# Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices.

# JOSHUA A. ENGEL\*

Introduction 1 I. II. A. Expectation of Privacy in Cell Phones......5 2. The Reach of the Container Doctrine and Application to III. B. Legal Analysis......31 SIMILAR TENSION AS COURTS ATTEMPT TO EXTEND TRADITIONAL TRACKING DEVICE THE FUTURE OF SEARCHES OF SMART PHONES AND OTHER SOPHISTICATED V. CONCLUSION 62 VI.

#### I. Introduction

In December 2009, an Ohio Supreme Court ruling about cell phones seemed to strike a popular nerve. In *State v. Smith*,<sup>1</sup> the court held that even if a cell phone is lawfully seized incident to arrest, the Fourth Amendment generally prohibits the police from searching the contents of the cell phone without a warrant.<sup>2</sup> This opinion received tremendous positive coverage in the media both locally and nationally, indicating that the public viewed the

<sup>\*</sup> J.D., cum laude, Harvard University Law School, 1995, B.A., magna cum laude, University of Pennsylvania, 1992. The author is former Chief Legal Counsel, Ohio Department of Public Safety. This paper was not prepared in the author's official capacity as counsel for the Ohio Department of Public Safety. Accordingly, any views expressed in this paper are the views of the author only and do not necessarily reflect the views of the State of Ohio or the Ohio Department of Public Safety.

<sup>1. 920</sup> N.E.2d 949 (2009), cert. denied, No. 09-1377, 2010 WL 1922721 (Oct. 4, 2010).

<sup>2.</sup> *Id.* at 956 ("We hold that the warrantless search of data within a cell phone seized incident to a lawful arrest is prohibited by the Fourth Amendment when the search is unnecessary for the safety of lawenforcement officers and there are no exigent circumstances.").

Dayton Daily News editorial, "Your Cell Phone Should Be Private," stated, "The Ohio court does point police in the right direction. As more phones become more like computers, getting a warrant should be required." The Akron (OH) Beacon Journal similarly praised the decision, "The Ohio Supreme Court ventured into new territory and delivered a sound result." The national media also favorably covered the decision. For example, a New York Times editorial stated, "The Ohio Supreme Court has struck an important blow for privacy rights."

The *Smith* opinion is remarkable because it departed from long-standing precedent that a search incident to arrest includes the ability to search the contents of any container found on the person.<sup>6</sup> A search incident to arrest is a traditional exception to the warrant requirement of the Fourth Amendment.<sup>7</sup> During this search, law enforcement is permitted to search the person and the immediately surrounding area for weapons and evidence.<sup>8</sup> Such searches were justified on the grounds that persons under arrest might possess a weapon to aid in an escape or may destroy or conceal evidence of their crimes.<sup>9</sup>

3. Op-Ed, Your Cell Phone Should Be Private, DAYTON DAILY NEWS, Dec. 24, 2009, at A12

4. Op-Ed, Our Opinion: Expecttaion of Privacy, AKRON BEACON JOURNAL (OH), Dec. 18, 2009, at A10.

5. Editorial, Cellphone Searches, N.Y. TIMES, Dec. 26, 2009, New York Edition, at A22.

6. See. e.g., United States v. Robinson, 414 U.S. 218, 235 (1973) (upholding search of contents of box of cigarettes); see also 3 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 5.2(c), at 110 (4th ed. 2004) (stating that in applying *Robinson*, the lower courts "have deemed evidentiary searches of an arrested person to be virtually unlimited").

7. See, e.g., Draper v. United States, 358 U.S. 307 (1959). It is not unusual for police to obtain warrants prior to searching cell phones. See Jackson v. Kelly, No. 4:09 CV 1185, 2010 WL 1913384, at \*3 (N.D. Ohio May 12, 2010); United States v. Reynolds, No. 3:08-CR-143, 2009 WL 1588413, at \*2 (E.D. Tenn. June 4, 2009).

8. See, e.g., Preston v. United States, 376 U.S. 364, 367 (1964).

9. Chimel v. California, 395 U.S. 752, 763 (1969).

Courts have historically imposed very few restrictions on the ability of law enforcement to search the contents of containers found on an arrestee, <sup>10</sup> even when the container is locked (the "container doctrine"). <sup>11</sup> When conducting a search incident to arrest, law enforcement has been permitted to open and review documentary materials found in containers such as address books <sup>12</sup> and diaries. <sup>13</sup> More recently, courts have refused to limit the ability of law enforcement during a search incident to arrest to review the contents of electronic devices, such as pagers, by viewing these electronic items as containers. <sup>14</sup> Federal courts have extended this analysis to include the contents of cell phones <sup>15</sup>

In rejecting the application of the container doctrine to cell phones, the Ohio Supreme Court reasoned that closed containers "have traditionally been physical objects capable of holding other physical objects." The court concluded that a cell phone is different from traditional containers because "even the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container." The Ohio Supreme Court is the first court to recognize that the technological

<sup>10.</sup> United States v. Donnes, 947 F.2d 1430, 1437 (10th Cir.1991) (recognizing that "a search incident to a lawful arrest permits a law enforcement officer to conduct a warrantless search of a container located in the area of the arrestee's immediate control").

<sup>11.</sup> United States v. Silva, 745 F.2d 840, 847 (4th Cir.1984) (upholding search incident to arrest where officer removed a key from the arrestee's pocket and unlocked a bag sitting next to the arrestee).

<sup>12.</sup> See, e.g., United State v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993).

<sup>13.</sup> United States v. Frankenberry, 387 F.2d 337, 339 (2nd Cir. 1967).

<sup>14.</sup> *See* United States v. Chan. 830 F.Supp. 531, 535–36 (N.D. Cal. 1993) (finding warrantless search of pager memory comparable to a search of container contents).

<sup>15.</sup> *See* United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007) (finding warrantless search of cell phone memory comparable to a search of container contents).

<sup>16.</sup> State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009).

<sup>17.</sup> *Id*.

sophistication and nature of modern cell phones has created a heightened expectation of privacy that renders previous doctrinal interpretations, like the container doctrine, obsolete. This result was not unpredictable. Some commentators have criticized the application of traditional Fourth Amendment doctrines to searches of sophisticated modern devices, such as smart cell phones, that hold the ability to reveal significant intimate details about the possessor. And at least one court has noted that "one might speculate whether the Supreme Court would treat laptop computers, hard drives . . . or even cell phones as it has a briefcase or give those types of devices preferred status because of their unique ability to hold vast amounts of . . . personal information."

This Article explains why the Ohio Supreme Court decision signals a growing recognition by courts to treat the difference or similarity between cell phones and containers as one of kind, not one of degree,<sup>20</sup> and examines the application of this analysis to other emerging technologies. Part II describes the doctrinal history of the container doctrine and its application to electronic devices, including cell phones. Part III discusses the *Smith* decision and its possible implication for future decisions. Part IV examines how another traditional Fourth Amendment doctrine, the *Knotts* doctrine, is unable to account for the invasion of privacy imposed by another sophisticated electronic device, GPS tracking. Finally, Part V attempts to provide a new

<sup>18.</sup> See, e.g., Adam M. Gershowitz, The iPhone Meets the Fourth Amendment, 56 UCLA L. REV. 27 (2008); Bryan Andrew Stillwagon, Bringing an End to Warrantless Cell Phone Searches, 42 GA. L. REV. 1165 (2008). These commentators have predicted that the U.S. Supreme Court is unlikely to adopt different rules for new technologies. Professor Gershowitz wrote, for example: "current Fourth Amendment doctrine strongly suggests that the Supreme Could would authorize invasive searches of the [cell phones] found in pockets or purses of arrested individuals." Gershowitz, supra, at 30.

<sup>19.</sup> United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009) ("Interesting as this issue may be, we need not now resolve it . . . .").

<sup>20.</sup> Cf. Burson v. Freeman, 504 U.S. 191, 209–10 (1992) (noting that a geographic restriction on political speech, if extended too far, may become a difference of "constitutional dimension"); Miller v. United States, 356 F.2d 63, 67 (5th Cir. 1966), cert denied, 384 U.S. 912 (1966) ("It is of continuing importance to take note of the fact that differences of kind and degree are crucial when constitutional principles are at stake.").

framework for sophisticated electronic devices that may defy traditional doctrinal analysis. Under this new approach, certain information stored on electronic devices would not be subject to the container doctrine. Rather than examining the particular capabilities of an electronic device, courts should determine whether the information that would be disclosed is the type of information that would reasonably lead to the disclosure of personal information typically covered by the right of informational privacy.

#### II. THE CONTAINER DOCTRINE AND ELECTRONIC DEVICES

The Supreme Court has not directly considered whether a search incident to arrest may include a search of a cell phone's contents and, if it does, the thoroughness of such a search. The extent to which the Fourth Amendment provides protection for the contents of electronic communications and images stored on a cell phone in a search incident to arrest remains an open question.

# A. Expectation of Privacy in Cell Phones

The Fourth Amendment states the following:

The 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.<sup>21</sup>

A search is deemed to have occurred "when an expectation of privacy that society is prepared to consider reasonable is infringed." In *Katz v. United States*, <sup>23</sup> Justice Harlan famously explained that the relevant inquiry under the Fourth Amendment has two parts: first, whether the

<sup>21.</sup> U.S. CONST. amend. IV.

<sup>22.</sup> United States v. Jacobsen, 466 U.S. 109, 113 (1984). A seizure occurs when there is some meaningful interference with an individual's possessory interests in that property. *Id.* 

<sup>23. 389</sup> U.S. 347 (1967).

person had "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable."<sup>24</sup>

The United States Supreme Court has been reluctant to determine the exact contours of the reasonable expectation of privacy in the face of new technology.<sup>25</sup> The closest the Court has come to addressing the reasonable expectation of privacy in cell phones was in a recent decision where the Court considered whether an employee has a reasonable expectation of privacy in personal text messages sent on an employer-owned pager.<sup>26</sup> The Court assumed, without deciding, that the employee did have an expectation of privacy.<sup>27</sup> In doing so, the Court cautioned that the "judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."<sup>28</sup> Significantly, nothing in this opinion suggests that the Court would look unfavorably on the suggestion that there is both a subjective and reasonable expectation of privacy in the contents of other sophisticated electronic devices, such as smart cell phones.

There is little disputing that a person has a subjective expectation of privacy in the contents of his or her cell phone.<sup>29</sup> The Fifth Circuit has noted, for example, that "cell phones contain a wealth of private information, including emails, text messages, call histories, address books, and subscriber numbers" and that, as a result, people have a "reasonable expectation of

<sup>24.</sup> *Id.* at 361 (1967) (Harlan, J., concurring).

<sup>25.</sup> A notable exception is possibly the use by law enforcement of a new technology in *Kyllo*. *See* discussion *infra* note 260.

<sup>26.</sup> City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010).

<sup>27.</sup> *Id.* at 2629.

<sup>28.</sup> *Id.* This observation was complicated by the fact that a government employer owned the pager in question.

<sup>29.</sup> *See, e.g.*, United States v. Finley, 477 F.3d 250, 259–60 (5th Cir. 2007); United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. 2009).

privacy regarding this information."<sup>30</sup> For a similar reason, another federal court observed that it "seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone."<sup>31</sup> This satisfies the first prong of the *Katz* test.

There is a dispute, however, about the second part of the *Katz* test. The starting point for an examination whether the expectation of privacy in information on cell phones is reasonable is the decision of the United States Supreme Court in *Smith v. Maryland*.<sup>32</sup> In *Smith v. Maryland*, the Court held that there is no reasonable expectation of privacy in numbers called by, or numbers calling, a private phone.<sup>33</sup> Specifically, the Court considered whether the installation of a pen register to record the phone numbers that have been dialed from a land line violated the Fourth Amendment.<sup>34</sup> The Court reasoned that people in general do not have any actual expectation of privacy in the numbers they dial, partially because the phone company maintains records of the numbers they dial.<sup>35</sup> The Court said that telephone users

[T]ypically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under

<sup>30.</sup> United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008). In order to maintain this expectation of privacy, cell phone owners must take steps to safeguard the information. In a recent § 1983 case, the court concluded that an owner did not have a reasonable expectation of privacy in the images on a cell phone because she lent the phone to another person for almost two months. Casella v. Borders, 649 F. Supp. 2d 435, 439 (W.D. Va. 2009). The court noted that the owner failed to take any protective measures "to secure the privacy of the images on the phone, such as password-protecting access to the phone's information" or otherwise exclude others from accessing the cell phone. *Id.* 

<sup>31.</sup> United States v. Wurie, 612 F. Supp. 2d 104, 109 (D. Mass. 2009).

<sup>32. 442</sup> U.S. 735 (1979).

<sup>33.</sup> *Id.* at 742.

<sup>34.</sup> *Id.* at 741–42.

<sup>35.</sup> *Id.* at 742.

these circumstances, harbor any general expectation that the numbers they dial will remain secret.<sup>36</sup>

Several courts have relied on *Smith v. Maryland* to hold that a person does not have a reasonable expectation of privacy in the records of incoming and outgoing calls contained on a cell phone.<sup>37</sup> One court stated, "[w]here a defendant fails to show . . . that the numbers searched disclosed more than the 'addressing information' that would be revealed by a pen register, his claim of an unreasonable search fails."<sup>38</sup>

A number of differences between a pen register and cell phone call records are significant, however, and likely limit the application of *Smith v. Maryland* to cell phone searches. In *Smith v. Maryland*, the Court noted that a pen register cannot determine whether a call has been completed.<sup>39</sup> The Court justified its holding in part on the observation that "a law enforcement official could not even determine from the use of a pen register whether a communication existed." In contrast, cell phone call records and address book records

<sup>36.</sup> *Id.* The doctrine can be summarized as follows: "[W]hen a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities." S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984). In other decisions, the Court held that individuals have no legitimate expectation of privacy in checks, financial statements, and deposit slips subpoenaed from an individual's bank by the government, even where the individual was given no notice of the subpoenas. United States v. Miller, 425 U.S. 435, 442–43 & 443 n.5 (1976).

<sup>37.</sup> *See*, *e.g.*, United States v. Maldonado, No. 09-40031-01/02-SAC, 2009 WL 2760798 (D. Kan. Aug. 26, 2009); United States v. Fierros-Alavarez, 547 F. Supp. 2d 1206, 121011 (D. Kan. 2008).

<sup>38.</sup> *Maldonado*, 2009 WL 2760798, at \*12. Some cell phone companies do not maintain such records, or may choose not to retain such records in the future. The use of disposable phones to frustrate attempts at record keeping further complicates this analysis. *See, e.g.*, Eric Zeman, *Could Virgin Mobile Have Saved Eliot Spitzer?*, INFORMATION WEEK (Mar. 14, 2008, 9:23 AM), http://www.informationweek.com/blog/main/archives/2008/03/could\_virgin\_mo.html (noting that that a person can obtain a prepaid phone for cash and leave few records to trace). For example, the HBO TV show *The Wire* showed drug dealers attempting to evade police surveillance by using disposable phones. *See generally* Thomas Rogers, *What Faisal Shahzad Could Learn From "The Wire"*, SALON (May 4, 2010, 7:01 PM) http://www.salon.com/books/int/2010/05/04/disposable\_phones.

<sup>39. 442</sup> U.S. at 741.

typically reveal not only whether a call was completed, but also the length of any communication and the identity of the other person. *Smith v. Maryland* also has no application on the content of text messages, e-mails, photographs, and other information commonly retained on cell phones but not shared with the cell phone provider. For these reasons, people likely have a greater and more reasonable expectation of privacy in the calling records maintained in their cell phones than a landline telephone user had in a pen register.<sup>41</sup>

#### B. Searches of Containers Incident to Arrest

# 1. Origin of the Container Doctrine

The Supreme Court has held that warrantless searches of an arrestee's person, including personal property contained in the arrestee's pockets and any containers in the arrestee's possession, do not violate the Fourth Amendment.<sup>42</sup> This is the search incident to arrest exception to the Fourth Amendment warrant requirement. The origin of the search incident to arrest exception is *Chimel v. California*.<sup>43</sup>

In *Chimel*, police officers arrived at the home of the defendant with an arrest warrant.<sup>44</sup> The defendant's wife permitted the officers to enter the home.<sup>45</sup> After the defendant returned home, the police arrested him and began a search

<sup>40.</sup> *Id.* (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)). *Smith v. Maryland* also has no application on the content of text messages, e-mails, photographs, and other information commonly retained on cell phones.

<sup>41.</sup> This expectation is bolstered by cell phone company privacy policies that restrict the situations in which such information may be revealed. *See, e.g., Verizon Privacy Policy,* VERIZON, http://www22.verizon.com/about/privacy/policy/ (last updated July, 2010).

