2008

The iPhone Meets the Fourth Amendment

Adam M. Gershowitz
William & Mary Law School, amgershowitz@wm.edu

THE iPHONE MEETS THE FOURTH AMENDMENT

Adam M. Gershowitz*

Under the search incident to arrest doctrine, police may search the entire body and immediate grabbing space of an arrestee, including the contents of all containers, without any probable cause. Because almost all traffic infractions are arrestable offenses, police have enormous opportunity to conduct such searches incident to arrest. In the near future, these already high-stakes searches will become even more important because millions of drivers will not only possess containers that hold a few scattered papers, such as wallets or briefcases, but also iPhones—capable of holding tens of thousands of pages of personal information. If current Fourth Amendment jurisprudence is extended to its logical conclusion, officers who arrest drivers for traffic infractions will be permitted to search the call histories, text messages, email, photos, movies, and internet browsing history on iPhones with no suspicion of wrongdoing whatsoever. This Article demonstrates how the full contents and multiple applications of iPhones can be searched without a warrant or probable cause under existing U.S. Supreme Court precedent. The Article also offers approaches courts and legislatures might adopt to ensure greater protection for the soon-to-be pervasive iPhone devices. Courts and legislatures can attempt to minimize this invasion of privacy by changing the legal rules to require that searches be related to the purpose of the arrest, by limiting searches to applications that are already open, by restricting suspicionless investigation to a small number of discrete steps, or by limiting searches to data already downloaded onto the iPhone, rather than data that is merely accessible through the iPhone's internet connection.

* Associate Professor, South Texas College of Law. I am grateful to John Blevins, Dale Carpenter, Sharon Finegan, John W. Hall, Orin Kerr, Dan Markel, Usha Rodrigues, and Andrew Solomon for their helpful comments.

INTRODUCTION

Imagine that Defendant Dan is stopped by the police for driving through a stop sign. The officer thinks that Dan looks suspicious, but has no probable cause to believe Dan has done anything illegal, other than driving recklessly. Because running a stop sign is an arrestable offense and the officer is suspicious that Dan might be involved in more serious criminal activity, the officer arrests Dan for the traffic violation.

Under the search incident to arrest doctrine, officers are entitled to search the body of the arrestee to ensure that he does not have weapons and to prevent him from destroying evidence. The search incident to arrest is automatic and allows officers to open containers found on the person, even when there is no probable cause to believe anything illegal is inside. For instance, a standard search incident to arrest often turns up drugs located in a small container such as a cigarette pack. Yet, Dan does not have a cigarette pack in his pocket; instead, like millions of other technophiles, Dan is carrying an iPhone.

The officer removes the iPhone from Dan's pocket and begins to rummage through Dan's cell phone contacts, call history, emails, pictures, movies, and, perhaps most significantly, his internet browsing history. Thus, in addition to finding Dan's personal financial data and embarrassing personal information, the police also discover incriminating pictures of stolen contraband, emails evidencing drug transactions, and internet surfing of websites containing child pornography. Is all of this evidence admissible even though Dan has only been arrested for a traffic infraction and there was no probable cause (not to mention no warrant) to search the contents of his iPhone? When one considers the breadth of information located in Dan's iPhone, it would seem shocking that officers need no suspicion whatsoever in order to search through that information. Yet, that result

appears to follow from longstanding U.S. Supreme Court precedent laid down well before handheld technology was even contemplated.

* * *

The iPhone may turn out to be the most popular invention of the decade. Before its release in July 2007, crowds lined up for days to be among the first to get the device.[1] In the first three days on the market, Apple sold more than a quarter of a million iPhones[2] and the company expects to sell more than ten million devices worldwide by the end of 2008.[3] And unlike many technological releases, customer satisfaction seemed to meet or exceed expectations.[4] Thus, sales can be expected to remain strong even as competing companies follow suit with similar products.[5]

For those who have not had the opportunity to tinker with one, the iPhone is a handheld wireless device that functions as a cell phone, BlackBerry, camera, music player, and video player, while simultaneously providing internet access. In short, for those on the go, the iPhone packages multiple applications into a single device small enough to fit into a back pocket. It does not take a crystal ball to predict that such devices will be ubiquitous in the United States within a few years. Just as almost everyone for the last few years has had a conventional cell phone at their disposal, it seems likely that tens of millions of Americans will be driving around with either iPhones or a competing product in their pockets or purses within the next few years.[6]

While the iPhone is a wonderful technological innovation and its proliferation will no doubt improve everyday life, it comes with unexplored

---

1. *See Long Wait Over for iPhone Fans: Some Waited in Line Three Days for Debut*, CHI. TRIB., June 30, 2007, at 1.

2. *See* Eric Benderoff, *Apple Credits iPhone Buyers: Early Adopters of the Device Who Are Upset Over Quick Price Cut Get $100 Compensation*, CHI. TRIB., Sept. 7, 2007, at 6 ("Apple sold about 270,000 iPhones [in] the first three days.").

3. *See* Katie Hafner, *iPhone Futures Turn Out to Be a Risky Investment*, N.Y. TIMES, July 6, 2007, at C3 ("Apple has said it expects to sell as many as 10 million phones by the end of 2008."). Analysts believe that the company can sell as many as forty-five million devices worldwide by the end of 2009, due to a recent international rollout reaching 575 million potential customers. *See* Philip Elmer-Dewitt, *iPhone Rollout: 42 Countries, 575 Million Potential Customers*, FORTUNE, May 16, 2008.

4. A Westlaw search of "iPhone w/10 love" in the allnews database on July 31, 2008 yielded 461 documents.

5. Michelle Roberts, *AT&T Profit Soars: iPhone Gives Cell Provider a Boost*, AUGUSTA CHRON., July 25, 2007, at B11; Bob Tedeschi, *Navigating the New World of Cellphones, as the Options Pile Up*, N.Y. TIMES, June 19, 2008, at C6; *cf.* Troy Wolverton, *iPhone Outselling Rivals: Even So, It May Be Falling Short of High Expectations*, SAN JOSE MERCURY NEWS, Sept. 5, 2007, at C2.

6. Although there are competing handheld wireless products, for ease of exposition I will simply refer to iPhones throughout this Article.

legal repercussions. Specifically, what type of Fourth Amendment protection should such devices receive? Can they be searched without a warrant or without probable cause at a conventional traffic stop? And if so, how far can law enforcement explore the contents of the devices without violating the U.S. Constitution? In conducting a warrantless search of the handheld device, are officers limited to scanning the displayed screen of an iPhone, or are they permitted to manipulate the touch screen to open picture files or an internet browser? And once those functions are open, how deep can officers continue to look? Must the police stop when they see nothing illegal in a list of displayed emails, or can they open different email folders and begin to read messages? If the history page of an internet browser lists a website that might suggest child pornography—for instance, "www.questionable-pornography-here.com"—can the officer click on the hyperlink to bring up the website? If the website page comes up and it appears that the arrestee had used a saved password to enter the site previously, can the officer click on the "submit" button to move beyond the front page and into the salacious content?

