup> Lockwood, *supra* note 151, at 312.

<sup>272</sup> See 47 C.F.R. § 20.18(h) (2006); see also *supra* Part III.B.

<sup>273</sup> See *supra* discussion Part II.C.

<sup>274</sup> See FISHMAN & MCKENNA, *supra* note 9, at 152 (“[T]he ECPA so broadly defines what a ‘tracking device’ is that it must be hard for the Assistant United States Attorney to argue with a straight face that a cell phone does not meet that broad definition.”)

<sup>275</sup> See, e.g., *Texas Pen/Trap Case*, *supra* note 10, at 751–52, 757.

<sup>276</sup> *Id.* at 756.

<sup>277</sup> The Supreme Court in *Smith* rejected the contention that an expectation of privacy exists in the numbers dialed on a phone. *Smith v. Maryland*, 442 U.S. 735, 742–43 (1979); see also discussion *supra* Part IV.A.

<sup>278</sup> *Texas Pen/Trap Case*, *supra* note 10, at 756–57.

expect service providers to collect the numbers they dial for billing and fraud prevention,<sup>279</sup> customers would have no reason to think that a phone company might collect information on their locations. On the contrary, customers have a reasonable expectation of privacy regarding their location information. However, cell service providers not only possess the technological capabilities to collect this information, but they are required by law to do so, and to a high degree of accuracy, under the E-911 program.<sup>280</sup> To call such a transmittal of information voluntary is to leave the would-be cell subscriber with a Hobson's choice: use a cell phone that is easily tracked by the government, or use none at all.<sup>281</sup> Inherent in the E-911 program is the recognition by the government of the importance of having a cell phone in case of emergency.<sup>282</sup> Given this recognized importance, it is crucial that the government protect location information rather than force cell subscribers to reject cell phones altogether in favor of privacy interests.

#### D. Trends Toward Protectionism by Requiring Probable Cause

With a handful of outliers, the courts that have been asked to grant cell site information have thus far demonstrated an inclination to protect privacy. That is, most courts have required the government to demonstrate probable cause before issuing a warrant for such cell site data. These courts have preferred to

---

<sup>279</sup> *Smith*, 442 U.S. at 742.

<sup>280</sup> 47 C.F.R. § 20.18 (2006). While it is true that cellular service providers may collect information on the locations of calls placed by customers for purposes of charging roaming fees, such customers reasonably expect that information to be used only for billing purposes. Justice Marshall in *Smith v. Maryland*, stated in his dissent that:

[E]ven assuming, as I do not, that individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular. . . . Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.

*Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (citation omitted).

<sup>281</sup> A Hobson's Choice is an apparently free choice that in reality leaves no choice whatsoever. The phrase derives from a 17th-century liveryman who required his customers to take either the horse nearest the stable door, or no horse at all. Merriam-Webster Online Dictionary, <http://www.m-w.com/dictionary/hobson's+choice> (last visited Nov. 7, 2007). Justice Marshall recognized this paradox writing that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Smith*, 442 U.S. at 750 (Marshall, J., dissenting) (citations omitted).

<sup>282</sup> FCC, FCC CONSUMER FACTS: WIRELESS 911 SERVICES (2006), <http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.pdf>.

err on the side of caution. They reasoned that the high standard of probable cause also grants access to the information if in truth it could have been obtained under a lower standard.<sup>283</sup> Although each section of the ECPA calls for a different standard, from the Pen/Trap Statute's relevance requirement up to the probable cause requirement of tracking devices,<sup>284</sup> "[o]ne feature of ECPA is that through use of greater legal process officials can gain access to any information that they could obtain with lesser process."<sup>285</sup>

## VI. CONCLUSION: THE CASE FOR LEGISLATIVE CLARIFICATION

While most courts have denied the government access to cell site data absent a probable cause warrant, a few have granted it with mere proof of relevance under the Pen/Trap Statute, the SCA, or a combination thereof. Such conflicting decisions leave both cellular users and law enforcement officers in the lurch, unsure of how any particular decision will come down the next time around. Such fact-specific decisions "seem to struggle to make statutes apply where they should not and only create a judicial headache with unwieldy results lacking in uniform consensus."<sup>286</sup>