<sup>42.</sup> See generally United States v. Robinson, 414 U.S. 218 (1973).

<sup>43. 395</sup> U.S. 752 (1969).

<sup>44.</sup> *Id.* at 753.

<sup>45.</sup> *Id*.

through the entire three-bedroom house, including the attic, the garage, and a small workshop. In some rooms the search was relatively cursory. In the master bedroom and sewing room, however, the officers directed the petitioner's wife to open drawers and 'to physically move contents of the drawers from side to side so that (they) might view any items that would have come from (the) burglary.<sup>46</sup>

The court held that the search, including the search of closed drawers, was overly broad.<sup>47</sup> The court then explained the limit of search incident to arrest exception:

When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidentiary items must, of course, be governed by a like rule. 48

*Chimel* thus established that a search incident to arrest must be justified either by officer safety concerns or by a need to preserve evidence.<sup>49</sup>

Following *Chimel*, the Court in *United States v. Robinson*<sup>50</sup> permitted the search of a "crumpled up cigarette package" in the defendant's possession incident to arrest.<sup>51</sup> This is the genesis of the container doctrine. Notably, the *Robinson* decision lacks an extensive discussion of the scope of the search of containers found on an arrestee.<sup>52</sup> Instead, the Court examined only

48. *Id.* at 762–63.

51. *Id.* at 223. Heroin was found in the cigarette package. *See id.* 

<sup>46.</sup> *Id.* at 753 (citations omitted).

<sup>47.</sup> *Id.* at 763.

<sup>49.</sup> This justification does not need to be present in every case but is based on generalizations about conditions. *See infra* notes 64 through 66 and accompanying text.

<sup>50. 414</sup> U.S. 218 (1973).

<sup>52.</sup> See id. at 255–56 (Marshall, J., dissenting). ("The majority opinion fails to recognize that the search... did not merely involve a search of respondent's person. It also included a separate search of effects found on his person. And even were we to assume, arguendo, that it was reasonable for [the officer] to remove the object

whether, following an arrest, "a full search of the person" was permitted.<sup>53</sup> Nonetheless, courts have relied on *Robinson* for the broader proposition that police may search the contents of any container found on a person.<sup>54</sup>

The Supreme Court's first substantive discussion of the container doctrine appears in *New York v. Belton.*<sup>55</sup> In *Belton*, the Court held that in the case of a full custodial arrest of an occupant or "recent occupant" of a vehicle, the police may search the passenger compartment of the vehicle as "a contemporaneous incident of that arrest." The Court concluded that such a search to ensure safety and to preserve evidence is "reasonable" under the Fourth Amendment. In expanding the search incident to arrest doctrine to include the passenger compartment of a vehicle operated by the arrestee, the *Belton* Court also permitted the search of any closed containers within the vehicle. The Court explained that containers may be searched whether they are "open or closed, since the justification for the search is not that the arrestee has no privacy interest in the container, but that the lawful custodial arrest justifies the infringement of

he felt in respondent's pocket, clearly there was no justification consistent with the Fourth Amendment which would authorize his opening the package and looking inside.").

- 55. 453 U.S. 454 (1981).
- 56. *Id.* at 460.

<sup>53.</sup> *Id.* at 235 (majority opinion) ("It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment.").

<sup>54.</sup> *See*, *e.g.*, United States v. Johnson, 846 F.2d 279, 281–82 (5th Cir. 1988) (per curiam); United States v. Benson, 631 F.2d 1336, 1341 (8th Cir. 1980); United States v. Xiarhos, 820 F. Supp. 634, 636 (D. Mass. 1993).

<sup>57.</sup> *Id.* at 459–61 (quoting United States v. Robinson, 414 U.S. 218, 235 (1973)); *see also* Thornton v. United States, 541 U.S. 615, 623 (2004) (permitting search of interior of vehicle even when occupant is outside of vehicle when placed under arrest). *Thornton* may no longer be good law following Arizona v. Gant, 129 S. Ct. 1710 (2009). *See infra* notes 67 through 70 and accompanying text.

<sup>58. 453</sup> U.S. at 460. In its attempt to craft a "workable rule," the Court assumed "that articles inside the relatively narrow compass of the passenger compartment of an automobile are in fact generally, even if not inevitably, within" the reach of an arrestee. *Id.* (quoting Chimel v. California, 395 U.S. 752, 763 (1969)).

any privacy interest the arrestee may have."<sup>59</sup> In a later decision, *United States v. Chadwick*,<sup>60</sup> the Court defined the outer limit of the container doctrine, holding that a warrant was required before the police could open a container found in the trunk of a car.<sup>61</sup>

In a footnote, the *Belton* Court defined a container as "any object capable of holding another object. It thus includes closed or open glove compartments, consoles, or other receptacles . . . as well as luggage, boxes, bags, clothing, and the like." There are no federal decisions discussing the meaning of this term beyond the definition provided by the Court. Instead, courts have tended to focus on whether locked or unlocked containers may be opened and examined.

Significantly, *Belton* and *Robinson* rely on the premise that, while the authority to search an arrestee following a lawful custodial arrest is premised upon concerns for officer safety and the preservation of evidence, an officer is not required to establish an actual belief that a weapon or evidence exists to justify the search.<sup>64</sup> The *Belton* Court sought to avoid litigation "in each

<sup>59.</sup> *Id.* at 461.

<sup>60. 433</sup> U.S. 1 (1977)

<sup>61.</sup> *Id.* at 15–16 (1977). In *Chadwick*, agents seized a footlocker from the trunk of the defendants' car, and searched the footlocker later while it was safely in custody at the Federal Building. *Id.* at 1. Supreme Court held invalid the subsequent warrantless search. *Id.* at 15–16. The container doctrine may appear to be somewhat limited by *Chadwick*. However, the *Chadwick* court expressly excluded "searches of the person" of the accused, as in *Robinson*.

<sup>62. 453</sup> U.S. at 461 n.4.

<sup>63.</sup> For example, federal circuit courts of appeal have held that the *Belton* rule allows a search of a locked glove box. *See* United States v. Nichols, 512 F.3d 789 (6th Cir. 2008); United States v. Gonzalez, 71 F.3d 819 (11th Cir. 1996); United States v. Woody, 55 F.3d 1257 (7th Cir. 1995); United States v. McCrady, 774 F.2d 868 (8th Cir. 1985).

<sup>64.</sup> See United States v. Robinson, 414 U.S. 218, 235 (1973) (noting that authority to conduct a search incident to arrest "does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect"); cf. Illinois v. Lafayette, 462 U.S. 640, 646 (1983) ("Examining all the items removed from the arrestee's person or possession and listing or inventorying them is an entirely reasonable administrative procedure. It is immaterial whether the police actually

case the issue of whether or not one of the reasons supporting a search incident to arrest was present in favor of establishing a "workable rule." The Court further explained that this rule permitted the search of containers that may "be such that they could hold neither a weapon nor evidence of the criminal conduct for which the suspect was arrested."

The Court recently reexamined, reaffirmed, and modified the search incident to arrest doctrine recently in *Arizona v. Gant.*<sup>67</sup> In *Gant*, the Court reconsidered the scope of a search of a vehicle incident to arrest and limited its prior holding in *Belton.*<sup>68</sup> The *Gant* Court explained that under *Chimel*, police may search incident to arrest only the space within an arrestee's "immediate control," meaning "the area from within which [the arrestee] might gain possession of a weapon or destructible evidence." In reviewing the scope of a search incident to arrest, the *Gant* Court further explained that if the general "justifications for the search-incident-to-arrest exception are absent . . . the rule does not apply." The *Gant* decision does not affect the

fear any particular package or container; the need to protect against such risks arises independent of a particular officer's subjective concerns.").

#### 67. 129 S. Ct. 1710 (2009).

<sup>65.</sup> *Belton*, 453 U.S. at 459–60 (quoting *Robinson*, 414 U.S. at 235). There is also a suggestion that a search incident to arrest is reasonable under the Fourth Amendment because the privacy interest protected by that constitutional guarantee is diminished abated by the fact of arrest. *Robinson*, 414 U.S. at 237–38 (Powell, J., concurring).

<sup>66. 453</sup> U.S. at 461. The Court explained that "A custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to the arrest requires no additional justification." *Id.* (quoting *Robinson*, 414 U.S. at 235).

<sup>68.</sup> *Id.* at 1719. The *Belton* decision acknowledged that the rule represented a "generalization" in order to establish a "workable rule this category of cases requires." 453 U.S. at 460; *see Gant*, 129 S. Ct. at 1727 (Alito, J., dissenting).

<sup>69. 129</sup> S.Ct. at 1716 (majority opinion). The Court explained that a search incident to arrest must be "commensurate with its purposes of protecting arresting officers and safeguarding any evidence of the offense of arrest that an arrestee might conceal or destroy." *Id.* 

<sup>70.</sup> *Id.* (citing Preston v. United States, 376 U.S. 364, 367–68 (1964)). This language does not suggest a move by the Court to requiring an individualized determination to justify each search incident to arrest.

container doctrine. The *Gant* court, however, did not limit the ability of law enforcement to open containers found within the scope of the search incident to arrest.<sup>71</sup>

# 2. The Reach of the Container Doctrine and Application to Electronic Devices Prior to Smart Cell Phones

Lower courts have interpreted the *Robinson-Belton* decisions to permit police to search personal objects—containers—found on a suspect incident to a lawful arrest. For example, many courts have upheld the search of a defendant's wallet under this exception.<sup>72</sup> Courts have applied the same rule to purses.<sup>73</sup> Additionally, courts have permitted searches on closed and locked containers, such as briefcases, found on or near a person.<sup>74</sup> Courts have also interpreted a permissible search of a container to include the contents of an address book.<sup>75</sup>

<sup>71.</sup> *Cf.* United States v. Shakir, 610 F.3d 315, 320 (3d Cir. 2010) ("To hold that a container search incident to arrest may not occur once the suspect is under the control of the police, but before he has been moved away from the item to be searched, would eviscerate this portion of *Chimel. Gant* did not purport to do any such thing.").

<sup>72.</sup> See, e.g., United States v. McCroy, 102 F.3d 239, 240–41 (6th Cir. 1996), cert. denied, 520 U.S. 1180 (1997) (upholding inventory search of defendant's wallet while he was held in temporary detention and seizure of pawn ticket which led to stolen rifles); United States v. Molinaro, 877 F.2d 1341, 1346–47 (7th Cir.1989) (upholding search of wallet); United States v. Castro, 596 F.2d 674, 677 (5th Cir. 1979), cert. denied, 444 U.S. 963 (1979) (unfolding and reading of paper found in defendant's wallet was valid search incident to his arrest); Evans v. Solomon, 681 F. Supp. 2d 233, 248 (E.D.N.Y. 2010) (reaching into arrestee's pocket to retrieve wallet and then remove identification "would comport with the Fourth Amendment as a search incident to arrest").

<sup>73.</sup> See, e.g., Curd v. City Ct. of Judsonia, Ark., 141 F.3d 839, 842 (8th Cir. 1998) (finding purse qualified as an object within arrestee's area of immediate control); United States v. Garcia, 605 F.2d 349, 355 (7th Cir. 1979) (discussing that a search of "a wallet, purse or shoulder bag" is permitted as a search incident to arrest); Donkers v. Camargo, No. 07 CR 11220, 2008 WL 2795960, at \*4 (E.D. Mich. July 18, 2008) (stating search of purse incident to arrest permissible to ensure that it did not contain any dangerous weapons).

<sup>74.</sup> See, e.g., United States v. Ivy, 973 F.2d 1184, 1187 (5th Cir. 1992) (finding search of a closed briefcase within the defendant's reach incident to an arrest is valid); United States v. Silva, 745 F.2d 840, 847 (4th Cir. 1984) (upholding search incident to arrest where officer removed a key from the arrestee's pocket and unlocked a bag sitting next to the arrestee).

<sup>75.</sup> See, e.g., United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993), cert. denied 510 U.S. 1029 (1993) (address book was lawfully seized from defendant's person as part of search incident to arrest); United States v. Holzman, 871 F.2d 1496, 1504 (9th Cir. 1989) (examination of address book permissible under *Belton* and *Robinson*).

Decisions of federal district courts and courts of appeals viewed earlier electronic devices, such as pagers, as containers that may be searched incident to arrest. For example, in *United States v. Chan*, <sup>76</sup> DEA agents seized a pager from the defendant at the time of arrest and searched the pager memory to retrieve telephone numbers. <sup>77</sup> The court, relying on *Belton*, held that the pager was a container that could be searched incident to arrest. <sup>78</sup> The court rejected an argument that a separate warrant was required prior to a search of the pager's memory because the pager was discovered on the arrestee's person. <sup>79</sup> The court reasoned, "the general requirement for a warrant prior to the search of a container does not apply when the container is seized incident to arrest." The court did not consider whether the electronic nature of the information contained in the pager distinguished the device from the type of objects described in *Robinson* or the *Belton* definition of a container.

Other courts have not hesitated to explicitly extend the wallet/address book line of cases to electronic devices such as pagers. For example, in *United States v. Lynch*, <sup>81</sup> Drug Enforcement agents arrested the defendant while the defendant was leaving a hotel room. <sup>82</sup> The agents seized a pager incident to arrest and obtained the numbers contained in the pager. <sup>83</sup> The court's analysis began with the observation that, under *Robinson*, a search incident to arrest of

<sup>76. 830</sup> F. Supp. 531 (N.D. Cal. 1993).

<sup>77.</sup> Id. at 533.

<sup>78.</sup> *Id.* at 535. The court rejected an argument that *Chadwick* was applicable because, in part, "the pager was the product of a search of [the defendant's] person, whereas the footlocker in *Chadwick* was obtained from the trunk of the defendant's car." *Id.* at 536; *see also* United States v. Robinson, 414 U.S. 218, 235 (1973).

<sup>79.</sup> *Id.* at 535–36

<sup>80.</sup> *Id.* at 536.

<sup>81. 908</sup> F. Supp. 284 (V.I. 1995).

<sup>82.</sup> *Id.* at 286.

<sup>83.</sup> *Id*.

the contents of a wallet or an address book is permissible.<sup>84</sup> The court extended the *Robinson* analysis to pagers, concluding:

The justification for allowing such searches is not that a person does not have an expectation of privacy in such personal effects such as a wallet or address book, but that once an arrest has been made, the privacy interests of the arrestee no longer take precedence over police interest in finding a weapon or obtaining evidence.

. . . .

. . . Just as police can lawfully search the contents of an arrestee's wallet or address book incident to an arrest, we hold that the agents here could lawfully search the contents of [the defendant's] pager incident to his arrest. 85

The conclusion the *Lynch* court reached is not unusual, and it does not appear that there are any contrary opinions in federal courts.<sup>86</sup>

The key to understanding these decisions is recognizing the courts' implicit assumption that the privacy interest in the electronic data held in pagers and similar electronic devices is the same as the privacy interest in non-electronic content such as address books. The arrestee's privacy interest is, in the view of these courts, outweighed by the law enforcement interests described in *Chimel* (officer safety and the preservation of evidence). In those situations where the courts consider the electronic data to be different, this difference has been used to justify, rather than limit, further police access to the information. The Seventh Circuit Court of Appeals,

<sup>84.</sup> *Id.* at 288.

<sup>85.</sup> *Id.* (citations omitted).

<sup>86.</sup> See e.g., United States v. Charles, 138 F.3d 257, 264 (6th Cir. 1998) (upholding a seizure of a pager found in an automobile in a search incident to the arrest of its occupant); United States v. Hunter, No. 96-4259, 1998 WL 887289, at \*3 (4th Cir. Oct. 29, 1998) (officers may retrieve telephone numbers from pager during search incident to arrest); United States v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996) (memory of pager seized incident to arrest could be accessed to obtain numbers and messages).

for example, applied the *Robinson-Belton* logic in *United States v. Ortiz.*<sup>87</sup> In *Ortiz*, officers searched the contents of a pager found in the front of the car the defendant was in when arrested.<sup>88</sup> The court noted that it agreed with the analysis of *Chan.*<sup>89</sup> The *Ortiz* court went a step further, however, and suggested that the electronic nature of the information created a relevant need to preserve evidence, akin to an exigent circumstance:

An officer's need to preserve evidence is an important law enforcement component of the rationale for permitting a search of a suspect incident to a valid arrest. Because of the finite nature of a pager's electronic memory, incoming pages may destroy currently stored telephone numbers in a pager's memory. The contents of some pagers also can be destroyed merely by turning off the power or touching a button. Thus, it is imperative that law enforcement officers have the authority to immediately "search" or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence. 90

Other courts have followed *Ortiz*, holding that the transient nature of information stored in pagers creates a circumstance justifying a search incident to arrest in order to preserve evidence. These courts, however, have continued to analyze the search of electronic devices under the *Robinson-Belton* search incident to arrest doctrine, and have not relied on a strict exigent circumstances justification. <sup>92</sup>

At the same time that courts permitted searches of electronic devices incident to arrest, courts started to limit searches of computers, recognizing that computers differed from traditional "containers." For example, in 1999, the Tenth Circuit reviewed the permissible

89. *Id.* at 984.