Obviously, the framers of the Fourth Amendment could not have conceived of a handheld technological device like the iPhone,[7] and courts have not yet been called upon to answer most of the difficult questions posed by such devices.[8] Yet, current Fourth Amendment doctrine strongly suggests that the Supreme Court would authorize invasive searches of the iPhones found in pockets or purses of arrested individuals.

For nearly four decades,[9] the search incident to arrest doctrine has functioned as a bright-line rule—allowing police to search the entire person of an arrestee without getting into sticky questions of whether there was

7. A large body of Fourth Amendment scholarship focuses on unforeseen technological changes making it easier for law enforcement to investigate criminal activity. For an excellent example deviating from the view that all advances merit greater court involvement, see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004). The iPhone scenario inverts the problem, however, by placing the advanced technology in the hands (or pockets) of the one being searched, rather than the officer doing the searching.

8. A handful of courts have been asked to decide whether a search of a traditional cell phone's call history or text messages is permissible incident to arrest. With very narrow exceptions, those courts have upheld the searches as valid. *See infra* notes 71–84 and accompanying text.

9. Scholars convincingly maintain that the search incident to arrest doctrine is more than nine decades old. *See* James J. Tomkovicz, *Divining and Designing the Future of the Search Incident to Arrest Doctrine: Avoiding Instability, Irrationality, and Infidelity*, 2007 U. ILL. L. REV. 1417 (dating the search incident to arrest exception back to *Weeks v. United States*, 232 U.S. 383 (1914), and *Carroll v. United States*, 267 U.S. 132 (1925)). The modern incarnation of the doctrine can be traced to U.S. Supreme Court decisions in the 1960s and 1970s.

probable cause to open a particular container.[10] While society and technology have changed drastically over the last few decades, the search incident to arrest rule has remained static.[11] Thus, if we think of an iPhone as a container[12]—like a cigarette package or a closed box—police can open and search the contents inside with no questions asked and no probable cause required, so long as they are doing so pursuant to a valid arrest. And as scholars have long recognized, states have expansive criminal codes that give police authority to arrest for a huge number of infractions.[13] Thus, police officers with nothing more than a hunch of illegal activity may arrest an individual for a simple traffic violation[14] and proceed to search thousands of pages of private data located on the iPhone found in the arrestee's pocket.[15]

---

10. *See* United States v. Robinson, 414 U.S. 218, 235 (1973) ("The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, 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. 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."); Chimel v. California, 395 U.S. 752 (1969).

11. As explained below, the Supreme Court has drastically expanded the reach of the search incident to arrest exception. *See infra* notes 28–52 and accompanying text. As Professor James J. Tomkovicz has chronicled in his recent article, over the last few decades "the Court [has] modestly, but consistently, increased the scope of law enforcement authority to conduct automatic searches following lawful arrests." Tomkovicz, *supra* note 9, at 1441. By "static," I mean only that the Court has not accounted for new technology. On the need for new rules of criminal procedure to deal with an increasingly digital world, see Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 281–89 (2005) (arguing that existing criminal procedure law is tailored toward tangible evidence in a way not suited to dealing with digital information).

12. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538 (2005). Kerr explains that "computer searches and home searches are similar in many ways. In both cases, the police attempt to find and retrieve useful information hidden inside a closed container"; yet he also describes significant differences between computer data collection and conventional searches.

13. *See* Henry M. Hart, Jr., *The Aims of the Criminal Law*, 23 LAW & CONTEMP. PROBS. 401, 431 (1958) ("What sense does it make to insist upon procedural safeguards in criminal prosecutions if anything whatever can be made a crime in the first place?"); William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 507 (2001) ("American criminal law, federal and state, is very broad; it covers far more conduct than any jurisdiction could possibly punish. The federal code alone has thousands of criminal prohibitions covering an enormous range of behavior, from the heinous to the trivial. State codes are a little narrower, but not much."). For instance, whereas the Massachusetts Code contained 214 crimes in 1860, today the total number of offenses exceeds 500. *See id.* at 514.

14. *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318 (2001) (finding no constitutional violation in arresting a driver for failure to wear a seatbelt and searching incident to that arrest). This problem is what Professor Donald Dripps has referred to as the "Iron Triangle," in which police can pull over an automobile for pretextual reasons (so long as they can point to an almost unlimited number of traffic violations), arrest individuals for almost any low-level misdemeanor infraction, and then proceed to search the individual for contraband totally unrelated to the stop and arrest. *See* Donald A. Dripps, *The Fourth Amendment and the Fallacy of Composition: Determinacy Versus*

Part I of this Article provides an overview of the history and scope of the search incident to arrest exception to the warrant requirement. Part II reviews the handful of cases dealing with searches of conventional cell phones and pagers incident to a lawful arrest. Part III then explains the complicated problems that develop when this doctrine is applied to iPhones. Finally, Part IV offers a number of approaches that courts and legislatures could adopt to narrow the scope of warrantless searches of iPhones and similar handheld wireless devices.

I. THE SEARCH INCIDENT TO ARREST DOCTRINE AS A SEARCH FOR BRIGHT-LINE RULES

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause."[16] Yet, as any criminal procedure student knows, the Supreme Court has long recognized a slew of exceptions allowing the police to search without first procuring a warrant.[17] For purposes of this Article, there is one exception of particular significance, perhaps the most common rationale for police to search without a warrant[18]—the search incident to arrest doctrine.

The history of the search incident to arrest exception dates back to the creation of the exclusionary rule in 1914, when the Supreme Court obliquely suggested in dictum that the government has the right "to search the person of the accused when legally arrested, to discover and seize the fruits or

---

Legitimacy in a Regime of Bright-Line Rules, 74 MISS. L.J. 341, 393 (2004) ("The Iron Triangle means in practice that the police have general search power over anyone traveling by automobile.").