As compared to cell site data obtained through tower triangulation, the integration of GPS technology to cell phones greatly improves the accuracy with which a phone and its user can be tracked. Notoriously slow to evolve, the common law lags far behind such technological evolution. Before courts have figured out how to treat one piece of technology, it becomes obsolete and is replaced by the next generation of stronger, faster, better machinery. In this case, courts have yet to find a consensus approach to cell site data, and already its more accurate GPS analogue has flooded the market. As this technology becomes ubiquitous and inevitably evolves and improves, it is crucial that Congress step in to clarify how it should be treated by the judicial system.<sup>287</sup> Congress must pass legislation carefully crafted to serve the dual purpose of

---

<sup>283</sup> See, e.g., *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Information*, No. 06-MISC-004, 2006 WL 2871743, at \*4 (E.D. Wis. 2006).

<sup>284</sup> And beyond that high burden to the so-called "super-warrant" showing required for wiretapping. *Id.* at \*1-2.

<sup>285</sup> JAMES G. CARR & PATRICIA L. BELLIA, *LAW OF ELECTRONIC SURVEILLANCE* § 4:77, at 4-193 (2006).

<sup>286</sup> FISHMAN & MCKENNA, *supra* note 9, at 154.

<sup>287</sup> See *Talk of the Nation: Surveillance via Cell Phone*, *supra* note 12 (interview of Professor Clifford Fishman) ("[T]he fact that judges are beginning to look at this issue critically is useful, it's good. I think the legislature, ultimately, is the body that should make these very nuanced policy judgments and decisions, but in the absence of legislative action the courts understandably feel compelled to step in.")

clarifying the judicial treatment that should be applied to presently existing technology, while also providing a clear guideline for the treatment of future technological advances.

However, cellular tracking technology is evolving at a pace far outmatching the speed at which congressional legislation can be enacted. Laws governing such technology are, if not out-of-date by the time they are drafted, very nearly so by the time they are enacted. Vagueness is a necessary and inevitable evil in such legislation, built in to compensate the lag time between technological innovation and congressional legislation. The vagueness that is necessary and beneficial in legislating about technology has left unanswered questions which the judiciary has proven unable to answer. Indeed, as one scholar has stated:

[T]he time is well past that Congress should have taken another good, hard look at the entire issue of surveillance technology, both in terms of when the government can use it and also in terms of when private industry should be allowed to use surveillance technology information. Congress has a wide range of priorities, obviously, but this one ought to be fairly high.<sup>288</sup>

The use of the Global Positioning System to locate cell phones is the latest, but certainly not the last, improvement in tracking technologies. Enacted in 1986, the ECPA is quite simply out of touch with the realities of today's technology. Some commentators have argued that the statutory scheme already in place for cellular location technology and cell phone tracking is clear.<sup>289</sup> Thus, one might expect the judiciary to reach the same conclusion time and again, yet they have not. The arguments presented herein and those made by scholars and judges necessitate the conclusion that proof of probable cause is required to obtain access to tracking data derived from cell phones. It is imperative that Congress legislatively mandate such requirements. The interests of uniformity, judicial efficiency and, greatest of all, privacy protection, demand such Congressional action.

---

<sup>288</sup> *Id.* Another commentator expressed his cynicism about the potential for misuse of GPS-enabled cellular tracking technology and the likelihood of the Congressional clarification called for herein:

My solution is a simple one. It's called the Off switch—the antidote to any new technology that threatens our life, liberty, or pursuit of happiness. . . . Of course, we could also use a formal law that expressly forbids GPS tracking without a warrant, but these days, I have more faith in engineers than in Congress.

Costa, *supra* note 68.

<sup>289</sup> *See, e.g.*, FISHMAN & MCKENNA, *supra* note 9, at 153–54.