90. *Id.* (citations omitted).

91. See, e.g., Hunter, 1998 WL 887289, at \*3.

<sup>87. 84</sup> F.3d 977 (7th Cir. 1996).

<sup>88.</sup> *Id.* at 983.

<sup>92.</sup> See, e.g., id. ("[A]n arresting officer's need to preserve evidence. . . . is an important law enforcement component of the rationale for permitting a search of a suspect incident to a valid arrest.").

search of a lawfully seized computer in *United Sates v. Carey*. In *Carey*, the defendant was arrested for the possession and sale of cocaine. He consented to a search of his apartment for drug related items. The police seized two computers and obtained a warrant to search the machines for "evidence pertaining to the sale and distribution of controlled substances." While forensically reviewing the computer, the detective discovered images of child pornography. He detective discovered images of child pornography.

The government in *Carey* suggested that a computer is like a file cabinet—a form of container. <sup>98</sup> In order to search a file cabinet, it is necessary to open each file drawer, regardless of labels, in order to discover the contents. <sup>99</sup> The court rejected this metaphor, stating:

[B]ecause this case involves images stored in a computer, the file cabinet analogy may be inadequate. "Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information." Relying on analogies to closed containers or file cabinets may lead courts to "oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."

The court concluded that the detective should have held the computer and sought a more detailed search warrant when confronted with the documents. <sup>101</sup>

<sup>93. 172</sup> F.3d 1268 (10th Cir. 1999).

<sup>94.</sup> *Id.* at 1270.

<sup>95.</sup> *Id*.

<sup>96.</sup> *Id*.

<sup>97.</sup> *Id.* at 1271. The detective did not seek an additional search warrant for the child pornography images. *See id.* 

<sup>98.</sup> *Id.* at 1272.

<sup>99.</sup> *Id.* at 1274–75.

<sup>100.</sup> *Id.* at 1275 (citations omitted) (quoting Ralph Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH, 75, 104 (1994)).

<sup>101.</sup> *Id.* at 1276.

The Tenth Circuit extended its concerns about the application of a container metaphor to computers in a subsequent case. <sup>102</sup> In another case where child pornography was discovered during a different computer search, the court explained the *Carey* decision:

In [Carey], this court recognized the particular Fourth Amendment issues surrounding the search and seizure of computer equipment. The advent of the electronic age and, as we see in this case, the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.

The underlying premise in *Carey* is that officers conducting searches (and the magistrates issuing warrants for those searches) cannot simply conduct a sweeping, comprehensive search of a computer's hard drive. <sup>103</sup>

The Tenth Circuit is not alone in expressing a reluctance to simply view computers as containers as that term was understood twenty years ago. The Fourth Circuit similarly noted that "[a]lthough cases involving computers are not *sui generis*, the law of computers is fast evolving, and we are reluctant to recognize a retroactive right based on cases involving footlockers and other dissimilar objects."<sup>104</sup>

<sup>102.</sup> United States v. Walser, 275 F.3d 981 (10th Cir. 2001).

<sup>103.</sup> *Id.* at 986. The Tenth Circuit has subsequently narrowly construed the holding of *Carey*. *See* United States v. Grimmett, 439 F.3d 1263, 1268–69 (10th Cir. 2006) (*Carey* stands for proposition that "law enforcement may not expand the scope of a search beyond its original justification" and that the evidence seized must be "consistent with the probable cause originally articulated by the . . . judge.").

<sup>104.</sup> Trulock v. Freeh, 275 F.3d 391, 404 (4th Cir. 2001). The dissent in *Trulock* argued, "[T]he differences between computer files and physical repositories of personal information and effects are legally insignificant. Courts have not hesitated to apply established Fourth Amendment principles to computers and computer files, often drawing analogies between computers and physical storage units such as file cabinets and closed containers." *Id.* at 410 (Micheal, J., concurring in part and dissenting in part).

Many federal courts have held that computers are analogous to containers for the purpose of the Fourth Amendment.<sup>105</sup> That said, the question of whether the container doctrine extends to computers remains unresolved.<sup>106</sup> In a recent opinion, the Tenth Circuit stated in dicta that "one might speculate whether the Supreme Court would treat laptop computers, hard drives, flash drives, or even cell phones as it has a brief case or give those types of devices preferred status because of their unique ability to hold vast amounts of diverse personal information."<sup>107</sup> The closest case is perhaps a 2008 opinion from the Ninth Circuit upholding the search of the contents of a computer by Customs and Border Patrol of a passenger arriving at the Los Angeles International Airport.<sup>108</sup> A search at the border at first seems like a much different context than a traffic stop or criminal arrest, as persons entering the country have a diminished expectation of privacy.<sup>109</sup> However, the Ninth Circuit did not completely rely on this circumstance and appears

<sup>105.</sup> See, e.g., United States v. Barth, 26 F. Supp. 2d. 920, 936–37 (W.D. Tex. 1998); United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (holding that a computer notebook "is indistinguishable from any other closed container" for the purpose of Fourth Amendment analysis).

<sup>106.</sup> It is initially a bit surprising that (at least prior to *Gant*) there are few decisions involving the search of a laptop incident to arrest. However, it appears that most law enforcement officers prefer to seize computers and then obtain a warrant for a forensic analysis. For example, an FBI manual recommends seizing computers and then obtaining a warrant. Computer Crime and Intellectual Property Section Criminal Division, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, 33–34 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf. The FBI Manual states, "Courts have not yet addressed whether electronic media with the vast storage capacity of today's laptop computers may be searched incident to arrest." *Id.* at 33. The FBI manual then notes that "[a]s a practical matter, it may not be feasible to conduct an appropriate search of a laptop incident to arrest" and that "agents may choose to seize a laptop incident to arrest and then obtain a search warrant for the subsequent thorough search." *Id.* at 33–34.

<sup>107.</sup> United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009).

<sup>108.</sup> United States v. Arnold, 523 F.3d 941 (9th Cir. 2008).

<sup>109.</sup> The Department of Homeland Security, through both Customs and Border Protection and Immigration and Customs Enforcement, asserts the constitutional and statutory ability to search and detain all electronic media entering or leaving the country. See CBP Border Search of Electronic Devices Containing Information, U.S. DEPARTMENT OF HOMELAND SECURITY (Aug. 20, 2009); ICE Border Searches of Electronic Media, U.S. DEPARTMENT OF HOMELAND SECURITY (Aug. 18, 2009); see also infra note 313.

to suggest that computers be treated like traditional containers.<sup>110</sup> The court noted that the "Supreme Court has refused to draw distinctions between containers of information and contraband with respect to their quality or nature for purposes of determining the appropriate level of Fourth Amendment protection."<sup>111</sup>

# 3. Application of the Container Doctrine to Smart Cell Phones

While the United States Supreme Court has not considered the issue, the overwhelming majority of lower courts which have examined the question of whether the container doctrine applies to cell phones have concluded that the contents of cell phones may be searched incident to arrest without limitation. Most of these courts have concluded that a cell phone is a "container" as the term was defined in *Belton*, even while acknowledging that "*Belton*, decided in 1981 prior to the widespread use of cell phones, did not expressly address the authority to search such a device's electronic memory."

<sup>110.</sup> Arnold, 523 F.3d at 947.

<sup>111.</sup> *Id.*; see also United States v. Roberts, 86 F. Supp. 2d 678, 688–89 (S.D.Tex. 2000).

<sup>112.</sup> See United States v. Wurie, 612 F. Supp. 2d 104, 109 (D. Mass. 2009) (noting a "trend heavily in favor of finding that the search incident to arrest" doctrine applies to cell phones).

<sup>113.</sup> United States v. Deans, 549 F. Supp. 2d 1085, 1093–94 (D. Minn. 2008). These decisions do not discuss cell phones within the context of the *Chimel* justifications for searches incident to arrest. For example, the decisions do not address the possibility that cell phones may also conceal weapons. Cell phone guns have been reported in Europe since at least 2000. *See* Paul Sussman, *Bond-Style Mobile Phone-Guns Seized*, CNN (Nov. 30, 2000), http://edition.cnn.com/2000/WORLD/europe/11/30/mobile.gun/. A stun gun disguised as a cell phone is available for purchase in the United States for \$55. *See The Cell Phone Stun Gun*, SAFETY PRODUCTS UNLIMITED, http://www.safetyproductsunlimited.com/cell\_phone\_stun\_gun.html (last visited Oct. 18, 2010). These reports have been used by law enforcement to justify the seizure of cell phones. *See* Randy Ludlow, *Deputy Confiscates Woman's Cell Phone. He Feared it had been Modified Into a Gun*, COLUMBUS DISPATCH (OH) (July 30, 2010, 2:54 AM), http://www.dispatch.com/live/content/local\_news/stories/2010/07/30/deputy-confiscates-womans-cell-phone.html?sid=101.

The leading case on this issue is the Fifth Circuit opinion in *United States v. Finley*. <sup>114</sup> In *Finley*, the defendant drove an accomplice to a controlled purchase of methamphetamine set up by local and federal law enforcement. Following the sale, the police arrested the defendant and his accomplice. <sup>115</sup> During the arrest, the police seized a cell phone from the defendant's pocket. <sup>116</sup> A DEA agent reviewed the text messages on the defendant's phone and found several that appeared to be related to drug trafficking; the messages were used in the defendant's trial. <sup>117</sup>

The defendant in *Finley* sought to suppress the evidence from the cell phone, arguing that the police lacked authority to view the contents of the cell phone without a warrant. The court rejected this argument on the grounds that the "permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person. The *Finley* Court cited both *Belton* and *Robinson* in support of this proposition. The court considered the cell phone a

<sup>114. 477</sup> F.3d 250 (5th Cir. 2007).

<sup>115.</sup> *Id.* at 254.

<sup>116.</sup> *Id.* The cell phone belonged to the defendant's employer, but the defendant was permitted personal use of the phone. *Id.* 

<sup>117.</sup> *Id.* at 254–55 & n.2. The Defendant admitted during an interview that that most of the messages referred to the sale of marijuana. *Id.* at 255 n.2.

<sup>118.</sup> *Id.* at 258, 260.

<sup>119.</sup> *Id.* at 259–60. The court held that *Chadwick* was inapplicable because the cell phone was found on the defendant's person. *Id.* at 260 n.7.

<sup>120.</sup> *Id.* at 260. A number of courts have applied the automobile exception to the warrant requirement to cell phones discovered in cars. *See* California v. Acevedo, 500 U.S. 565 (1991). Under this exception, police may search closed containers in an automobile if there is probable cause to believe that evidence of a crime will be discovered. This is distinct from a search incident to arrest, where there is no requirement that law enforcement actually believe that the closed container contains evidence of a crime or a weapon to justify the search.

In the automobile exception cases, courts have permitted the search of the contents of cell phones when law enforcement had probable cause to believe that the phones contained evidence of a crime such as drug trafficking. *See* United States v. Fierros-Alavarez, 547 F. Supp. 2d 1206 (D. Kan. 2008) (automobile exception justified search of cell phone found in vehicle); United States v. Rocha, No. 06-40057-01-RDR, 2008 WL 4498950, at \*6 (D. Kan. Oct. 2, 2008) (automobile exception allows search of cell phone); United States v. James, No. 1:06CR134 CDP, 2008 WL 1925032, at \*5 (E.D. Mo. April 29, 2008) ("Because probable cause existed to believe that evidence of a crime would be found in the cell phone records and address book, the automobile exception allows the search of the

container, and, accordingly, law enforcement could search the contents of the phone incident to the defendant's arrest.

The analysis of the applicability of the container doctrine to cell phones in *Finley* was cursory. Other courts, however, have provided a more detailed review of the issue. For example, in *United State v. Wurie*, <sup>121</sup> the court stated that there was "no principled basis for distinguishing a warrantless search of a cell phone from the search of other types of personal containers found on a defendant's person." In reaching this conclusion, the *Wurie* court cited cases permitting searches incident to arrest of an address book, pockets, hand held luggage, a wallet, and a purse. Another federal district court that followed *Finley* reasoned that there is nothing to indicate that a higher court would "treat the retrieval of information from a cell phone differently than it treats other evidence gathered in a search incident to arrest."

The application of the container doctrine to searches of cell phones incident to arrest has been closely tied to another exception to the warrant requirement: exigent circumstances. <sup>125</sup>

Under this exception, the possible destruction of evidence before a warrant can be obtained

cell phone just as it allows the search of other closed containers found in vehicles"). These cases provide little assistance in analyzing whether law enforcement may search the contents of cell phones during a search incident to arrest because in these cases the officers lack probable cause to believe that the cell phones contain evidence of a crime. In *Finley*, for example, the officers did not appear to have probable cause to believe that the text messages would contain evidence of the controlled buy which formed the basis for the defendant's arrest. *See Finley*, 477 F.3d at 254.

- 121. 612 F. Supp. 2d 104 (D. Mass. 2009).
- 122. *Id.* at 110.

123. *Id.* (citing United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir.1993) (contents of an address book in arrestee's wallet); United States v. Rust, 650 F.2d 927, 928 (8th Cir.1981) (per curiam) (arrestee's pockets); United States v. Castro, 596 F.2d 674, 677 (5th Cir.1979) (man's wallet); United States v. Garcia, 605 F.2d 349, 355 (7th Cir.1979) (hand-held luggage); United States v. Moreno, 569 F.2d 1049, 1052 (9th Cir.1978) (woman's purse)).

- 124. United States v. Dennis, No. 07-088-DLB, 2007 WL 3400500 at \*7 (E.D. Ky. Nov. 13, 2007).
- 125. See, e.g., Mincey v. Arizona, 437 U.S. 385, 393–94 (1978); Warden v. Hayden, 387 U.S. 294, 298 (1967). "The police [however] bear a heavy burden in attempting to demonstrate an urgent need that might justify warrantless searches." Welsh v. Wisconsin, 466 U.S. 740, 749 (1984).

justifies a warrantless search. <sup>126</sup> A number of courts, excluding *Finley*, have relied upon the possible destruction of evidence in the finite memory of cell phones to justify warrantless searches or support the search incident to arrest. <sup>127</sup> For example, in *United States v. Mercado-Nava*, the court quoted from pager cases to support an argument that "evidence may be lost due to the dynamic nature of the information stored on and deleted from cell phones or pagers." <sup>128</sup> The viability of the argument that a possible loss of data justifies a search incident to arrest of the contents of a cell phone is likely limited, however. Greater storage capacity and the external storage of records by cell phone companies and e-mail providers alleviates much of the risk of data loss. <sup>129</sup>

One of the few pre-*Smith* decisions to suggest that the container doctrine may be inapplicable to cell phones is *United States v. Park*. <sup>130</sup> In *Park*, following the execution of a search warrant, the defendant was arrested for allegedly operating a marijuana cultivation operation. <sup>131</sup> During booking, police seized the defendant's cell phone (as well as other property). <sup>132</sup> Although there is some confusion as to exactly when the police searched the content of the cell phone, it appears that the search took place after booking. <sup>133</sup>

<sup>126.</sup> See Georgia v. Randolph, 547 U.S. 103, 117 n.6 (2006) ("a fairly perceived need to act on the spot to preserve evidence may justify entry and search under the exigent circumstances exception to the warrant requirement") (citing Schmerber v. California, 384 U.S. 757, 770–71 (1966)).

<sup>127.</sup> See generally discussion supra notes 87–90.

<sup>128. 486</sup> F. Supp. 2d 1271, 1278 (D. Kan. 2007).

<sup>129.</sup> The Fourth Circuit has noted that it would be impractical for officers to determine the storage capacity of any individual phone before conducting a search. United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009).

<sup>130.</sup> No. CR 05-375 SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007).

<sup>131.</sup> *Id.* at \*2.