15. Police will also likely conduct warrantless searches of iPhones at traffic stops under the consent and automobile exceptions, though far less often than under the search incident to arrest doctrine. Under the first, police will be permitted to search the contents of an iPhone if a reasonable person would have thought his consent extended that far. *See, e.g.*, United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996) (finding that consent to search a car in which suspect was traveling extended to a search of a pager found inside the car). Under the automobile exception to the warrant requirement, police will be permitted to search the contents of the iPhone at a traffic stop if they have probable cause to believe it contains evidence of the crime they are investigating. For instance, if police have probable cause to believe the owner of the iPhone is utilizing the phone's text message function to facilitate drug dealing, police could look through the text messages of an iPhone found in a vehicle. *See* California v. Acevedo, 500 U.S. 565, 581 (1991) (allowing police to open containers in an automobile without a warrant).

16. U.S. CONST. amend. IV.

17. Exceptions to the Fourth Amendment's warrant requirement are so pervasive and disorganized that Professor Akhil Amar has referred to Fourth Amendment jurisprudence as "a sinking ocean liner—rudderless and badly off course." Akhil Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759 (1994).

18. *See* WAYNE R. LAFAVE, 3 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 5.2(c) & n.55 (2007) (describing the search incident to arrest as probably the most common type of police search).

evidences of crime."[19] Although the Court alluded to such searches in that case and a handful of other early decisions,[20] the doctrine's modern conception was the 1969 decision in *Chimel v. California*.[21]

In *Chimel*, police arrested a suspect in his home for burglary and proceeded to search the entire three-bedroom house, as well as the attic and garage, for proceeds of that burglary.[22] While the Court found this warrantless search to be unconstitutionally broad, it nevertheless recognized that police can search suspects incident to arrest in narrower circumstances.[23] The Court explained that a search incident to arrest must be limited to a search for weapons that an arrestee could use against the officer and to prevent an arrestee from concealing or destroying evidence.[24] The Court concluded that a search for weapons and evidence must be limited to the arrestee's person and the area within his immediate control from which he might gain possession of a weapon or destroy evidence.[25] The Court specifically rejected the contention that police could search areas beyond that from which an arrestee could grab a weapon or evidence.[26]

A few years after *Chimel*, the Supreme Court addressed the question of whether police could open closed containers located on an arrestee's person. In *United States v. Robinson*,[27] police arrested a suspect for operating a motor vehicle with a revoked license.[28] While conducting a search incident to arrest, the officer felt an object in Robinson's coat pocket but could not tell what it was.[29] The officer reached into the pocket and pulled out a "crumpled up cigarette package."[30] Still not sure what was in the package, the officer opened it and discovered capsules of heroin.[31] In rejecting Robinson's challenge to the search, the Court made clear that officers conducting a search incident to arrest can open and search through all items on an arrestee's person, even if they are in a closed container, and even if the officers have no suspicion that the contents of the container are illegal.[32] The Court explained

19. Weeks v. United States, 232 U.S. 383, 392 (1914).
20. For a recent and excellent discussion of the history of the search incident to arrest doctrine, see Tomkovicz, *supra* note 9, at 1421–45.
21. 395 U.S. 752 (1969).
22. *Id.* at 754.
23. *Id.* at 763, 768.
24. *Id.* at 763.
25. *Id.*
26. *Id.* at 768.
27. 414 U.S. 218 (1973).
28. *Id.* at 220.
29. *Id.* at 223.
30. *Id.*
31. *Id.*
32. *Id.* at 235–36.

that the search incident to arrest doctrine does not require case-by-case adjudication and that there need not be analysis of each step of the search to determine whether it was necessary to prevent the arrestee from acquiring weapons or destroying evidence.[33] Rather, *Robinson* made clear that searches of the arrestee's person and the containers thereon can be conducted automatically incident to an arrest. The Court's decision thus created a bright-line rule.

The Court's affinity for bright-line rules became even clearer eight years later in *New York v. Belton*.[34] In *Belton*, the officer stopped a car for speeding and, upon smelling marijuana, arrested the occupants.[35] With the occupants away from the vehicle, the officer then searched the passenger compartment of the car and found a jacket in the backseat. The officer unzipped the pockets of the jacket and found cocaine.[36] Praising its decision in *Robinson*, the Court reaffirmed that police officers must be afforded "a straightforward rule, easily applied, and predictably enforced."[37] Lamenting that there was not yet such straightforward rule for the search of the interior of a car at a traffic stop, the Court adopted another bright-line rule permitting the search of the entire passenger compartment of an automobile when an occupant of the car is lawfully arrested.[38]

Just as in *Robinson*, the Court made clear that the bright-line rule would apply even if there were no chance that an arrestee could break free of his restraints to grab a weapon or destroy evidence in the passenger compartment of the car. The Court further explained that the search of the passenger compartment included any containers found therein, whether open or closed, and irrespective of whether they could contain a weapon or evidence.[39] The *Belton* decision marked a considerable expansion of the search incident to arrest doctrine.[40]

---

33. *Id.* at 235.
34. 453 U.S. 454 (1981).
35. *Id.* at 455–56.
36. *Id.* at 456.
37. *Id.* at 459.
38. *Id.* at 460.
39. *Id.* at 461. The Court did not make clear in *Belton*, nor has it in any subsequent cases, whether locked containers in an automobile can be opened incident to arrest. For a survey of the lower court authority, see LAFAVE, *supra* note 18, § 7.1(c) n.99. Likewise, the Court has never squarely addressed the question of whether the trunk portion of an SUV, station wagon, or hatchback qualifies as being part of the passenger compartment of the vehicle. *See, e.g.*, Sellman v. State, 828 A.2d 803, 818 (Md. 2003) (describing the issue of whether a hatchback is in the passenger compartment as a "fact-bound question"). For a long list of cases reaching different conclusions on this issue, see LAFAVE, *supra* note 18, § 7.1(c) n.96.
40. *See* Tomkovicz, *supra* note 9, at 1437 (explaining that the *Belton* Court "was instigating a new era of expansion for search incident authority").

In the Court's last significant search incident to arrest decision, the 2004 decision in *Thornton v. United States*,[41] an automobile was again the focus of attention.[42] Unlike the occupant in *Belton*, the *Thornton* case involved a driver who had already exited and walked away from his vehicle before being approached by police.[43] After Thornton was arrested for drug possession, the officer then proceeded to his vehicle and searched the passenger compartment incident to arrest. The officer found a handgun under the seat, which led to a charge of possessing a firearm in furtherance of a drug-trafficking crime.[44] The Court once again stressed the need for a "clear rule, readily understood by police officers and not depending on differing estimates of what items were or were not within reach of an arrestee at any particular moment."[45] In rejecting Thornton's suppression argument, the Court extended the *Belton* rule to permit a full-scale search of the passenger compartment of a vehicle incident to the arrest of a "recent occupant" of a vehicle.[46]

The Court's decisions over the last forty years suggest that the search incident to arrest exception to the warrant requirement should be interpreted expansively. Indeed, in *Belton*, the Court specifically stated that "container" should be interpreted broadly to include "any object capable of holding another object. It thus includes closed or open glove compartments, consoles, or other receptacles located anywhere within the passenger compartment, as well as luggage, boxes, bags, clothing, and the like."[47] Consistent with this guidance, lower courts have taken a broad approach and upheld searches of numerous small containers incident to arrest, such as wallets,[48] envelopes,[49] and aspirin

41. 541 U.S. 615 (2004).
42. *Id.* at 617–19.
43. *Id.* at 618.
44. *Id.*
45. *Id.* at 623.
46. *See id.* at 623–24. Ironically, the Court's celebration of a bright-line approach makes little sense when the Court has provided no guidance as to who qualifies as a "recent occupant" of a vehicle. *See* George Dery & Michael J. Hernandez, *Turning a Government Search Into a Permanent Power:* Thornton v. United States *and the "Progressive Distortion" of Search Incident to Arrest*, 14 WM. & MARY BILL RTS J. 677, 698 (2005) ("The stage is thus now set for needless litigation as to the boundaries of *Thornton*'s not-so-bright-line rule. Attorneys in the courts and officers on the beat will struggle in their attempts to determine who qualifies as a 'recent occupant' of a vehicle. The spawning of case after case attempting to clarify the outer boundaries of *Thornton*'s time and space rule creates the very confusion *Belton* originally aimed to avoid.").
47. New York v. Belton, 453 U.S. 454, 460 n.4 (1981).
48. *See, e.g.*, United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993) (permitting the searching of a wallet and photocopying of an address book incident to arrest); United States v. Hatfield, 815 F.2d 1068, 1071–72 (6th Cir. 1987) (upholding the search of a wallet incident to arrest as well as the admission of lock picks found in the wallet); State v. Winston, 295 S.E.2d 46 (W. Va. 1982) (upholding the search of a wallet).
49. *See, e.g.*, United States v. McCrady, 774 F.2d 868, 872 (8th Cir. 1985) (upholding the search of an envelope found in a locked glove compartment).

bottles.[50] Although some state courts have interpreted their own constitutions and criminal codes to be more restrictive than the Constitution,[51] most lower courts have not hesitated to apply the search incident to arrest doctrine to new situations unforeseen by the Supreme Court.[52]

II. BRIGHT-LINE RULES IN AN ERA OF PAGERS AND CELL PHONES

The Supreme Court's decisions in *Robinson*[53] and *Belton*[54] made clear that, incident to a lawful arrest, officers can open containers located on a person or in their immediate grabbing space without having any independent probable cause to search those containers.[55] 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. These courts have been forced to confront whether the search incident to arrest doctrine—designed with a world of tangible evidence in mind—should apply to data digitally contained in electronic devices. Most courts have upheld such searches.

The earliest of these electronic data cases (and consequently the most primitive of the technology at issue) was a 1993 decision from the Northern District of California dealing with a pager found on an arrestee.[56] The defendant, Chan, was arrested as part of a drug sting operation and police found a pager on Chan's person.[57] The police then activated the pager's memory function and retrieved telephone numbers stored inside it.[58] Two numbers found in the pager linked Chan to the drug sting the police were

50. *See* Daniels v. State, 416 So.2d 760 (Ala. Crim. App. 1982).

51. *See, e.g.*, State v. Stroud, 720 P.2d 436 (Wash. 1986) (en banc) (relying on a state constitution to conclude that the police may not search a locked glove compartment incident to arrest without procuring a warrant).

52. *See, e.g.*, *supra* notes 48–50.

53. United States v. Robinson, 414 U.S. 218 (1973).

54. New York v. Belton, 453 U.S. 454 (1981).

55. *See* Wayne A. Logan, *An Exception Swallows a Rule: Police Authority to Search Incident to Arrest*, 19 YALE L. & POL'Y REV. 381, 381 (2001) ("Compared to Fourth Amendment jurisprudence more generally, with its well-earned reputation for complexity and variability, the search incident to arrest exception to the Amendment's warrant requirement would appear an oasis of consistency.").

56. United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993).

57. *Id.* at 533.

58. *Id.*

conducting.[59] Chan contended that he had a reasonable expectation of privacy in the pager and that activating it amounted to a search that required a warrant.[60]

The court sided with Chan in part by agreeing that a pager is analogous to a closed container and that individuals have a reasonable expectation of privacy in the contents of electronic containers.[61] However, the court ultimately concluded that because the search of the pager came on the heels of a lawful arrest of Chan, a warrantless search was permitted under the search incident to arrest doctrine.[62] Citing *Belton* and *Chimel*,[63] the court concluded that all containers can be searched incident to a lawful arrest, including electronic containers.[64] Moreover, the court considered and specifically rejected as irrelevant the fact that Chan could not retrieve a weapon from the pager nor plausibly destroy any evidence from the pager.[65] Accordingly, the evidence found when the officer turned on and searched the pager was admissible.[66]

Over the next few years, a handful of other courts were called upon to analyze the question raised in *Chan* and these courts likewise permitted the search of the contents of a pager incident to arrest.[67] These courts reiterated that the search incident to arrest exception allows police to open all containers on a person and further explained that pagers are analogous to a wallet or address book, which courts have long permitted police to search incident to a lawful arrest.[68] One court further recognized that it was especially important to search pagers quickly because an incoming page could destroy existing numbers currently stored in the pager's memory.[69]

---

59. *Id.*
60. *Id.*
61. *Id.* at 535.
62. *Id.* at 535–36.
63. Chimel v. California, 395 U.S. 752 (1969).
64. *Chan*, 830 F. Supp. at 536.
65. *Id.*
66. *Id.* at 536.
67. *See* United States v. Hunter, No. 96-4259, 1998 WL 887289, at *3 (4th Cir. Oct. 29, 1998) (per curiam) (upholding the retrieval of numbers from a pager); United States v. Ortiz, 84 F.3d 977, 983–84 (7th Cir. 1996) (same); United States v. Stroud, No. 93-30445, 1994 WL 711908, at *2 (9th Cir. Dec. 21, 1994) (same); United States v. Diaz-Lizaraza, 981 F.2d 1216, 1223 (11th Cir. 1993) (holding that it is permissible to insert batteries and reactivate the beeper so that it may be called after an arrest); United States v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996) (upholding the retrieval of numbers from a pager); United States v. Lynch, 908 F. Supp. 284, 290 (D.V.I. 1995) (same).
68. *See Lynch*, 908 F. Supp. at 288.
69. *See Ortiz*, 84 F.3d at 984; *see also* United States v. Zamora, No. 1:05CR250(WSD), 2006 WL 418390, at *4 (N.D. Ga. Feb. 21, 2006) (recognizing with respect to cell phones that they are dynamic and that "[w]ith each call is the risk that a number stored would be deleted").