<sup>132.</sup> *Id.* The seizure, but not search, of cell phones was standard procedure. *Id.* 

The *Park* court concluded that cell phones did not fall within the *Robinson* line of cases because cell phones should be more properly considered to be locked possessions, like the footlocker in *Chadwick*.<sup>134</sup> The court explained:

[M]odern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages. <sup>135</sup>

The *Park* court believed that the application of traditional rules to cell phones may be inappropriate because "the line between cell phones and personal computers has grown increasingly blurry." This blurry line was used to distinguish the pager line of cases because searches of pagers "implicated significantly fewer privacy interests given the technological differences between pagers and modern cell phones." In doing so, the court also rejected the position taken by the government that the contents of laptop computers would also be subject to search incident to arrest, noting that a "contrary holding could have far-ranging consequences." 138

Additionally, the *Park* court concluded that the search of the contents of the cell phone violated the Fourth Amendment because the search did not accomplish the traditional

<sup>133.</sup> *Id.* at \*3–\*5.

<sup>134.</sup> *Id.* at \*8; see United States v. Chadwick 433 U.S. 1, 16 (1977).

<sup>135.</sup> Park, 2007 WL 1521573, at \*8

<sup>136.</sup> *Id.* at \*8 (citing United States v. Arnold, 454 F. Supp. 2d 999, 1004 (C.D. Cal. 2006)).

<sup>137.</sup> *Id.* at \*9. The *Park* court also distinguished the pager cases, including *Ortiz*, on the grounds that the record did not support a claim that the evidence on the cell phone would be lost if not immediately searched.

<sup>138.</sup> *Id.* at 8. Accordingly, in the court's view, as in *Chadwick*, the officers should have seized the phones and then sought a warrant to review the contents. *Id.* (noting that the purpose for the search of the cell phone "was purely investigatory. Once the officers lawfully seized defendants' cellular phones, officers could have sought a warrant to search the contents of the cellular phones").

justifications for searches incident to arrest—officer safety and the prevention of the destruction of evidence.<sup>139</sup> In this respect, the *Park* court misinterpreted the *Chimel-Robinson-Belton* line of cases, which did not explicitly require officers to justify the search on an actual belief that the container contained a weapon or evidence of the crime for which the suspect was arrested.<sup>140</sup>

Some courts have attempted to distinguish *Park* from *Finley* on the basis of the fact that the search in *Park* took place during booking, not contemporaneously with the arrest. For example, in *United States v. Carroll*, the court noted that the search in *Park* took place perhaps over an hour after the arrest, whereas the search in *Finley* occurred at the time of the defendant's arrest. However, the *Park* court noted that, while the facts of *Park* and *Finely* may "differ slightly," the difference between the reasoning of the two decisions was "more fundamental." Other courts have simply dismissed the reasoning of *Park*, believing that the privacy concerns were given too much weight or that the decision ignored "general Fourth Amendment

<sup>139.</sup> *Id.* at \*9.

<sup>140.</sup> See supra notes 63–65 and accompanying text.

<sup>141. 537</sup> F. Supp. 2d 1290, 1302 (N.D. Ga. 2008); *see also* United States v. Yockey, No. CR09-4023-MWB, 2009 WL 2400973, at \*5 (N.D. Iowa Aug. 3, 2009) (stating that search of cell phone was impermissible because "[n]o reasonable claim [could] be made that the search was contemporaneous with the arrest"); United States v. Curry, No. 07-100-P-H, 2008 WL 219966, at \*9 (D. Me. Jan. 23, 2008) ("[T]he *Park* court distinguished *Finley* not only on the basis of doctrinal disagreement but also on the facts . . . ."); United States v. Santillan, 571 F. Supp. 2d 1093, 1102 n.5 (D. Ariz. 2008) ("In *Park* the booking search of the cell phones was conducted approximately an hour and a half after the arrests occurred, and thus the search was not roughly contemporaneous with the arrests.").

<sup>142.</sup> Park, 2007 WL 1521573 at \*8. The reluctance of the Park court to accept the reasoning of Finley and other cases was clear. The court said, "[A]bsent guidance to the contrary from the Ninth Circuit or the Supreme Court, this Court is unwilling to further extend [the search incident to arrest] doctrine to authorize the warrantless search of the contents of a cellular phone-and to effectively permit the warrantless search of a wide range of electronic storage devices . . . ." Id. at \*9; see also Curry, 2008 WL 219966, at \*9.

<sup>143.</sup> *See* United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at \*3 (E.D. Wis. Feb. 8, 2008). In contrast, a Massachusetts Superior Court judge, in dicta, noted that *Park* represented a "persuasive departure" from the line of cases permitting the searches of cell phones incident to arrest. Commonwealth v. Diaz, No ESCR2009-00060, 2009 WL 2963693, at \*7 n.1 (Mass. Super. Ct. Sept. 3, 2009).

jurisprudence on exceptions to the search warrant simply because the container is a cellular phone."<sup>144</sup>

While few courts prior to *Smith* followed the doctrinal analysis of *Park*, commentators and law professors have started to note the possible inapplicability of the container doctrine to content stored on cell phones. One commentator argued that the decision of the Supreme Court in *Belton* was based on the "justification that objects within the containers capable of harming the arresting officer or effect an escape were just as assessable as other objects within the arrestee's immediate reach." For this reason, the "Court's definition for 'container' as laid out in *Belton*, hardly seems applicable to cell phones." Instead, courts should treat cell phones more like computers than wallets or pagers. 147

Professor Adam Gershowitz, in analyzing the development of the iPhone, noted that smart phones present new challenges to the container doctrine because the new devices would provide "law enforcement with access to information that the typical arrestee would otherwise be incapable of carrying in his pocket." In reviewing *Robinson* and *Belton*, Professor Gershowitz noted:

<sup>144.</sup> United States v. Fierros-Alavarez, 547 F. Supp. 2d 1206, 1214 (D. Kansas 2008)

<sup>145.</sup> Stillwagon, *supra* note 18, at 1195.

<sup>146.</sup> *Id.* Stillwagon acknowledges that an arrestee may use the cell phone arrange for an escape of may erase evidence in the phone. However, he argues, "these risks are . . . eliminated by seizing the cell phone." *Id.* at 1196. This argument ignores *Robinson*, however, and would result in a fundamental shift in the law surrounding searches incident to arrest by forbidding the search of any container. In *Robinson*, for example, the same reasoning could have applied. The Court could have held that the officer in *Robinson* should have seized the cigarette package and held it for a later search with a warrant. *But see* United States v. Barth, 26 F. Supp. 2d. 929, 936–37 (W.D. Tex. 1998); United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (holding that a computer notebook "is indistinguishable from any other closed container" for the purpose of Fourth Amendment analysis).

<sup>147.</sup> Stillwagon, *supra* note 18, at 1202. Stillwagon also suggest that the "pager cases may have been wrongly decided." *Id.* at 1198.

<sup>148.</sup> Gershowitz, *supra* note 18, at 41. Gershowitz notes that smart phones can store photographs, audio, and e-mail messages, as well as the ability to access the Internet.

For many years, the only evidence found as a result of such searches was tangible physical evidence, such as drugs or illegal weapons. As technology has advanced however, a handful of lower courts have been forced to rule on the admissibility of nontangible digital evidence located in electronic devices, specifically pagers, cell phones, and computers. 149

Matthew Orso has further developed this tangible/non-tangible theme.<sup>150</sup> Orso wrote that "one must . . . question whether traditional notions of the lawful scope of a search incident to arrest even fit in the cellular phone context."<sup>151</sup> Orso explained:

With cellular phones, a different notion of scope is at play—virtual rather than spatial. The vast amount of information that may be stored digitally in a cellular phone far exceeds traditional concepts of the physical evidence that an arrestee can reach. This observation is magnified when one considers that many cellular phones can access remote databases. The virtual scope of a cellular phone's contents is thus very different from the spatial scope of a defendant's "grab area." <sup>152</sup>

Orso concluded that cellular phones require "a new articulation of the proper scope of a cellular phone's search incident to arrest." <sup>153</sup>

# III. STATE V. SMITH

Despite criticisms, most observers believed that searches of cell phones would continue to be permitted as searches of containers incident to arrest. For example, Professor Gershowitz predicted that courts would "almost certainly" apply the container doctrine to smart phones seized incident to an arrest. Another commentator, though critical, thought the container

<sup>149.</sup> *Id.* at 36.

<sup>150.</sup> Matthew E. Orso, Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence, 50 Santa Clara L. Rev. 183 (2010)

<sup>151.</sup> *Id.* at 206.

<sup>152.</sup> *Id.* 

<sup>153.</sup> *Id.* at 207.

<sup>154.</sup> Gershowitz, *supra* note 18, at 44. Orso noted that "most courts" have accepted the *Finley* position, although he suggests that *Park* represents a "budding divide." Orso, *supra* note 150, at 205.

doctrine was on solid ground, noting that the container doctrine has been accepted by many courts and that, as a result, "information in a cell phone, including text messages, is admissible under the same circumstances as the contents of a container." Then along came *State v. Smith*, 156 signaling a possible shift away from the container doctrine.

#### A. Facts

The *Smith* decision arose out of a drug sting operation outside of Dayton, Ohio.<sup>157</sup> A detective assigned to a regional drug task force received information that a large amount of cocaine had been discovered at the residence of a patient who had been taken to the hospital for a suspected drug overdose.<sup>158</sup> After police questioned the patient, she agreed to become an informant and to set up a controlled buy from her supplier at her home.<sup>159</sup> The patient did not know the name of her supplier, referring to him only as "Capo."<sup>160</sup> The police were able to obtain the identity of Smith as the supplier based on information from the informant.<sup>161</sup> The

<sup>155.</sup> Katharine M. O'Connor, Note, :O OMG They Searched My TXTS: Unraveling the Search and Seizure of Text Messages, 2010 U. ILL. L. REV. 685, 710 (2010).

<sup>156. 920</sup> N.E.2d 949 (Ohio 2009).

<sup>157.</sup> See id.

<sup>158.</sup> See id. at 950. The police observed the drugs in plain view when responding to a call about a suspected overdose. Merit Brief for Appellee at 3, State v. Smith, 920 N.E.2d 949 (Ohio 2009) (No. 2008-1781); Merit Brief for Appellant app. at A-28, State v. Smith, 920 N.E.2d 949 (Ohio 2009) (No. 2008-1781). The Ohio Supreme Court opinion does not mention the drugs found at the patient's home. The appellant's Merit Brief does not mention the drugs found in the patient's possession, and the appellant does not contest these facts in his Reply Brief. See Merit Brief for Appellant, supra, at 1; Reply Brief of Appellant at 1, State v. Smith, 920 N.E.2d 949 (Ohio 2009) (No. 2008-1781).

<sup>159. 920</sup> N.E.2d at 950.

<sup>160.</sup> Merit Brief for Appellee, *supra* note 158, at 3; Merit Brief for Appellant, *supra* note 158 app. at A-28.

<sup>161.</sup> Merit Brief for Appellee, *supra* note 158, at 3 (stating that patient told police that her supplier had recently been cited for marijuana possession on her street and that police looked up the traffic stop information and identified Smith as the passenger); Merit Brief for Appellant, *supra* note 158 app. at A-28 (stating that patient described Smith's vehicle).

police confirmed Smith's identity by showing the informant a bureau of motor vehicles photograph of Smith. 162

The controlled buy was set up through calls to Smith's cell phone.<sup>163</sup> Smith agreed to deliver an ounce of crack cocaine to the informant's home.<sup>164</sup> Smith arrived to the house late, by which time the informant was being taken back to the jail.<sup>165</sup> Smith called the informant's cell phone to let her know that he was at her residence.<sup>166</sup> Officers who were watching the house were informed of the call and placed Smith, who had returned to his car, under arrest.<sup>167</sup> During a search incident to arrest, the police found a cell phone on Smith.<sup>168</sup>

The police searched the call records and phone numbers on Smith's phone, confirming that Smith's cell phone had been used to speak with the informant. Exactly when the search occurred is unclear. The Ohio Supreme Court stated that "the record does not show exactly when [the police] searched Smith's cell phone." The court did note that some testimony

169. *Id*.

170. *Id*.

<sup>162.</sup> Merit Brief for Appellee, *supra* note 158, at 3. The Ohio Supreme Court opinion states only that the informant "identified" Smith as her supplier. 920 N.E.2d at 950.

<sup>163. 920</sup> N.E.2d at 950. The calls were placed from a police station and were recorded. *Id.*; Merit Brief for Appellee, *supra* note 158, at 3.

<sup>164.</sup> Merit Brief for Appellee, *supra* note 158, at 4; Merit Brief for Appellant, *supra* note 158, at 1.

<sup>165.</sup> Merit Brief for Appellee, *supra* note 158, at 4; Merit Brief for Appellant, *supra* note 158, at 1.

<sup>166.</sup> Merit Brief for Appellee, *supra* note 158, at 4; Merit Brief for Appellant, *supra* note 158, at 1 app. at A-29 (State v. Smith, No. 2007-CR-073, slip op. at 3 (C.P. Ct. Greene Cnty. Ohio April 11, 2007)).

Merit Brief for Appellant, *supra* note 158, at 1; *see* Merit Brief for Appellee, *supra* note 158, at 4. No cocaine was found on the Smith. *See* Merit Brief for Appellee, *supra* note 158, at 4; Merit Brief for Appellant, *supra* note 158, at 1. However, a bag of crack cocaine was found in the snow in a footprint left by Smith as he exited his vehicle. Merit Brief for Appellee, *supra* note 158, at 4. The police also found other indicia of drug dealing on Smith and in the car: \$2500 in cash, a digital scale, a marijuana blunt, a holster, and a loaded gun magazine. Merit Brief for Appellant, *supra* note 158, at 1.

<sup>168. 920</sup> N.E.2d at 950.

supported the conclusion that "at least a portion of the search took place when officers returned to the police station." Smith, in his brief to the Ohio Supreme Court, claimed that the search was "later that night" and that the police also searched through photographs on the cell phone. The trial court's finding of facts merely recites, "subsequently, the detectives searched the Defendant's cell phone prior to it being booked into evidence." The phone also contained photographs of Smith "posing with what appeared to be handguns and cocaine while wearing a bullet proof vest," but these photographs were not entered into evidence at trial. The Court of Appeals described the cell phone search as occurring "prior to booking."

Smith was convicted of five felonies: trafficking in cocaine, two counts of possession of criminal tools, possession of cocaine, and tampering with evidence. He was sentenced to twelve years in prison and fined \$10,000. The company of the company

### B. Legal Analysis

Smith sought to suppress the evidence obtained from his cell phone as having been obtained in violation of his Fourth Amendment rights.<sup>178</sup> The state, acknowledging that officers searched the cell phone without a warrant, argued that the search was permissible as a search

<sup>171.</sup> *Id*.

<sup>172.</sup> Merit Brief for Appellant, *supra* note 158, at 1. The State's brief addresses the issue of exactly when the phone was searched.

<sup>173.</sup> *Id.* at app. at A-30.

<sup>174.</sup> *Id.* The trial court excluded the use of the photographs at trial on relevancy grounds, stating that "the photographs recovered from the cell phone had nothing to do with the present offense." *Id.* at app. at A-32.

<sup>175.</sup> State v. Smith, No. 07-CA-47, 2008 WL 2861693, at \*1 (Ohio Ct. App. July 25, 2008).

<sup>176.</sup> State v. Smith, No. 2007-CR-0073, 2007 WL 6787908 (C.P. Ct. Greene Cnty. Ohio April 26, 2007) (judgment entry).

<sup>177.</sup> *Id*.

<sup>178.</sup> State v. Smith, 920 N.E.2d 949, 951 (Ohio 2009).

incident to arrest.<sup>179</sup> The state suggested in its brief that the search of the phone log was "akin to the search for an identification card or a phone number contained in a purse or a wallet."<sup>180</sup> The state relied upon the line of cases, starting with *Robinson*, that permits the search of a closed container seized during a lawful search incident to arrest. The state argued in its brief:

In *State v. Matthews*, [the Ohio Supreme Court] held that the warrantless search of a woman's purse, clutched under her arm and under her immediate control, incident to her lawful arrest is reasonable. It is hard to imagine that a cell phone, which can only contain data, is entitled to greater protection than the contents of a purse or wallet.<sup>181</sup>

The defendant responded that cell phones, which contain multiple types of "electronically stored information, such as photographs, text messages, and telephone numbers" are "patently . . . out of the realm of closed-container jurisprudence." <sup>182</sup>

The Ohio Supreme Court's decision focused on the question presented by the parties: whether "a cell phone is akin to a closed container and is thus subject to search upon a lawful arrest." The court concluded that a cell phone is not like a closed container as the term was used in *Belton*. The court said:

Objects falling under the banner of "closed container" have traditionally been physical objects capable of holding other physical objects. Indeed, the United States Supreme Court has stated that in this situation, "container" means "any object capable of holding another object." One such example is a cigarette package containing drugs found in a person's pocket, as in [*Robinson*]. <sup>184</sup>

180. Merit Brief for Appellee, *supra* note 158, at 6.

<sup>179.</sup> *Id*.

<sup>181.</sup> *Id.* (citation omitted).

<sup>182.</sup> Merit Brief for Appellant, *supra* note 158, at 7. The defendant suggested, "[I]f the police had wanted to physically open Mr. Smith's cell phone and search for contraband 'objects'—for example, if the battery had been removed and a small amount of contraband had been inserted in the battery compartment—then such a search would have been permissible . . . ." *Id*.

<sup>183. 920</sup> N.E.2d at 953–54.

The court reasoned that a "container" must "actually have a physical object within it" and that "[e]ven the more basic models of modern cell phones are capable of storing a wealth of digitized information wholly unlike any physical object found within a closed container."<sup>185</sup>

Significantly, the *Smith* court suggested that cell phones require a new and unique method of analysis.

Given their unique nature as multifunctional tools, cell phones defy easy categorization. On one hand, they contain digital address books very much akin to traditional address books carried on the person, which are entitled to a lower expectation of privacy in a search incident to an arrest. On the other hand, they have the ability to transmit large amounts of data in various forms, likening them to laptop computers, which are entitled to a higher expectation of privacy.<sup>186</sup>

The court rejected previous comparisons of electronic devices to containers, arguing that modern cell phones are different because of their advanced capabilities. The court said, "the pagers and computer memo books of the early and mid 1990s bear little resemblance to the cell phones of today." The court also stated that cell phones cannot be equated with computers because the ability of a computer "to store large amounts of private data gives their users a reasonable and justifiable expectation of a higher level of privacy." In the end, the court concluded that the

<sup>184.</sup> *Id.* at 954 (citations omitted). The dissent suggested that the search in this case resembled a permissible search of an address book. *Id.* at 957 (Cupp, J., dissenting).

<sup>185.</sup> *Id.* at 954 (majority opinion). The state suggested that exigent circumstances may be presented because the cell phone could only store a limited number of calls. *Id.* at 955. However, the Ohio Supreme Court did not address this issue because it had not been raised below. *Id.* 

<sup>186.</sup> *Id.* at 955.

<sup>187.</sup> *Id.* at 954. Some commentators have suggested that different rules could apply for different cell phones, depending upon the capabilities of the phone. *See supra* note 18. The Ohio Supreme Court felt this approach would be difficult to implement. "Because basic cell phones in today's world have a wide variety of possible functions, it would not be helpful to create a rule that requires officers to discern the capabilities of a cell phone before acting accordingly." *Smith*, 920 N.E.2d at 954.

<sup>188.</sup> *Id.* at 955.

heightened interest in privacy in the contents of cell phones outweighed the traditional justification of a search incident to arrest.<sup>189</sup>

#### C. Reaction to Smith

The *Smith* case received significant attention in the popular media and has been cited in a number of recent decisions.<sup>190</sup> The reaction to the *Smith* decision suggests that there is a public perception that cell phones warrant a reasonable and heightened expectation of privacy that outweighs the law enforcement justifications for a search incident to arrest. However, this public perception has only just started to penetrate the judiciary.

The Supreme Court of Wisconsin examined the search of a cell phone, pursuant to a warrant, in *State v. Carroll*.<sup>191</sup> In *Carroll*, law enforcement officers investigating an armed robbery observed the defendant leaving a residence under surveillance.<sup>192</sup> The defendant fled from the officers at a high rate a speed, before coming to a stop at a gas station parking lot.<sup>193</sup> When the defendant exited the car he dropped his cell phone on the ground; the phone fell open revealing a photograph of the defendant apparently smoking marijuana.<sup>194</sup> While the defendant was seated in the back of a patrol car, an officer scrolled through the phone and saw images of

<sup>189.</sup> *Id*.

<sup>190.</sup> The case has been followed by a number of lower Ohio courts. These decisions are not discussed in detail because *Smith* is binding on these courts. *See e.g.*, State v. Woodard, No. 2009-A-0047, 2010 WL 2557715, at \*3 (Ohio Ct. App. Jun 25, 2010); State v. Christopher, No. CA2009-08-041, 2010 WL 1660489, at \*6 (Ohio Ct. App. Apr 26, 2010); State v. Ewing, No. 09AP-776, 2010 WL 1248837, at \*6 (Ohio Ct. App. Mar 31, 2010); State v. Williams, No. 92822, 2010 WL 866130, at \*4 (Ohio Ct. App. Mar 11, 2010).

<sup>191. 778</sup> N.W.2d 1, 4 (Wis. 2010).

<sup>192.</sup> *Id.* at 5.

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

<sup>194.</sup> *Id.* A narcotics detective recognized a blunt in the photograph, which was labeled "Big Boss Player." *Id.* at n.2.

drugs, firearms, and a large amount of currency. The officer, pretending to be the defendant, also answered a call to the phone from a person seeking to purchase drugs. The officer, relying in part on the images observed on the phone, subsequently obtained a search warrant for the phone.

In reviewing the initial search of the cell phone, the Wisconsin court was satisfied the seizure and possession of the phone by the officers was permissible. The court, however, held that the initial viewing of the images in the cell phone violated the defendant's Fourth Amendment rights. The court's majority opinion did not address the question of whether the search of the phone was permissible as a search of a container found incident to arrest. Instead, the court distinguished this case from cases where phone logs may be reviewed immediately because of a risk that new calls might delete older calls. In finding that the search was not permissible, the court held that there was no similar risk of loss of data in the review of the photographs. However, the court refused to order the suppression of the evidence under the independent source doctrine because the officer had sufficient information without the images to justify a search warrant.

195. *Id.* at 5–6.

196. *Id.* at 6.

197. *Id*.

198. *Id.* at 9–12.

199. *Id.* at 12–13.

200. *Id.* at 12–14.

201. *Id.* Notably, the court cites to decisions, such as *Finley*, that rely on the container doctrine.

<sup>202.</sup> *Id.* at 14-15. The independent source doctrine serves as an exception to the exclusionary rule and permits the introduction of "evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality." Murray v. United States, 487 U.S. 533, 537 (1988).

While the majority opinion in *Carroll* did not address *Smith*, a dissenting justice cited the *Smith* decision.<sup>203</sup> The dissent disagreed that there was enough independent evidence to justify a search warrant and distinguished cases where phones were searched as situations where the police had reason to believe the suspect was a drug dealer.<sup>204</sup> Like the majority, the dissent did not address the whether the phone could be searched like a container found on an arrestee.

In *Jackson v. Kelly*, <sup>205</sup> a federal district court magistrate in Ohio reviewed on habeas a state court conviction for, inter alia, rape and possession of child pornography. <sup>206</sup> Significant incriminating evidence was found on the defendant's cell phone, including photographs of the defendant with his penis in the victim's mouth. <sup>207</sup> The defendant's cell phone was seized during his arrest, and before obtaining a warrant, the police examined the cell phone and observed the incriminating photographs. <sup>208</sup> The police then obtained a search warrant to conduct further examination of the defendant's phone. <sup>209</sup> The state court of appeals had concluded that, while there is "some debate as to whether the officers could proceed to examine the contents of the [cell phone]" prior to obtaining a warrant, the evidence would have been admissible under the inevitable discovery exception to the exclusionary rule because a search warrant was being sought and would have been granted even without the evidence observed during the initial search

<sup>203.</sup> *Carroll*, 778 N.W.2d at 28 ("[T]he Ohio Supreme Court recently took a restrictive view of warrantless cell phone searches.") (Prosser, J., dissenting).

<sup>204.</sup> *Id*.

<sup>205.</sup> No. 4:09CV1185, 2010 WL 1913385 (N.D. Ohio April 5, 2010).

<sup>206.</sup> *Id.* at \*1.

<sup>207.</sup> *Id.* at \*2.

<sup>208.</sup> *Id.* at \*3. One of the detectives testified that the police intentionally sought to arrest the defendant while he was carrying his cell phones so that they could be lawfully seized. *Id.* at \*7.

<sup>209.</sup> *Id.* at \*3.

of the phone.<sup>210</sup> In this respect, *Jackson* is similar to *Carroll*. The *Jackson* court distinguished *Smith* on the grounds that the Ohio Supreme Court had not considered the inevitable discovery rule.<sup>211</sup>

The California Court of Appeals has declined to follow *Smith*. In *People v. Chho*,<sup>212</sup> the defendant's car was stopped for a minor traffic violation.<sup>213</sup> The Defendant admitted to having some marijuana under his seat and consented to a search of the car to recover the drugs.<sup>214</sup> The officer recovered the drugs and noticed a cell phone on the center console, which was ringing repeatedly.<sup>215</sup> The officer then received consent to search the trunk of the car where more marijuana was found.<sup>216</sup> After finding the marijuana in the trunk, the officer believed that the defendant may have been engaged in drug dealing.<sup>217</sup> According to the opinion, because "of this

<sup>210.</sup> *Id.* at \*7–8 (citing State v. Jackson, 2007 WL 4481412, at \*4–\*6 (Ohio Ct. App. Dec. 21, 2007)).

<sup>211.</sup> *Id.* at \*8. The Magistrate also noted that *Smith* was not a United States Supreme Court decision which must be considered on habeas review, and that the decision cannot be applied retroactively. *Id.* Although not argued by the parties, the inevitable discovery rule may have been applicable to *Smith*. Under this doctrine, unlawfully obtained evidence is admissible if the government can "establish by a preponderance of the evidence that the information ultimately or inevitably would have been discovered by lawful means." Nix v. Williams, 467 U.S. 431, 432 (1984). In *Smith*, because the informant called the defendant's cell phone, there was probably sufficient probable cause to justify the issuance of a warrant had the police sought one. The doctrine would not be applicable in those situations where the police had no prior independent knowledge that the cell phone was likely to contain evidence of a crime and wished to review the contents of the phone for an unrelated investigatory purpose. *Cf.* United States v. Park, No. CR 05-375 SI, 2007 WL 1521573 (N.D. Cal. May 23, 2007). Thus, the inevitable discovery rule has no bearing on the broader question of whether police may search cell phones incident to arrest.

<sup>212.</sup> No. H034693, 2010 WL 1952659 (Ca.. Ct. App. May 17, 2010).

<sup>213.</sup> *Id.* at \*1.

<sup>214.</sup> *Id*.

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

<sup>216.</sup> *Id*.

<sup>217.</sup> *Id.* at \*2.

suspicion, and for investigatory purposes," the officer seized the phone, opened it, and read two incoming text messages. <sup>218</sup>

The *Chho* court concluded that the search of the phone was reasonable under the automobile exception—not as a search incident to arrest—because the officer had probable cause to search the automobile for additional evidence of drug dealing. The *Chho* court distinguished cases where cell phones were searched as closed containers incident to arrest. In distinguishing *Smith* and other decisions on this basis, the court said, "whether a cell phone constitutes a closed container . . . do[es] not bear on our analysis and conclusion in this case, which is premised on the automobile exception to the warrant requirement."

In *State v. Boyd*,<sup>222</sup> the Connecticut Supreme Court considered a case in which the defendant was convicted of murder.<sup>223</sup> Part of the evidence was obtained from a cell phone that the police seized from the passenger seat of the car the defendant had been driving when he was arrested.<sup>224</sup> The state argued, in part, that the search of the contents of the cell phone was valid

<sup>218.</sup> *Id*.

<sup>219.</sup> *Id.* at \*4. Under the automobile exception, if officers have probable cause to believe that a vehicle contains contraband or evidence, it may be searched without a warrant. Chambers v. Maroney, 399 U.S. 42, 47–48, 52 (1970). This search of the vehicle may include any items or containers found in the vehicle. California v. Acevedo, 500 U.S. 565, 579–80 (1991); United States v. Ross, 456 U.S. 798, 825 (1982).

<sup>220.</sup> Other courts have held that the seizure of the cell phones and the extraction of data from them is permissible under the automobile exception. *See e.g.*, United States v. James, No. 1:06CR134 CDP, 2008 WL 1925032 at \*3-9 (E.D. Mo. April 29, 2008) ("Because probable cause existed to believe that evidence of a crime would be found in the cell phone call records and address book, the automobile exception allows the search of the cell phone just as it allows a search of other closed containers found in vehicles"); United States v. Fierros-Alavarez, 547 F. Supp. 2d 1206, 1211–14 (D. Kan. 2008) (stating that the automobile exception justified search of cell phone found in vehicle).

<sup>221.</sup> Chho, 2010 WL 1952659, at \*6.

<sup>222. 992</sup> A.2d 1071 (Conn. 2010).

<sup>223.</sup> *Id.* at 1075.

<sup>224.</sup> *Id.* at 1077.

under the automobile exception to the warrant requirement.<sup>225</sup> In a footnote, the *Boyd* court stated that a "number of courts have analogized cell phones to closed containers"<sup>226</sup> but also noted that *Park* and *Smith* stand for the opposite conclusion."<sup>227</sup>

The media's reaction to *Smith* was significantly and almost universally positive.<sup>228</sup> A Cleveland newspaper, in an editorial, stated, "[w]hile we're sensitive to the needs of police and want them to be provided with as many resources as possible to apprehend suspected criminals, we also believe an individual's rights should be protected."<sup>229</sup> The *New York Times* also published an editorial about the opinion. The editorial described the opinion as "an important blow for privacy rights" and "a model for other courts to follow."<sup>230</sup> The *Times* acknowledged that cell phones are perceived as different from traditional containers. The editorial continued:

<sup>225.</sup> *Id.* at 1078. The state conceded that, unlike in *Smith*, the search in this case was not a search incident to arrest. *Id.* at 1084. The seizure and search of the cell phone was permissible under *Arizona v. Gant*, 129 S. Ct. 1710, 1719 (2009), because the cell phone could constitute evidence related to the offense of arrest. *Id.* at 1089 n.16.

<sup>226.</sup> *Gant*, 129 S. Ct. at 1089 n.17 (citing United States v. Rocha, No. 06-40057-01-RDR, 2008 WL 4498950 (D. Kan. October 2, 2008); United States v. James, No. 1:06CR134 CDP, 2008 WL 1925032, at \*4 (E.D. Mo. April 29, 2008)).

<sup>227.</sup> *Id*.

The Associated Press Report on the decision stated, in part: "A divided Ohio Supreme Court has ruled that police must obtain a search warrant before searching the contents of a suspect's cell phone except under certain circumstances. The court's 5-4 decision Tuesday appears to be the first on the topic among state high Ohio Supreme Court rules cell phone searches require warrant, Associated Press, http://www.wfmj.com/Global/story.asp?S=11680226 (last visited Oct. 14, 2010); see, e.g., Stephen Majors, Ohio Court: Cell Phone Searches Require Warrant, ASSOCIATED http://www.msnbc.msn.com/id/34445730/ns/technology\_and\_science-security/ (last updated Dec. 16, 2009). Blog entries that merely reported the decision noted that "[c]ourts have struggled with how to apply Fourth Amendment protections to modern technology." Jaclyn Belczyk, Ohio Supreme Court Rules Warrantless Cell Phone Searches Violate Fourth Amendment, JURIST LEGAL NEWS & RESEARCH (Dec. 16, 2009, 9:02 AM), http://jurist.law.pitt.edu/paperchase/2009/12/ohio-supreme-court-rules-warrantless.php.

<sup>229.</sup> Editorial, *Court Dials in Good Phone Ruling*, THE NEWS-HERALD (Dec. 28, 2009), http://www.news-herald.com/articles/2009/12/28/opinion/nh1846182.txt.

<sup>230.</sup> Editorial, *Cellphone Searches*, N.Y. TIMES, December 26, 2009 p. A22, *available at* http://www.nytimes.com/2009/12/26/opinion/26sat2.html.

Rather than seeing a cellphone [sic] as a simple closed container, the majority noted that modern cellphones [sic]—especially ones [sic] that permit Internet access—are "capable of storing a wealth of digitized information."

This is information . . . for which people reasonably have a high expectation of privacy . . . .

. . . The Ohio ruling eloquently makes the case for why the very personal information that new forms of technology aggregate must be accorded a significant degree of privacy.  $^{231}$ 

Some legal blog entries noted that the Ohio Supreme Court decision represented a different manner of viewing the Fourth Amendment issues presented by cell phones. The *Jurist* blog research editor noted, "[c]ourts have struggled with how to apply Fourth Amendment protections to modern technology."<sup>232</sup> Other blogs simply reprinted news articles about the decision.<sup>233</sup>

The reaction from civil liberties and criminal defense advocates was also predictably positive. Notably, these observers saw the opinion as likely to lead to more changes in the law. One defense attorney exclaimed, "[f]inally, a court recognizing what had become obvious." A press release from the American Civil Liberties Union mentioned that the Ohio Supreme Court seemed to be moving in a new direction because of the changing technology. The ACLU attorney said:

<sup>231.</sup> *Id*.