The era of pagers has all but ended, making way for the age of cell phones. At first, cell phones were used primarily for phone calls, but in recent years text messaging has become a very commonly used feature as well.[70] To date, fewer than a dozen courts have addressed searches of cell phones incident to arrest. The Fifth Circuit's recent 2007 decision in *United States v. Finley*[71] is representative. Police arrested Finley after a staged drug sale.[72] The police then searched Finley incident to arrest and found a cell phone in his pocket.[73] One of the investigating officers searched through the phone's records and found text messages that appeared to relate to drug trafficking.[74] One incoming text message said, "So u wanna get some frozen agua," a common term for methamphetamine.[75] Another text message said, "Call Mark I need a 50," a likely reference to asking for fifty dollars' worth of narcotics.[76] Finley was convicted of aiding and abetting drug possession with intent to distribute.[77]

On appeal, Finley contended that the search of his cell phone was unlawful. The Fifth Circuit rejected Finley's contention that the cell phone could be seized but not searched.[78] Relying on the conventional search incident to arrest caselaw—namely *United States v. Robinson* and *New York v. Belton*[79]—the court explained that "police officers are not constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial."[80] The court further explained that police can open containers found on the arrestee's person and saw no reason why the doctrine should not be extended to text messages contained in a cell phone.[81]

In short, the Fifth Circuit did not recognize any conceptual difference between searching a person's body or physical containers on that body for

70. *See* David Hayes, *The Cell Phone Is Called on to Do It All—A Wireless Wonder: With Features Ad Infinitum, It's Getting to Be Like Your Personal Computer*, KAN. CITY STAR, Oct. 30, 2005, at A1 ("After years of relatively slow growth, U.S. wireless subscribers now are sending billions of text messages each month.").
71. 477 F.3d 250 (5th Cir. 2007).
72. *Id.* at 253–54.
73. *Id.* at 254.
74. *Id.*
75. *Id.* at 254 n.2.
76. *Id.*
77. *Id.* at 255.
78. *See id.* at 260.
79. *See supra* text accompanying notes 28–40.
80. *Finley*, 477 F.3d at 259–60.
81. *See id.* at 260.

drugs and searching electronic equipment for digital information. A handful of district courts have reached the same conclusion as the Fifth Circuit and admitted evidence seized from cell phones.[82]

To be sure, two lower courts have suppressed evidence found on cell phones pursuant to a search incident to arrest. Yet, those decisions rested primarily on grounds that the search took place too long after the arrest to be considered a contemporaneous search incident to arrest.[83]

Perhaps the reason for the lack of contrary authority is that searching a conventional cell phone or pager incident to arrest is relatively easy to square with precedent that permits police to search tangible containers found on an

---

82. *See* United States v. Valdez, No. 06-CR-336, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008) (upholding the search of a cell phone's address book and call logs incident to arrest, though noting that "we can leave for another day the propriety of a broader search equivalent to the search of a personal computer"); United States v. Curry, No. 07-100-P-H, 2008 U.S. Dist. LEXIS 5438, at *30–31 (D. Me. Jan. 23, 2008) (upholding the search of a cell phone for call logs from a drug informant); United States v. Lottie, No. 3:07-CR-51-AS, 2007 WL 4722439, at *4 (N.D. Ind. Oct. 12, 2007) (upholding the search of a cell phone primarily on exigency grounds but arguably under the search incident to arrest exception as well); United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1275–76 (D. Kan. 2007) (upholding the search of a cell phone for numbers of outgoing and incoming calls); United States v. Murphy, No. 1:06CR00062, 2006 WL 3761384, at *4 (W.D. Va. Dec. 20, 2006) (upholding the search of a cell phone's text messages); United States v. Diaz, No. CR 05-0167 WHA, 2006 WL 3193770, at *4–5 (N.D. Cal. Nov. 2, 2006) (upholding the recording of names and numbers in an address book and recording messages); United States v. Zamora, No. 1:05 CR 250 WSD, 2006 WL 418390, at *5 (N.D. Ga. Feb. 21, 2006) (upholding the search of a cell phone for numbers of outgoing and incoming calls); United States v. Cote, No. 03 CR271, 2005 WL 1323343, at *6 (N.D. Ill. May 26, 2006) (upholding the search of a cell phone's call log, phone book, and wireless web inbox); United States v. Brookes, No. CRIM 2004-0154, 2005 WL 1940124, at *3 (D.V.I. June 16, 2005) (upholding the search of numbers in a cell phone and pager); United States v. Parada, 289 F. Supp. 2d 1291, 1303–04 (D. Kan. 2003) (upholding the search of stored numbers to prevent destruction of evidence).

83. *See* United States v. Park, No. CR-05-375SI, 2007 WL 1521573, at *11–12 (N.D. Cal. May 23, 2007); United States v. Lasalle, No. 07-00032 SOM, 2007 WL 1390820, at *7–8 (D. Haw. May 9, 2007); *cf.* United States v. Carroll, 537 F. Supp. 2d 1290, 1299 (N.D. Ga. 2008) (expressing skepticism at search incident to arrest of a BlackBerry when the suspect surrendered at the police station, but ordering further briefing before deciding the issue). In *Park*, the court stated that "due to the quantity and quality of information that can be stored on a cellular phone, a cellular phone should not be characterized as an element of [an] individual's clothing or person, but rather as a possession within an arrestee's immediate control that has fourth amendment protection at the station house." 2007 WL 1521573, at *9 (internal quotation marks omitted). This approach conceivably makes sense if the court is saying that the search of the cell phone was impermissible because it occurred too long after the arrest. But if the court is contending that the search was instead invalid because it was a search of the possessions within the arrestee's immediate control rather than on his person, it is difficult to square with the Supreme Court's decision in *New York v. Belton*, 453 U.S. 454, 462–63 (1981), and other cases that repeatedly reaffirm that a search incident to arrest extends to the person's area of immediate control. Perhaps for this reason, the *Park* decision stands contrary to eleven other decisions upholding the searches of cell phones incident to arrest and another seven decisions permitting the search of pagers incident to arrest. *See* sources cited *supra* notes 67, 82.

arrestee.[84] A cell phone's memory of incoming and outgoing calls, as well as its text messages, can easily be analogized to an address book or a letter in an envelope.[85] Much as the traditional search incident to arrest cases permit police to open a wallet, take out a letter, and read it before the arrestee has an opportunity to destroy the evidence, it also makes sense to allow the police to review electronic call histories and text messages in a cell phone.[86] An arrestee familiar with the functions of his cell phone could just as easily delete text messages or call logs as he could tear up a letter or an incriminating list of addresses on a piece of paper.