<sup>232.</sup> Belczyk, *supra* note 228. In the blog entry, the author compares the *Smith* decision to the Supreme Court's consideration of text messages in *City of Ontario*, *Cal. v. Quon*, 130 S. Ct. 2619 (2010)

<sup>233.</sup> See e.g., Philip Smith, Search and Seizure: Ohio Supreme Court Rules Police Need Warrant to Search Cell Phones, DRUG WAR CHRON. (Dec. 18, 2009, 12:00 AM), http://stopthedrugwar.org/chronicle/613/ohio\_supreme\_court\_cell\_phone\_search\_warrant; The Fourth Amendment Applies to Cell Phones, ASK THE JUDGE (Feb. 3, 2010), http://askthejudge.info/the-fourth-amendment-applies-to-cell-phones/4012/.

<sup>234.</sup> *OH: Cell Phone Search Without Exigent Circumstances Not Reasonable*, FOURTH AMENDMENT (Dec. 15, 2009, 11:10 AM), http://fourthamendment.com/blog/index.php?blog=1&title=oh\_cellphone\_search\_incident\_without\_exi&more=1&c=1&tb=1&pb=1. The blog entry refers to Professor Gershowitz's article.

"Oftentimes, the law fails to keep up with the fast pace of technology, but this decision lays the groundwork for greater privacy protections as the digital age advances.

The modern cell phone is often not used simply to make and receive calls—many people use them to access the internet, manage finances, house personal photos, catalogue personal contact information and a host of other functions. The Court clearly holds that law enforcement cannot go on "fishing expeditions" and search this information without a warrant"....<sup>235</sup>

In a similar way, a DUI defense-related blog entry said of the Smith opinion, "[t]his landmark case is sure to provide great precedent for future cases addressing this same issue." <sup>236</sup>

## IV. SIMILAR TENSION AS COURTS ATTEMPT TO EXTEND TRADITIONAL TRACKING DEVICE DECISIONS TO GPS DEVICES

The growing inability of existing doctrines to account for changes in technology is not limited to cell phones. In recent years, law enforcement has commonly placed GPS tracking devices on private vehicles parked in public places.<sup>237</sup> The permissible placement of these devices without a warrant is based on the theory that there is no expectation of privacy in movements on a public roadway, and that the GPS device merely augments what the police

<sup>235.</sup> Ohio Supreme Court Decision on Cell Phone Searches Protects Privacy and Due Process, ACLU (Dec. 15, 2009) http://www.aclu.org/technology-and-liberty/ohio-supreme-court-decision-cell-phone-searches-protects-privacy-and-due-proc.

<sup>236.</sup> Can Police Search Your Cell Phone If You Are Pulled Over?, GA. DUI LAW BLOG (Dec. 30, 2009), http://www.georgiaduilawblog.com/2009/12/30/can-police-search-your-cell-phone-if-you-are-pulled-over/.

<sup>237.</sup> Modern GPS tracking devices permit law enforcement to follow vehicles in real time and store data on time, position, and speed for later analysis. Privately available devices and services are as small as pager size and provide current and historical location information through Internet mapping programs. The devices can also be set to provide notifications if the device enters or exits certain designated geographic zones. See David Pogue, Zoombak Tracks Your Dog, Your Car, Even Your Children, N.Y. TIMES, April 23, 2009, at B1, available at http://www.nytimes.com/2009/04/23/technology.personaltech/23pogue.html. GPS cell phone tracking is also available for families for as little as \$5/month. Press Release, Bus. Wire, Soar Into the Sch. Year with Straight 'A' Devices and Honor-Roll Worthy **Applications** from Sprint 11, (Aug. http://www.marketwatch.com/story/soar-into-the-school-year-with-straight-a-devices-and-honor-roll-worthyapplications-from-sprint-2010-08-11?reflink=MW news stmp (visited August 12, 2010); see also Life360 Launches Real-Time Family Tracking App for iPhone That Lets Parents Monitor and Protect Children Bus. Wire (Aug. 2010. AM). http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news\_view&newsId=20100810005886&ne wsLang=en ("By equipping children with the Life360 mobile app, or a small GPS locator device available for purchase, parents can continuously track and monitor their family members).

could accomplish through traditional surveillance. Yet, as with cell phones, courts are beginning to express concerns that law enforcement use of surreptitious GPS monitoring raises concerns that the technological sophistication and nature of use of GPS devices has created a threat to expectations of privacy that renders previous doctrinal interpretations obsolete.<sup>238</sup>

The Supreme Court has not considered whether law enforcement must obtain a warrant before placing a GPS device on a private vehicle. The Court considered police use of less sophisticated electronic tracking devices placed on vehicles first in *United States v. Knotts*<sup>239</sup> and again in *United States v. Karo*. In *Knotts*, the defendant was suspected of manufacturing methamphetamine. With the consent of a chemical company, law enforcement officers installed a beeper inside a five-gallon drum of chemicals used in the manufacture of the drugs. When the defendant's co-conspirator purchased the chemicals, the officers were able to follow the transit of the chemicals through both visual surveillance and a monitor that received the

<sup>238.</sup> Law enforcement has also obtained real-time and historical location tracking information from cell phones. These efforts are most likely governed by the Electronic Communications Privacy Act of 1986. The majority of courts examining this issue have concluded that the government must obtain a court order, upon a showing of probable cause, in order to obtain cell phone tracking information. See Adam Koppel, Note, Warranting a Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking, 64 U. MIAMI L. REV. 1061, 1081–82 and n. 160 (2010) (collecting cases). For this reason, the same doctrinal pressures seen in the searches of cell phones incident to arrest and the use of GPS devices on vehicles without a warrant are not present.

The view that cell phone tracking may only occur pursuant to a showing of probable cause is not unanimous, however. Some courts have suggested that the government must obtain a warrant in order to obtain this information. *In re* Application for Order of a Pen Register, 402 F.Supp.2d 597, 604–05 (D. Md. 2005). In contrast, some courts have suggested that the Fourth Amendment is not implicated if law enforcement only seeks cell tower information from cell phone providers to permit the tracking of a person in public places. *See* United States v. Suarez-Blanca, No. 1:07-CR-023-MHS/AJB, 2008 WL 4200156, at \*10 (N.D. Ga. April 21, 2008) ("[T]he Court finds that there is no Fourth Amendment search in tracking the location of the cell phone towers used in making phone calls . . . .").

<sup>239.</sup> United States v. Knotts, 460 U.S. 276 (1983).

<sup>240.</sup> United States v. Karo, 468 U.S. 705 (1984).

<sup>241.</sup> Knotts, 460 U.S. at 277.

<sup>242.</sup> *Id.* at 278.

signals sent from the beeper.<sup>243</sup> At one point, because of the driver's evasive maneuvers, the police lost both visual contact with the vehicle and the signal from the beeper.<sup>244</sup> The officers reestablished the location of the vehicle at the defendant's home with the assistance of a monitoring device located in a helicopter.<sup>245</sup>

The Supreme Court held that a warrant was not required to track the vehicle using the beeper.<sup>246</sup> The Court's analysis began with the premise established by *Katz* and *Smith v*. *Maryland* that the Fourth Amendment is applicable only when the person subject to surveillance had a legitimate, justifiable, or reasonable expectation of privacy.<sup>247</sup> The Court then reasoned that, for Fourth Amendment purposes, no reasonable privacy interest exists in the movement of a vehicle traveling on a public roadway because drivers voluntarily convey to the public their location and direction of travel.<sup>248</sup> The Court explained:

Visual surveillance from public places . . . would have sufficed to reveal all of these facts to the police. The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of [the] automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.<sup>249</sup>

243. *Id*.

244. Id.

245. *Id.* at 278–79. Relying in part upon the information obtained through the use of the beeper, officers obtained a search warrant for the defendant's cabin. The officers discovered a drug laboratory, \$10,000 worth of laboratory equipment, and chemicals in quantities sufficient to produce fourteen pounds of pure amphetamine. Officers located the five-gallon container with the beeper under a barrel outside the cabin. *Id.* at 279.

246. See id. at 281.

247. *Id.* at 280–81 (citing Katz v. United States, 389 U.S. 347, 361 (1967)); Smith v. Maryland, 442 U.S. at 740-41(1979); *see supra* text accompanying notes 32–40.

248. *Knotts*, 460 U.S. at 281–82. This includes the fact of the location where private property is entered from the public highway. *Id*.

In other words, even when technology such as helicopters, airplanes, and satellites aid law enforcement's vision, people have no legitimate expectation of privacy in their location so long as law enforcement can view them.<sup>250</sup> The *Knotts* Court compared the use of the beeper to the use of a searchlight or binoculars by police in other situations.<sup>251</sup> The court also compared voluntary travel on the roads in view of the public with the voluntary provision of phone number information in *Smith v. Maryland*.<sup>252</sup>

Although a first view of *Knotts* seems to suggest that the Court would approve the warrantless use of GPS devices, the *Knotts* Court stopped short of permitting the type of surveillance permitted by GPS devices.<sup>253</sup> The defendant argued that permitting the use of electronic tracking devices without a warrant would inevitably lead to twenty-four-hour surveillance of any citizen.<sup>254</sup> The Court reserved that issue, saying, in response, "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."<sup>255</sup> Justice Stevens's concurring opinion emphasizes his view that there was a limit

<sup>249.</sup> *Id.* at 282. The fact that visual surveillance failed in this case, and the beeper allowed the officers to obtain information they would not have obtained with electronic support, was inconsequential. It was sufficient, in the Court's view, that the officers "could have observed" the vehicle at all times. *Id.* at 285 (emphasis added).

<sup>250.</sup> In *Dow Chemical v. United States*, 476 U.S. 227 (1986). the Court considered the use by law enforcement of aerial photography and surveillance. The Court noted that the use of satellite technology may present different Fourth Amendment issues because it is not readily available to the public. *Id.* at 238. However, as at least one observer has pointed out, the easy availability of these images through on-line services such as Google Earth<sup>TM</sup> has eliminated this concern because a reduced expectation of privacy occurs when a technology becomes generally available. Brian Craig, *Online Satellite and Aerial Images: Issues and Analysis*, 83 N.D. L. REV. 547, 572 (2007).

<sup>251.</sup> Knotts, 460 U.S. at 283 (citing United States v. Lee, 274 U.S. 559, 563 (1927)).

<sup>252.</sup> *Id*.

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

<sup>254.</sup> *Id.* 

to police use of technology, stating, "[a]lthough the augmentation in this case was unobjectionable, it by no means follows that the use of electronic detection techniques does not implicate especially sensitive concerns." <sup>256</sup>

A little over a year later, the Court considered whether the warrantless monitoring of a beeper in a private residence violated the Fourth Amendment. In *Karo*, as in *Knotts*, law enforcement officers placed a beeper in a container of chemicals to be used by suspected drug dealers.<sup>257</sup> The Court reaffirmed that there is no Fourth Amendment violation where the beeper provided information that could have been "observed by the naked eye."<sup>258</sup> However, the Court would not permit the beeper to be used to continue to monitor the container after it had entered a private residence without a warrant.<sup>259</sup> In doing so, the Court maintained the view that the privacy interests at stake were tied to whether the container had or had not been "withdrawn from public view."<sup>260</sup>

<sup>255.</sup> *Id.* at 283–84 (noting that the "reality hardly suggests abuse" (quoting Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978)).

<sup>256.</sup> *Id.* at 287 (Stevens, J., concurring).

<sup>257.</sup> United States v. Karo, 468 U.S. 705, 708–10 (1984). The drug dealers in *Karo* were using the chemical ether to remove cocaine from clothing.

<sup>258.</sup> *Id.* at 713–14; *see also* United States v. McIver, 186 F.3d 1119, 1127 (9th Cir. 1999) (holding that in placing a tracking device, officers did not infringe on any area of vehicle owner intended to shield from public view).

<sup>259.</sup> Karo, 468 U.S. at 716.

<sup>260.</sup> *Id.* The Court expressed a similar protective view of a residence in *Kyllo v. United States*, 533 U.S. 27 (2001). In *Kyllo*, the Court considered whether law enforcement could use thermal imagers to obtain information about the inside of residences. *Id.* The Court held that the use of such devices without a warrant violated the Fourth Amendment because the devices were not readily available to the public and the devices revealed information about the interior of a residence that could not be obtained by the naked eye. *Id.* at 34–35. GPS tracking devices are readily available to the public, are intended to reveal information available to an observer with a naked eye, and do not provide information about the interior of a residence.

Based on *Knotts* and *Karo*, the federal courts that have considered the question of GPS monitoring have generally permitted the placement and use of the devices on public streets. <sup>261</sup> For example, in *United States v. Marquez*, the Eighth Circuit Court of Appeals found that the Fourth Amendment was not violated when law enforcement officers placed a GPS device on a truck in a Wal-Mart parking lot and then monitored the truck traveling back and forth from Iowa to Denver. <sup>262</sup> The court, like others, relied on the *Knotts* doctrine: persons traveling by automobile have no reasonable expectation of privacy in their movements from one place to another. <sup>263</sup> Similarly, the Ninth Circuit, in *United States v. Pineda-Moreno*, <sup>264</sup> upheld the warrantless placement of a GPS device on the jeep of a suspected marijuana grower by DEA agents. <sup>265</sup> The court observed that "the only information the agents obtained from the tracking devices was a log of the locations where [the defendant's] car traveled, information the agents could have obtained by following the car." <sup>266</sup>

<sup>261.</sup> See, e.g., United States v. Williams, 650 F. Supp. 2d 633, 668 (W.D. Ky. 2009) ("Given the absence of a legitimate expectation of privacy that [the] Defendant . . . would have in the exterior of a publicly parked vehicle" there is no requirement that officers obtain a warrant before installing a GPS device.); United States v. Coulombe, No. 1:06-CR-343, 2007 WL 4192005, at \*4 (N.D.N.Y. Nov. 26, 2007) ("There is no Fourth Amendment violation when the installation of a tracking device on a vehicle's undercarriage does not damage the vehicle or invade its interior."); United States v. Moran, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) (tracking GPS device on public roads is permissible because officers could have conducted surveillance by following vehicle). The public-private distinction emphasized in Karo was relied upon in United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006). In Jones, the court suppressed evidence from a GPS tracking device obtained while the vehicle was in a private garage, but permitted the government to use evidence obtained while the vehicle was on public streets. Id.

<sup>262. 605</sup> F.3d 604, 607, 609 (8th Cir. 2010). The police in *Marquez* accessed the device seven times to change the battery—all while the truck was parked in a public place. *Id.* at 607.

<sup>263.</sup> *Id.* at 609. The *Marquez* court described GPS devices as "merely allow[ing] police to reduce the costs of lawful surveillance." *Id.* at 610.

<sup>264. 591</sup> F.3d 1212 (9th Cir. 2010).

<sup>265.</sup> *Id.* at 1217. Numerous devices were placed on the vehicle over a four month period of time. *Id.* at 1213. Sometimes the devices were placed on the vehicle while it was parked on a public street; other times the device was placed on the vehicle while it was parked in the defendant's driveway. *Id.* at 1213.

<sup>266.</sup> *Id.* at 1216.

However, some courts have started questioning whether the doctrine is applicable to GPS and similar tracking devices. On the federal level, Judge Richard Posner of the Seventh Circuit questioned whether the *Knotts* doctrine was applicable to GPS tracking devices. <sup>267</sup> In *United States v. Garcia*, the defendant was suspected of manufacturing and dealing methamphetamine. While the defendant's car was parked on a public street, the police placed a GPS tracking unit underneath the rear bumper of his vehicle. The police later retrieved the device and learned that the car had traveled to a large tract of private land. With the consent of the landowner, the police conducted a search of the land and found equipment and materials used in the manufacture of methamphetamine. While the police were on the property, the defendant arrived and was subsequently charged and convicted of crimes related to the manufacture of methamphetamine.

The defendant in *Garcia* sought to suppress the evidence obtained from the tracking device.<sup>273</sup> The *Garcia* court began its analysis with the *Knotts* doctrine, emphasizing that police may use advanced technology to augment their senses, stating the following:

[I]f police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search. Well, but the tracking in this case *was* by satellite. Instead of transmitting images, the satellite transmitted geophysical coordinates. The only difference is that in the

<sup>267.</sup> United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).

<sup>268.</sup> *Id.* at 995.

<sup>269.</sup> *Id*.

<sup>270.</sup> *Id*.

<sup>271.</sup> *Id*.

<sup>272.</sup> *Id.* at 995–96.

<sup>273.</sup> *Id.* at 996.

imaging case nothing touches the vehicle, while in the case at hand the tracking device does. But it is a distinction without any practical difference.<sup>274</sup>

The court ultimately concluded, on the basis of the *Knotts* doctrine, that no search, and consequently no Fourth Amendment violation, had occurred.<sup>275</sup> *Garcia* is, nonetheless, significant because the court noted that the new technology of GPS tracking devices may eventually make the *Knotts* doctrine inapplicable. The court said,

There is a practical difference lurking here, however. It is the difference between, on the one hand, police trying to follow a car in their own car, and, on the other hand, using cameras (whether mounted on lampposts or in satellites) or GPS devices. In other words, it is the difference between the old technology—the technology of the internal combustion engine—and newer technologies (cameras are not new, of course, but coordinating the images recorded by thousands of such cameras is).<sup>276</sup>

The court was concerned that while the beeper in *Knotts* was "only a modest improvement over following a car by means of unaided human vision," the GPS device permitted "an extent of surveillance that in earlier times would have been prohibitively expensive." The *Garcia* court was also concerned that the new technology could permit the type of "wholesale surveillance" mentioned as potentially problematic in *Knotts* and that such a broad surveillance program could violate the Fourth Amendment even if it were an "efficient alternative to hiring another 10

<sup>274.</sup> *Id.* at 997. The court later said, "GPS tracking is on the same side of the divide with the surveillance cameras and the satellite imaging, and if what they do is not searching in Fourth Amendment terms, neither is GPS tracking." *Id.* 

<sup>275.</sup> *Id.* at 997–98.

<sup>276.</sup> *Id.* at 997. The *Marquez* court noted Judge Posner's concerns. United States v. Marquez, 605 F3d 604, 610 (8th Cir. 2010) ("We are mindful of the concerns surrounding the use of electronic tracking devices."). However, the *Marquez* court seemed inclined to not view the use of the devices as raising the problems of large-scale surveillance reserved by the *Knotts* Court so long as "there was nothing random or arbitrary about the installation and use of the device." *Id.* The *Pineda-Moreno* court also took note of Judge Posner's concerns, but similarly declined to address the issue of mass surveillance programs. United States v. Pineda-Moreno, 591 F.3d 1212, 1216 n.2 (9th Cir. 2010).

<sup>277.</sup> *Garcia*, 474 F.3d at 998.

million police officers to tail every vehicle on the nation's roads."<sup>278</sup> Ultimately, the *Garcia* court declined to address that issue because it was satisfied that the government had "abundant grounds" to suspect the defendant of criminal activity.<sup>279</sup>

State courts have, in some instances, refused to apply the logic of the *Knotts* doctrine to the use of tracking devices on vehicles. In these cases, rather than addressing directly the Supreme Court opinions in *Knotts* and *Karo*, the state courts have based their decisions on the state constitutional equivalents of the Fourth Amendment. As early as 1988, the Oregon Supreme Court held that the Oregon Constitution prohibited the placement of a tracking device on a vehicle without a warrant. In reaching this conclusion, the Oregon Supreme Court specifically rejected the core of the *Knotts* doctrine: that an electronic tracking device does not infringe on a reasonable privacy interest because it merely discloses what the police and public could legitimately observe. The court said that the electronic monitoring was so different from traditional surveillance as to constitute a different category:

<sup>278.</sup> *Id.* at 997–98.

<sup>279.</sup> *Id.* at 998. The court added: "Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case. . . . Should government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search." *Id.* 

<sup>280.</sup> See Sarah Rahter, Privacy Implications of GPS Tracking Technology, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 755, 763–66 (2008). Some state courts have picked up on the concerns expressed by the Garcia court while still holding that the use of GPS tracking devices did not violate the Fourth Amendment. See e.g., State v. Sveum, 769 NW.2d 53, 60 (Wis. Ct. App. 2009) ("We are more than a little troubled by the conclusion that no Fourth Amendment search or seizure occurs when police use a GPS or similar device . . . ."). The Sveum court urged the legislature to impose restrictions on both the public and private use of such devices. Id. at 61.

<sup>281.</sup> State v. Campbell, 759 P.2d 1040 (Or. 1988). "Article 1, Section 9, of the Oregon Constitution provides: 'No law shall violate the right of the people to be secure in their persons, houses, papers and effects, against unreasonable search, or seizure . . . ." *Id.* at 1041 n.1. The Oregon Supreme Court has interpreted this constitutional provision as having a broader reach than the Fourth Amendment. *Id.* at 1049.

<sup>282.</sup> *Id.* at 1045. The Oregon Supreme Court also did not accept the factual assumption underlying the argument that the electronic device merely replaced police observations. *Id.* The court noted, that in the case before

[The] use of a radio transmitter to locate an object to which the transmitter is attached cannot be equated with visual tracking. Any device that enables the police quickly to locate a person or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny . . . . The limitation is made more substantial by the fact that the radio transmitter is much more difficult to detect than would-be observers who must rely upon the sense of sight. Without an ongoing, meticulous examination of one's possessions, one can never be sure that one's location is not being monitored by means of a radio transmitter. <sup>283</sup>

The Oregon court based its conclusions on the observation that the use of an electronic tracking device, even in those situations where police could observe the suspect, provides a high level of scrutiny that violated "social and legal norms." <sup>284</sup>

The Washington Supreme Court, a few years later, adopted the reasoning of the Oregon Supreme Court in interpreting its state constitution, holding that police may not install a GPS tracking device on a vehicle without a warrant.<sup>285</sup> As did the Oregon Court, the Washington Supreme Court specifically rejected the idea that the *Knotts* doctrine could be applied to electronic devices. The Washington Supreme Court accepted the premise that no search occurs when officers can lawfully observe the suspect, even with the use of binoculars and flashlights.<sup>286</sup> However, the Washington Supreme Court was unwilling to extend this doctrine to electronic tracking devices.

it, the police had been unable to track the suspect through traditional means and, in fact, had a policy that permitted the use of electronic devices only when "visual surveillance had failed." *Id*.

284. *Id*.

286. *Id*.

<sup>283.</sup> *Id.* at 1048. The Oregon Supreme Court defined the privacy interest established by the Oregon constitution as "an interest in freedom from particular forms of scrutiny." *Id.* at 1047.

<sup>285.</sup> State v. Jackson, 76 P.3d 217 (Wash. 2003). In *Jackson*, the defendant did not argue that the use of a GPS device violated the Fourth Amendment. *Id.* at 222 n.1. Instead, the defendant relied solely on Article I, section 7 of the Washington Constitution ("[N]o person shall be disturbed in his private affairs, or his home invaded, without authority of law."). *Id.* at 222. The Washington Supreme Court has interpreted this constitutional provision as having a broader reach than the Fourth Amendment. *Id.* 

[W]hen a GPS device is attached to a vehicle, law enforcement officers do not in fact follow the vehicle. Thus, unlike binoculars or a flashlight, the GPS device does not merely augment the officers' senses, but rather provides a technological substitute for traditional visual tracking. . . . We perceive a difference between the kind of uninterrupted 24-hour a day surveillance possible through use of a GPS device, which does not depend upon whether an officer could in fact have maintained visual contact over the tracking period, and an officer's use of binoculars or a flashlight to augment his or her senses. <sup>287</sup>

Like the Oregon Supreme Court, which believed that the use of electronic devices violated social and legal norms, the Washington Supreme Court expressed a concern that the use of GPS devices was "particularly intrusive" and made it possible for the government to acquire "an enormous amount of personal information about the citizen."

The New York Court of Appeals recently recognized the failure of the *Knotts* doctrine to adequately account for advanced technology like GPS tracking devices. The New York Court described the new technology as "doctrine-forcing" in this respect. Compared with the beeper in *Knotts*, the New York court observed, "GPS is a vastly different and exponentially more sophisticated technology that is easily and cheaply deployed and has virtually unlimited and

<sup>287.</sup> *Id.* at 223.

<sup>288.</sup> *Id.* at 224.

People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009). The Massachusetts Supreme Judicial Court also recognized the limitations of the *Knotts* doctrine, but declined to determine whether the use of a GPS tracking device constituted a search. Commonwealth v. Connolly, 913 N.E.2d 356, 370 n.13 (Mass. 2009). The Massachusetts Court, relying on *Dow Chemical*, expressed concern that the level of sophistication of GPS devices might lead to a Fourth Amendment violation because the technology "replaces rather than enhances officers' physical abilities . . . ." *Id.* at 367. However, the Massachusetts Court did not reach this issue because it concluded that, because the GPS device used in this particular case required the use of the defendant's vehicle's electrical system, the actions of the police asserted control over private property and, therefore, constituted an unconstitutional seizure. *Id.* at 369. Three of the seven justices, in a concurring opinion, believed that the Massachusetts Court should have concluded that the use of a GPS tracking device constituted a search. *Id.* at 377 (Gants, J., concurring) ("The court's decision suggests that the constitutional concern we have with GPS monitoring is that attaching the device to the outside of a motor vehicle interferes with the owner's property interest. In fact, the appropriate constitutional concern is not the protection of property but rather the protection of the reasonable expectation of privacy.").

<sup>290.</sup> Weaver, 909 N.E.2d at 1198. The New York Court relied on article I, section 12 of the New York Constitution.

remarkably precise tracking capability."<sup>291</sup> The court explained that this made the *Knotts* doctrine inapplicable:

Constant, relentless tracking of anything is now not merely possible but entirely practicable, indeed much more practicable than the surveillance conducted in *Knotts*. GPS is not a mere enhancement of human sensory capacity, it facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period. The potential for a similar capture of information or "seeing" by law enforcement would require, at a minimum, millions of additional police officers and cameras on every street lamp. <sup>292</sup>

The New York court concluded that in the face of this sophisticated technology, the argument that GPS is able to capture what an officer could observe, collapses. The court explained,

It is, of course, true that the expectation of privacy has been deemed diminished in a car upon a public thoroughfare. But, it is one thing to suppose that the diminished expectation affords a police officer certain well-circumscribed options for which a warrant is not required and quite another to suppose that when we drive or ride in a vehicle our expectations of privacy are so utterly diminished that we effectively consent to the unsupervised disclosure to law enforcement authorities of all that GPS technology can and will reveal.<sup>293</sup>

Like the Oregon and Washington decisions, the New York Court did not suggest a principle for when, in the face of advanced technology, the *Knotts* doctrine would be applicable, as the dissent noted, "[t]he attempt to find in the Constitution a line between ordinary, acceptable means of observation and more efficient, high-tech ones that cannot be used without a warrant seems . . . illogical, and doomed to fail."<sup>294</sup>

<sup>291.</sup> Id. at 1199.

<sup>292.</sup> *Id.*; cf. United States v. Garcia, 605 F.2d 349, 355 (7th Cir. 1979).

<sup>293.</sup> *Id.* at 1200.

<sup>294.</sup> *Id.* at 1203–04 (Smith, J., dissenting).

The D.C. Circuit Court of Appeals, in *United States v. Maynard*,<sup>295</sup> recently broke from the previous federal decisions on this issue, holding that the continuous use of a GPS monitor on the vehicle of a suspected drug dealer for four weeks without a warrant violated the Fourth Amendment.<sup>296</sup> In *Maynard*, the court first found that *Knotts* was not controlling on the grounds that *Knotts* did not hold that "a person has no reasonable expectation of privacy in his movements whatsoever, world without end . . . ."<sup>297</sup> The court then held that *Knotts* was inapplicable despite the fact that the subject of tracking in both cases was theoretically visible to an observer.<sup>298</sup> The court reasoned that, unlike with the beeper in *Knotts*, a person had an expectation of privacy in the type of information a GPS device gathers because "the whole" of a person's movements is not "actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil."<sup>299</sup> The court explained the difference as follows:

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer [sic], a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

<sup>295. 615</sup> F.3d 544 (D.C. Cir. 2010).

<sup>296.</sup> *Id.* at 560.

<sup>297.</sup> *Id.* at 557. The *Maynard* court stated that the defendants in both *Garcia*, and *Pineda-Moreno*, did not directly address whether *Knotts* was controlling. *Id.* at 557–58.

<sup>298.</sup> *Id.* at 560.

<sup>299.</sup> *Id.* at 558. The court also noted that observing the "whole" of a person's movements over a period of time is distinct from observing a series of individual movements.

The *Maynard* court was willing to apply a different analysis and abandon the *Knotts* doctrine because "the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave."<sup>301</sup>

The public view of law enforcement use of GPS tracking devices has been more muted and balanced than the reaction to the *Smith* decision. Some news articles have simply noted that this generally remains an unsettled area of law "without a clear legal answer." A *New York Times* editorial praised the *Weaver* decision but noted, "It is never easy to fit modern technology into the broad privacy principles that the drafters of the federal and state constitutions laid out." In contrast, an editorial in the *New York Daily News* criticized the *Weaver* decision as a "breathtakingly foolhardy decision that will severely hamper New York law enforcement." The *Pineda-Moreno* decision received positive editorial commentary in the media. An editorial in the Portland Press Herald praised the decision, stating, "[W]hen you look at the totality of a person's movements over an extended period of time, you have information that no individual

<sup>300.</sup> *Id.* at 562; *see also In re* United States Order Authorizing the Release of Historical Cell-Site Info., 2010 U.S. Dist. LEXIS 88781, at \*17–18 (E.D.N.Y. Aug. 27, 2010) (following *Maynard* and concluding that "prolonged surveillance reveals information that differs in kind, not just in degree, from the results of any short-term surveillance.").

<sup>301.</sup> *Maynard*, 615 F.3d at 565. A few days after the decision in *Maynard* was announced, the Ninth Circuit announced a motion for rehearing en banc in *Pineda-Moreno*. Chief Judge Kozinski filed a dissent to this decision. In this dissent, Judge Kozinski wrote, that the GPS devices have "little in common with the primitive devices in *Knotts*" and expressed his concern that the new technology "can provide law enforcement with a swift, efficient, silent, invisible and *cheap* way of tracking the movements of virtually anyone and everyone they choose." United States v. Pineda-Moreno, No. 08-30385, 2010 WL 3169573, at \*4, \*6 (9th Cir. Aug. 12, 2010) (Kozinski, J., dissenting). Judge Kozinski summarized his views as follows: "There is something creepy and un-American about such clandestine and underhanded behavior." *Id.* at \*7.

<sup>302.</sup> Yvonne Zipp, *Courts Divided on Police Use of GPS Tracking*, THE CHRISTIAN SCIENCE MONITOR, May 15, 2009, http://www.csmonitor.com/USA/2009/0515/p02s13-usgn.html.

<sup>303.</sup> Editorial, GPS and Privacy Rights, N.Y. TIMES, May 14, 2009, at A38.

<sup>304.</sup> Editorial, Way Off Track: New York's High Court Rendered Foolhardy Decision on Police Use of GPS, N.Y. DAILY NEWS, May 17, 2009, http://www.nydailynews.com/opinions/2009/05/18/2009-05-18\_way\_off\_track.html.

## V. THE FUTURE OF SEARCHES OF SMART PHONES AND OTHER SOPHISTICATED ELECTRONIC DEVICES

The public reaction to *Smith* suggests that legal doctrine concerning searches incident to arrest has not yet caught up with the public perception of privacy. It is important to recall how the courts got to this point. In *Robinson*, the police were permitted to search a cigarette package incident to a lawful arrest. And in *Belton*, a container was defined as "any object capable of holding another object." The extension of these decisions to wallets, purses, and address books did not seem to upset traditional notions of the extent of searches incident to arrest, as the person under arrest intentionally placed information or objects in these containers. The extension of the doctrine to pagers also did not seem to upset traditional notions of the extent of searches incident to arrest, as the information on pagers is relatively limited—pagers function more like pen registers than modern cell phones. The public, however, seems to view cell phones differently.

Orin Kerr, Comment to *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, THE VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/#more-35137 (emphasis omitted).

<sup>305.</sup> Editorial, *Our View: Court makes right call on warrantless GPS tracking*, PORTLAND PRESS HERALD, August 10, 2010, http://www.pressherald.com/opinion/court-makes-right-call-on-warrantless-gps-tracking\_2010-08-10.html (last visited August 12, 2010). In one comment on the decision in a criminal law blog, the author of the post agreed with the decision, writing, "GPS tracking, like cell site locator information, reveals a lot about you." Jeralyn, *Federal Appeals Court Tosses Drug Conviction, Says GPS Tracking Requires Warrant*, TALKLEFT (Aug. 7, 2010, 8:00 PM), http://www.talkleft.com/story/2010/8/7/101/34078. In contrast, Professor Orin Kerr posted critical comments about the decision on the Volokh Conspiracy blog. Professor Kerr wrote:

Maynard introduces a novel theory of the Fourth Amendment: That whether government conduct is a search is measured not by whether a particular individual act is a search, but rather whether an entire course of conduct, viewed collectively, amounts to a search. That is, individual acts that on their own are not searches, when committed in some particular combinations, become searches. Thus in Maynard, the court does not look at individual recordings of data from the GPS device and ask whether they are searches. Instead, the court looks at the entirety of surveillance over a one-month period and views it as one single "thing."