III. THE STAKES AND LIKELY RESULTS WHEN THE iPHONE MEETS THE SEARCH INCIDENT TO ARREST DOCTRINE

To date, no court has been called upon to address the constitutionality of searching an iPhone. In light of the handful of cell phone and pager cases discussed by the lower federal and state courts,[87] it might seem that there is no difference in searching an iPhone. Just as text messages stored on a cell phone are evidence within a digital container, it would seem that call histories, emails, and pictures on an iPhone would simply be characterized as evidence stored in a (larger) digital container. As a conceptual matter, there is no real difference between a crumpled up cigarette package, an early-generation cell phone, and an iPhone with a much larger memory. Yet, this is cause for concern because no matter what theoretical similarities exist between

84. More puzzling is why there are so few reported cases of police searching cell phones or pagers incident to arrest. One possibility is that such searches are regularly conducted, but no evidence is found. This result would tend to make sense because unless police are actively investigating a case, a series of pager numbers or an address book of contacts may not be incriminating without further information. While text messages might be more immediately incriminating, it is only in the last few years that the text message craze has begun in earnest. *See* David Ovalle, *Texting Gets Dicey With Booze*, MIAMI HERALD, June 13, 2005, at 1A. A related possibility is that police are not yet regularly engaged in searching cell phones and electronic devices, possibly because they are so accustomed to searching for tangible evidence such as drugs. A third explanation is that police are conducting such searches but that defendants plead guilty rather than continuing to challenge the search and risk conviction. In any event, the paucity of cases is not likely to last for long as iPhones will likely become an attractive target for police searching for evidence of illegal activity.

85. *See, e.g.*, United States v. Rodriguez, 995 F.2d 776 (7th Cir, 1993) (upholding the search of a wallet and photocopying of an address book incident to lawful arrest); United States v. Meriwether, 917 F.2d 955, 958 (6th Cir. 1990) ("The digital display pager, by its very nature, is nothing more than a contemporary receptacle for telephone numbers.").

86. *See, e.g.*, United States v. Lynch, 908 F. Supp. 284 (D.V.I. 1995) (refusing to suppress data found from search of pager incident to arrest because the search of a pager for phone numbers is just like the search of a wallet or address book found on a person); *see also Cote*, 2005 WL 1323343, at *6 (refusing to suppress data found on a cell phone for the same reason).

87. *See supra* notes 56–83 and accompanying text.

an iPhone and a conventional cell phone (or a cigarette package for that matter), the former stores tremendously more information and in a very different way. The differences can be demonstrated by thinking about how many steps or searches police might be able to take with respect to the new and old technology.

The cell phone and pager cases decided by courts in the last few years are what we might call first level cases because they do not require in-depth searching to obtain evidence. Police need to push only a limited number of buttons in order to reach pager numbers and only a few additional buttons to retrieve text messages. If we think of each step that police must take to retrieve information as a separate search, then reviewing pager numbers might amount to only two levels of searches: first, pushing the memory button for the list of recent pages; and second, scrolling through the numbers to find the incriminating calls. Reviewing text messages on a cell phone can be conceptualized as three separate searches: (1) opening the text message function; (2) opening the list of received text messages; and (3) opening and reading a particular text message. This is similar to the searches in *Robinson*[88] where the police officer (1) felt the cigarette package; (2) pulled out the package; and (3) opened the package.

Put simply, the data on early-generation cell phones is limited in its amount and usefulness, and police officers will either find the evidence or run into a dead end rather quickly. Accordingly, the degree of privacy invasion can be measured by the number of steps an officer must take to retrieve the incriminating information. In the cases decided to date dealing with text messages and pagers, this number has been small because those devices have few, relatively simple functions capable of storing electronic data. The same can be said for tangible evidence such as cigarette packages, purses, wallets, or suitcases.

The iPhone drastically changes this situation for two reasons. First, the iPhone stores tremendously more information—thereby providing law enforcement with access to information that the typical arrestee would otherwise be incapable of carrying in his pocket. In addition to the text messages, contact information, and call histories found on conventional phones, iPhones also contain an iPhoto application. This application holds far more pictures than could be stored on a conventional cell phone and displays them in much clearer detail. Similarly, the iPhone's easily accessible email application makes it simple to access thousands of new, saved, and sent email messages. The iPhone enables users to store thousands of audio and

88. United States v. Robinson, 414 U.S. 218 (1973).

video files. Music, books, and videos ranging from classical music to potentially obscene pornographic videos can be accessed with the touch of a few buttons.

Second, and perhaps with greater ramifications than the data stored on the actual device, the iPhone provides a mechanism for accessing information via the internet. The iPhone's internet browser is just like the one found on a standard computer; it can dial out and retrieve information stored remotely with an internet service provider. An example is instructive.

Imagine that an officer arrests an individual following a lawful traffic stop and finds an iPhone in the driver's pocket. The officer then takes the following steps: (1) activates the touch screen to view the phone's contents; (2) clicks on the internet browser icon; (3) clicks on the toolbar to find the bookmarks link; (4) finds a suspicious-looking bookmark labeled "porn pictures"; (5) clicks on that particular bookmark to bring up the webpage; (6) sees that the webpage contains a series of icons including a "members" button and clicks on that image; (7) brings up the "members" page which has a saved account number and password already entered; (8) clicks on the "submit" button which utilizes the saved account information and password to bring up the content of the website; (9) sees that, in addition to pictures, the website also has a message function and the account owner has two new messages; and (10) clicks on the message icon and brings up the two new messages, both of which detail an incriminating conversation about exchanging pictures of underage children.

Or imagine how an officer could utilize the internet to circumvent an arrestee's privacy protections, such as if an arrestee had password-protected his iPhoto application to hide his photographs. After (1) turning on the iPhone; and (2) attempting to open the iPhoto application, the officer discovers that the application is password-protected and cannot be opened.[89]

89. The Supreme Court has not clearly determined whether officers can open a locked container, such as a glove compartment, during a search incident to arrest. Many courts have permitted such searches. *See, e.g.*, United States v. Woody, 55 F.3d 1257, 1269–70 (7th Cir. 1995); State v. Fry, 388 N.W.2d 565, 577 (Wis. 1986). There is contrary authority however. *See* State v. Stroud, 720 P.2d 436 (Wash. 1986) (en banc) (relying on a state constitution to conclude that police may not search a locked glove compartment incident to arrest without procuring a warrant).

In a recent decision, a federal magistrate concluded that it would violate a defendant's Fifth Amendment protection against self-incrimination to be compelled to provide the government with the password that encrypted a laptop found during a search at the Canadian border. *See In re* Boucher, No. 2:06-mj-91, 2007 WL 4246473, at *6 (D. Vt. Nov. 29, 2007). For criticism of the decision, see Sherry F. Colb, *Does the Fifth Amendment Protect the Refusal to Reveal Computer Passwords? In a Dubious Ruling, A Vermont Magistrate Judge Says Yes*, FINDLAW'S WRIT, Feb. 4, 2008, http://writ.news.findlaw.com/colb/20080204.html. On the rise of computer searches at the border, see Adam Liptak, *If Your Hard Drive Could Testify . . .* , N.Y. TIMES, Jan. 7, 2008, at A12 (discussing

The officer might then (3) activate the internet browser; (4) click on the browsing history to see what webpages the owner had visited; (5) click on the history link that referenced the arrestee's web-based email account—for instance, Yahoo! or Gmail; (6) read through the folders in the email account until finding one labeled "personal information"; (7) read through the messages in that folder until finding an email with the subject "passwords"; (8) open that email and retrieve the password for the iPhoto application; (9) close the internet browser and again click on the iPhoto application; (10) enter the password found in the email, thus opening the iPhoto application; (11) search through the folders in the iPhoto application, finding the most suspiciously labeled folder—for instance, "kid pics"; and (12) open that folder and search through all of the pictures inside that folder.

Countless other complicated scenarios could likewise be envisioned. As the scenarios become more convoluted, it becomes harder to analogize them to a closed container or a wallet containing an address list. And indeed, the iPhone provides access to information that would almost never before be found in arrestees' pockets or immediate grabbing space, but which could potentially subject them to criminal prosecution. For instance: (1) bank statements accessed via the saved password on your banking website[90] or (2) MySpace or Facebook webpages that have personal data, pictures, contacts, and exchanges of messages, might be rich sources of incriminating information.[91]

---

emerging cases in which the government compares searching a hard drive to rummaging through a suitcase); Ellen Nakashima, *Clarity Sought on Electronic Searches: U.S. Agents Seize Travelers' Devices*, WASH. POST, Feb. 7, 2008, at A1 (describing suspicionless searches of electronic data of international air travel passengers at the border, including requiring passengers to enter passwords into their laptops, copying the histories of websites visited on those laptops, reviewing documents saved in Microsoft Word, compiling lists of phone numbers in cell phones, and demanding to see emails). For a scholarly assessment of the border searches, see Christine A. Coletta, Note, *Laptop Searches at the United States Borders and the Border Search Exception to the Fourth Amendment*, 48 B.C. L. REV. 971 (2007).

90. "Banking data is a fertile source of evidence for prosecution." *See, e.g.*, Cassondra Kirby, *Two Lexington Women Indicted on Money Laundering Charges: Accused of Bilking Millions for Luxuries*, LEXINGTON-HERALD LEADER, Dec. 3, 2005, at B4 (recounting how a defendant denied money laundering charges but prosecutors said that "her bank records show otherwise").

91. Prosecutors increasingly are finding MySpace and Facebook profiles to be a source of evidence. *See* Erica Perez, *Getting Booked by Facebook: Police Are Finding, With Help of Networking Sites, That Students Are Incriminating Themselves Online*, MILWAUKEE J. SENTINEL, Oct. 3, 2007, at A1 ("Facebook.com and MySpace.com are the newest crime-busting tools in a police officer's repertoire, particularly for campus police, who are using the sites to investigate student crimes and violations and gather information about where students live and whom they know. In some cases, the information they find is making its way into court."); Michael A. Scarcella, *14 Are Targeted in Gang Sweep: Accused of Ties to Manatee's SUR 13, and Facing Racketeering Charges*, SARASOTA HERALD TRIB., July 7, 2007, at B1 ("A new trend in law enforcement has police surfing MySpace pages on the Internet for evidence in criminal cases."); Joseph Person, *Uploading Zone a Risky Place to*

In searching for incriminating information, officers will no doubt come into contact with extremely sensitive personal information that is not remotely illegal but which is nevertheless highly embarrassing. For instance, by searching an arrestee's internet browsing history, police might stumble across chat rooms demonstrating that the arrestee has unusual sexual proclivities. Or police might discover that the arrestee is homosexual and is trying to keep that information secret from her family or employer. If the arrestee is a politician, the ramifications would be particularly devastating if police were to discover from his emails that he has been having an affair or that he made derogatory comments about other political figures. Additionally, an arrestee's internet browsing history or his bookmarked webpages might lead to a health insurance website that includes bills for a serious or embarrassing medical condition. The list of scenarios is endless. And while such embarrassing, but not incriminating, information probably would not be admissible in a prosecution, its discovery would cause emotional distress. Moreover, while noncriminal information should never be released beyond the initial traffic stop if it has no place in a prosecution, it sometimes manages to find its way into the public domain.[92]

In sum, the search incident to arrest doctrine permits police to search the contents of any container found on the arrestee, including electronic receptacles of digital information. Courts already have held that the doctrine applies to the electronic contents of pagers and cell phones and permits the copying of phone numbers and the reading of text messages. If courts take the next step—and they almost certainly will—by applying the search incident to arrest doctrine to the iPhone, officers will be in a position to review incoming and outgoing call histories, scan contact lists, read thousands of emails, view nearly limitless numbers of color photographs and movies, listen to voicemail at the touch of the button, and view the internet websites that an arrestee has visited.

Park, STATE, May 28, 2006, at C1 (describing college athletes who videotaped their underage drinking and posted it online on Facebook).

92. *See, e.g.*, Brian Rogers & Matt Stiles, *County DA Wants Court to Seal Revealing Emails: Correspondence Brings to Light His Close Relationship With Secretary*, HOUSTON CHRON., Dec. 26, 2007, at A1 (describing romantic emails from the Harris County District Attorney to his secretary that were intended to be produced under seal as part of a civil rights lawsuit but that were nevertheless released into the public domain).

IV. DISENTANGLING THE iPHONE FROM A BRIGHT-LINE RULE: POSSIBLE APPROACHES TO CABINING THE SEARCH INCIDENT TO ARREST DOCTRINE

The difference between the data found on a cell phone and an iPhone is dramatic but, at present, the Fourth Amendment and its search incident to arrest doctrine make no distinction. In this Part, I consider what approaches, if any, courts and legislatures might adopt to address this problem.