At some point, however, the difference in degree between the amount of information traditionally carried in tangible objects and contained in electronic devices becomes a difference in kind. In science, the moment when a difference in degree becomes a difference in kind is easy to see. Water at 33 degrees, 150 degrees, and 210 degrees is in the same liquid form as water at 211 degrees. But at 212 degrees, the water becomes a gas. In law, however, differences of degree may appear essentially immeasurable because they are not simply correlated with differences in kind. For this reason, courts tend to be resistant to differences in degree becoming differences in kind—or courts are at least incapable of determining when a shift has occurred. For example, in discussing the difference between government intrusion to effectuate a warrantless arrest and a warrantless arrest, the United States Supreme Court has stated, "[T]he critical point is that any differences in the intrusiveness of entries to search and entries to arrest are merely ones of degree rather than kind." 307

Yet, in some constitutional cases, the Supreme Court has recognized that a difference in degree *can* become a difference in kind. In a case involving a the constitutionality of a 25-foot or 100-foot boundary around polling places, the Court said, "Reducing the boundary to 25 feet . . .

<sup>306.</sup> *Cf.* CURT DUCASSE, PHILOSOPHY AS A SCIENCE, 1941 (noting that in philosophy, as opposed to science, differences of degree may be difficult to measure, even at certain critical points (discussing R.G. COLLINGWOOD, PHILOSOPHICAL METHOD (1933)).

<sup>307.</sup> Peyton v. New York, 445 U.S. 573, 589 (1980). The reluctance of courts to find differences in degree becoming differences in kind perhaps reached a peak in an Indiana case where an electrician was killed when the metal crane and bucket in which he was working came into contact with overhead electrical wires. In discussing whether the plaintiff was aware of the risk of injury or death, the court considered whether electrocution and electric shock were different degrees of the same injury, or distinct injuries. The court reasoned:

The question becomes whether the difference between an electrical shock and electrocution is one of kind or degree. We answer that the difference is one of degree. Anderson experienced an initial shock of electricity while standing in the metal basket attached to the steel crane. He was aware that an amount of electricity could surge through his person. The fact that a fatal amount of electricity surged through him is a matter of degree, not a matter of a completely different injury.

. is a difference only in degree, not a less restrictive alternative in kind."<sup>308</sup> However, the Court acknowledged that "[a]t some measurable distance from the polls, of course, governmental regulation of vote solicitation could effectively become an impermissible burden."<sup>309</sup> In a subsequent case, the Louisiana Supreme Court struck down a 600-foot boundary around polling places on the basis of *Burson v. Freeman*. The court said, "[W]hen that blanket proscription on political speech is extended to 600 feet we find that 'a difference only of degree' becomes a difference of kind, a difference of 'constitutional dimension."<sup>310</sup>

The state court decisions, the dicta in the Seventh Circuit in *Garcia*, and the D.C. Circuit opinion in *Maynard* concerning the warrantless use of GPS tracking devices by law enforcement are illustrative of courts struggling with and ultimately resisting the application of traditional Fourth Amendment doctrines to new technologies. The questioning of the applicability of the *Knotts* doctrine to GPS devices suggests that courts have recognized that while people accept that police may observe them while traveling on public ways, the level of detail that police obtain from a GPS device raises distinct privacy concerns.<sup>311</sup> These courts' treatment of GPS tracking devices provides an example where a difference in degree becomes a difference in kind with doctrinal significance. The D.C. Circuit was explicit on this point:

The whole of one's movements over the course of a month is not constructively exposed to the public because . . . that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a

<sup>308.</sup> Burson v. Freeman, 504 U.S. 191, 210 (1992).

<sup>309.</sup> *Id*.

<sup>310.</sup> State v. Schirmer, 646 So.2d 890, 901 (La. 1994); *see also* United States v. Mannarino, 850 F. Supp. 57, 70 (D. Mass. 1994) (noting that effect of cumulative evidence can change from difference in degree to difference in kind).

<sup>311.</sup> *See* Koppel, *supra* note 238 at 1084 ("Most drivers would be shocked, if not outraged, to learn that law enforcement has the ability to conduct these activities without any judicial intervention.").

day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more. <sup>312</sup>

Thus, in these cases, the courts have started to recognize that traditional Fourth Amendment doctrines, like the *Knotts* doctrine, are unable to adequately account for technologies that implicate novel expectations of privacy and must be abandoned.

The *Smith* decision, like the GPS cases, could signal a collapse of the container doctrine as applied to electronic devices, as courts begin to recognize that the volume and types of information available on electronic devices distinguish them from traditional containers. A traditional container, as conceived in *Robinson* and *Belton*, may contain pictures, contact information, letters, personal notes or journals, or any other type of information. However, because of the ever-increasing ability of cell phones, the sheer amount of these pieces of personal information that can be contained in an electronic device far exceeds what could have been originally conceived as held on, or within the reach of, an arrestee. For this reason, the inspection of a physical container incident to arrest raises exponentially fewer legitimate privacy concerns.<sup>313</sup>

<sup>312.</sup> United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010).

<sup>313.</sup> The Department of Homeland Security recently recognized this distinction in reviewing its policy on border searches of computers. The Department's Privacy Impact Statement notes:

The . . . more central privacy concern is the sheer volume and range of types of information available on electronic devices as opposed to a more traditional briefcase or backpack. In the past, someone might bring a briefcase or similar accessory across the border that contains pictures of their friends or family, work materials, personal notes or journals, or any other type of personal information. Because of the availability of electronic information storage and the capacity for comfortable portability, the amount of personal and business information that can be hand-carried by a single individual has increased exponentially. Where someone may not feel that the inspection of a briefcase would raise significant privacy concerns because the volume of information to be searched is not great, that same person may feel that a search of their laptop increases the possibility of privacy risks due to the vast amount of information potentially available on electronic devices.

The ability of electronic devices to store information is changing rapidly, and it is foolish consistency to continue to try to place the square pegs of electronic devices in the round hole of the container doctrine.<sup>314</sup> This is not to suggest that the entire search incident to arrest doctrine should be abandoned or even re-examined.<sup>315</sup> The search incident to arrest doctrine, as described in *Chimel*, remains good law, and the *Gant* decision is a clear indication that the Supreme Court does not intend to radically change or abandon its traditional approach.<sup>316</sup> The problem is narrower—what devices should be excluded from the definition of containers, and how does a court make this determination?

Many of the solutions commentators have offered to the problem of applying the container doctrine to electronic devices have been unduly complicated. For example, Professor Gershowitz suggested several possible rules including limiting the police to searches of open applications, a fixed number of steps, or information stored only on the device (as opposed to the Internet). Gershowitz acknowledged, "At the end of the day, all [of the approaches] appear to be somewhat unsatisfying." Other proposed solutions to the challenge of searches incident to

Privacy Impact Assessment for the Border Searches of Electronic Devices, U.S. DEPARTMENT OF HOMELAND SECURITY (August 25, 2009),

http://www.dhs.gov/xlibrary/assets/privacy/privacy pia cbp laptop.pdf.

<sup>314.</sup> See Kyllo v. United States, 533 U.S 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.").

<sup>315.</sup> Rahter, for example, suggests that a "proportionality principle" developed by Christopher Slobogin could replace the current Fourth Amendment framework. Rahter, *supra* note 280, at 773–75 (quoting Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment (Univ. of Chicago Press 2007)).

<sup>316.</sup> While the *Gant* decision modified the rule for searches of vehicles incident to arrest, it accepted the underlying rationale of broad searches incident to arrest. Arizona v. Gant, 129 S. Ct. 1710, 1724–25 (2009) (Scalia, J., concurring) (noting that the contours of permissible search may shift, but the Court has consistently accepted the underlying rationale behind the search incident to arrest exception to the warrant requirement).

<sup>317.</sup> Gershowitz, *supra* note 18, at 53–57.

arrest involving advancing technology are too vague to be useful.<sup>319</sup> The approach the Ohio Supreme Court suggested in *Smith* appears simple to apply.<sup>320</sup> By excluding from the definition of container certain devices capable of storing electronic information, the court removes such devices from the container doctrine, yet still retains the underlying rationale behind *Chimel*.<sup>321</sup>

The tougher aspect of the question *Smith* leaves unanswered is how to determine that a certain electronic device is not subject to the existing doctrine.<sup>322</sup> The Supreme Court's observation that "[1]egitimation of expectations of privacy by law must have a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."<sup>323</sup> The answer is not found in examining the technological capabilities of a particular electronic device, as that is constantly evolving. Rather, courts should review whether an examination of the contents of the device is reasonably likely to lead to the discovery of the type of intimate details about a person that the

<sup>318.</sup> *Id.* at 57. Gershowitz concludes that despite the flaws with various approaches, "all are likely preferable to doing nothing and allowing police to search thousands of pages of electronic data without probable cause or a warrant." *Id.* at 58.

<sup>319.</sup> See, e.g., Ramya Shah, From Beepers to GPS: Can the Fourth Amendment Keep Up With Electronic Tracking Technology?, 2009 U. ILL. J.L. TECH. & POL'Y 281, 293–94 (2009) (suggesting that courts "should analyze Fourth Amendment concerns with GPS technology as a novel issue of law").

<sup>320.</sup> Law enforcement should still retain the ability to inspect electronic devices to determine that they do not contain concealed weapons. *See supra* notes 48–49 and accompanying text (noting that search incident to arrest is justified by officer safety concerns).

<sup>321.</sup> The same is true of the approach by the Oregon, Washington, and New York courts in dealing with GPS tracking. *See* cases cited *supra* notes 281–94 and accompanying text. By asserting that the use of a GPS tracking device is a search because it implicates an expectation of privacy, the court removes such devices from the *Knotts* doctrine.

<sup>322.</sup> GPS devices present the same question. The *Kyllo* Court examined the "power of technology to shrink the realm of guaranteed privacy." Kyllo v. United States, 533 U.S. 27, 34 (2001). In doing so, the Court noted, "The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable." *Id*.

<sup>323.</sup> Rakas v. Illinois, 439 U.S. 128, 143 n. 12 (1978); *see also* United States v. Jacobsen, 466 U.S. 109, 122 n. 22 (1984) ("[I]t would, of course, be merely tautological to fall back on the notion that those expectations of privacy which are legitimate depend primarily on cases deciding exclusionary-rule issues in criminal cases.").

due process right of "informational privacy," the individual's right to avoid the "disclosure of personal matters," protects.<sup>324</sup> In the context of advanced technology, this right to informational privacy includes not only those personal rights traditionally thought of as fundamental, but also medical information, sexual activity, and financial information.<sup>325</sup> The definition of the exact scope of the right of information privacy is beyond this paper; the purpose of this paper is to suggest a framework for courts to determine if a warrant is required before law enforcement examines the contents of an electronic device.

Regarding smart phones, specifically, it is not necessary to sketch out the exact contours of the type of information encompassed to determine that the answer would be in the affirmative.

Again, the GPS cases are instructive. The courts that have been most troubled by the use of

<sup>324.</sup> Whalen v. Roe, 429 U.S. 589, 599 (1977). The *Whalen* Court, to be sure, does not clearly define whether the right of nondisclosure of personal information is limited to an area of life protected by either the autonomy branch of the right of privacy or by other fundamental rights, or whether the right is broader. *See generally* Symposium, *Informational Privacy: Philosophical Foundations and Legal Implications*, 44 SAN DIEGO L. REV. 695 (2007).

Orin Kerr recently suggested that the application of the Fourth Amendment to the Internet should be based on the distinction between inside, or high privacy spaces, and outside, or low privacy spaces, in the physical world. Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1006 (2010). Kerr explains that this distinction can be applied to electronic information:

In the online setting, courts should treat non-content information relating to communications as if it were functionally "outside" and content information as if it were functionally "inside." Internet surveillance of non-content information should not trigger the Fourth Amendment just like surveillance of public spaces does not trigger Fourth Amendment, and surveillance of content should presumptively trigger the Fourth Amendment in the Internet setting just like surveillance of inside spaces presumptively triggers the Fourth Amendment in the physical world.

*Id.* at 1018. One of the primary challenges to Kerr's approach, as he acknowledges (at 1032–34), is that the type of information that GPS surveillance, or a review of the content of a cell phone, can reveal significantly more information about personal matters than was possible with "traditional" surveillance. The primary difference between the approach urged by Kerr and the approach presented by this paper is that Kerr maintains that differences between traditional "outside" surveillance and non-content Internet surveillance "are differences in degree, not differences in kind. They rest on fluid practical judgments about the likely impact of a type of surveillance that may fluctuate as technology shifts." *Id.* at 1033.

<sup>325.</sup> See, e.g., Nelson v. NASA, 530 F.3d 865, 877 (9th Cir. 2008); J.P. v. Desanti, 653 F.2d 1080, 1090 (6th Cir 1981) (right to privacy is triggered only when those rights "that can be deemed 'fundamental' or 'implicit in the concept of ordered liberty" are at stake); cf. Bloch v. Ribar, 156 F.3d 673, 683–85 (6th Cir. 1998) (holding that right to informational privacy is linked to Fourteenth Amendment).

warrantless GPS tracking have been concerned that the gathering of detailed data on a person's whereabouts could provide an observer the opportunity to learn about a person's habits and associates. These constitute personal matters that an individual has a right to keep secret, and about which an individual has a reasonable expectation of privacy. The same principles apply to smart phones because an examination of the contents of a person's e-mails, text messages, documents, and photographs could provide an observer with potentially unlimited information about the device's owner, including personal, medical, or financial information or political or religious views.

## VI. CONCLUSION

"The Fourth Amendment protects people, not places."<sup>327</sup> The development of smart phones is not the first and will not be the last time that the courts will be asked to determine precisely what protection the Fourth Amendment affords people. Furthermore, the development of smart phones is not the first and will not be the last time that the courts will be confronted with a new technology that renders the prior answers to that question obsolete.

The challenge smart phones pose is that the devices contain information and communications that people reasonably expect to be free from intrusion, even when placed under arrest. The public reaction to the *Smith* decision suggests that society is willing to recognize that

<sup>326.</sup> The Washington Supreme Court described the level of intrusiveness presented by a GPS device:

<sup>[</sup>T]he device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the "wrong" side of town, the family planning clinic, the labor rally.

State v. Jackson, 76 P.3d 217, 223 (Wash. 2003); see also Susan J. Walsh & Ivan J. Dominguez, *Privacy and Technology: Law Enforcement's Secret Use of GPS Devices*, THE CHAMPION, May 12, 2009, at 26, available at http://www.nacdl.org/public.nsf/0/6666338cb48c6cf9852575e600629c0c?OpenDocument.

<sup>327.</sup> Katz v. United States, 389 U.S. 347, 351 (1967).

expectation of privacy is reasonable, and to impose tighter limits on law enforcement's review of cell phone data than, for example, law enforcement's review of what numbers were dialed. This does not mean that law enforcement should never be permitted to review the contents of cell phones incident to arrest without a warrant, as exigent circumstances and other law enforcement needs may justify exceptions.

Arrests, even for minor offenses, such as seat belt violations, are not uncommon and could permit police unprecedented access into data stored on electronic devices held by the arrestee. To continue to treat advanced devices like smart phones as containers under an analytical doctrine originally developed when such devices were nonexistent or new would be to permit the use of technology that is commonly available and used by the public to erode the privacy guarantees of the Fourth Amendment. Instead, courts should recognize that certain electronic devices are reasonably likely to contain intimate personal information about a person, and to exclude these devices from the traditional doctrines.

\_

<sup>328.</sup> See, e.g., Atwater v. City of Lago Vista, 532 U.S. 318, 323 (2001) (holding that the Fourth Amendment does not prohibit a law enforcement officer from arresting a person for a misdemeanor offense committed); see also Gershowitz, supra note 18, at 31 (noting that "police officers with nothing more than a hunch of illegal activity may arrest an individual for a simple traffic violation and proceed to search thousands of pages of private data located on the iPhone found in the arrestee's pocket").

<sup>329.</sup> The first cell phone was invented in 1973 by Martin Cooper. *See Did You Know?*, FCC, http://www.fcc.gov/cgb/kidszone/faqs\_cellphones.html (last visited Aug. 9, 2010).