A. Change Nothing: The Search Incident to Arrest Rule Works Well, So Changing It to Account for New Technology Is Not a Good Idea

While it is undoubtedly troubling to permit suspicionless searches of the many applications of an iPhone, one could plausibly argue that attempting to craft a rule disallowing such searches would be worse. At present, the search incident to arrest doctrine is a bright-line rule that is easy for police officers to understand and apply. And courts faced with a search incident to arrest usually have an easy time determining whether the officers' actions were permissible. Compare this to the rest of Fourth Amendment law, which is riddled with exceptions, caveats, and uncertainty.[93] Indeed, the typical Fourth Amendment section of a criminal procedure textbook is at least twice as long as the Fifth Amendment section.[94] Carving out an exception to the search incident to arrest doctrine to deal with the iPhone might afford more privacy protection to a device that is capable of holding reams of personal information that individuals reasonably expect to be protected against government intrusion, but at what cost? There is a colorable argument

93. *See* Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473 (1985) ("In fact, the exceptions [to the Fourth Amendment's warrant requirement] are neither few nor well-delineated. There are over twenty exceptions to the probable cause or the warrant requirement or both."); *see also* California v. Acevedo, 500 U.S. 565, 582 (1991) (Scalia, J., concurring in the judgment) (contending that the Fourth Amendment's warrant requirement has "become so riddled with exceptions that it [is] basically unrecognizable").

94. *See, e.g.*, JOSHUA DRESSLER & GEORGE C. THOMAS, III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES, AND PERSPECTIVES (2d ed. 2003); MARC L. MILLER & RONALD F. WRIGHT, CRIMINAL PROCEDURES: CASES, STATUTES, AND EXECUTIVE MATERIALS (3d ed. 2007). Justice Sandra Day O'Connor made this very point in opposing a public safety exception to the *Miranda* doctrine. *See* New York v. Quarles, 467 U.S. 649, 663–64 (1984) (O'Connor, J., concurring in the judgment and dissenting in part) ("The end result will be a finespun new doctrine on public safety exigencies incident to custodial interrogation, complete with the hair-splitting distinctions that currently plague our Fourth Amendment jurisprudence.").

that any benefit to be had from a new rule would be outweighed by muddling one of the few areas of Fourth Amendment law that is currently intelligible.[95]

Moreover, as Professor Orin Kerr has explained, not every change in technology necessitates changing the rules of constitutional criminal procedure to be more protective of individuals.[96] The same courts that have made a mess of current Fourth Amendment law may lack the institutional competence to draft rules for emerging technology. As Professor Kerr has explained, "[j]udges cannot readily understand how the technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical."[97]

While I do not desire that Fourth Amendment law be made any more complicated, ultimately, I am not convinced that courts should restrain themselves by applying an ill-fitting bright-line rule to the iPhone.[98] I see two primary reasons.

First, the major informal constraints typically facing police in executing searches are not present with respect to the iPhone. As Professor Bill Stuntz has explained, police investigations are ordinarily constrained by limited resources and limited time.[99] New technology is typically expensive in law and economic terms. Thus, while the Supreme Court has held that there is no Fourth Amendment search when police observe backyards from helicopters or planes,[100] that has not enabled police to do so with impunity. Police departments typically cannot afford to buy or rent helicopters, nor do they

95. By "intelligible" I do not mean to suggest that the search incident to arrest doctrine is sound or logical. To the contrary, I am in agreement with Professor James J. Tomkovicz's recent criticism that the bright-line rule allows police to conduct an automatic search incident to arrest when there is no conceivable way that the arrestee could grab a weapon or destroy evidence. *See* Tomkovicz, *supra* note 9, at 1452–53.

96. *See* Kerr, *supra* note 7, at 805.

97. *Id.* at 858–59.

98. Professor Orin Kerr might very well agree because he has explained that

> [his] argument applies only when technologies are in flux. [His] concern is the institutional competence of courts and legislatures when facts are changing quickly. As a result, [his] interest is not whether a given case involves a "technology" in an absolute sense, but rather whether the basic assumptions upon which rules are generated are likely to remain constant or to shift in unpredictable ways.

See id. at 859.

99. *See* William J. Stuntz, *Race, Class, and Drugs*, 98 COLUM. L. REV. 1795, 1821 (1998) (explaining how it is lower cost for police to search for drugs in poor neighborhoods where transactions are conducted on the street while searching for drugs in upscale neighborhoods costs more because transactions are behind closed doors and more secretive).

100. *See* Florida v. Riley, 488 U.S. 445 (1989) (plurality opinion) (holding that warrantless aerial surveillance does not constitute a Fourth Amendment search); California v. Ciraolo, 476 U.S. 207 (1986) (same).

have the time to file flight plans, spend hours in the air, and simply look around without being guided by some particularized suspicion.[101]

With respect to the iPhone, however, the new technology inverts the typical state of affairs because it is the individual, not the police officer, who has the new technology. Moreover, unlike flyovers or costly thermal imaging devices,[102] the technology is everywhere. Apple expects to sell more than ten million iPhones by the end of 2008.[103] In the next decade, millions of drivers will have an iPhone or a substantially similar device in their pockets during many of the nearly thirty million traffic stops that occur each year.[104] And unlike helicopters or thermal imagers, the cost to police in searching is almost nil. A study by the Bureau of Justice Statistics found that police searched the car or the driver in 6.6 percent of the twenty-seven million traffic stops that occurred in a particular year.[105] Upwards of 470,000 searches were conducted incident to arrest at a traffic stop.[106] If police are already conducting such searches incident to arrest, they can easily take a few extra moments to seize the iPhone, turn it on, and start rummaging through its files and applications.[107]

---

101. *See* Craig Wong, *Fleet Expansion Chops Earnings*, TORONTO STAR, Sept. 15, 2006, at F5 (noting that the average cost of a new helicopter is roughly CAD $500,000); Laura Fasbach, *Should N.J. Governors Go by Chopper? Corzine Smash-Up Prompts a New Look at Air Travel*, RECORD, Apr. 23, 2007, at A1 (explaining that a state police helicopter costs about $2800 an hour to pay for fuel and the pilot). As one British police officer explained, "we never go on a [helicopter] job without the economics of it being evaluated." Gerry Hold, *Police Helicopter Costs Pounds: 19-a-Minute to Run*, S. WALES ECHO, June 26, 2006, at 6.

102. In *Kyllo v. United States*, 533 U.S. 27 (2001), the Supreme Court held that the use of a thermal imaging device to measure heat coming from a house amounted to a Fourth Amendment search requiring probable cause and a warrant. Nevertheless, the Court's 2001 decision turned in large part on the fact that the thermal imaging technology was not in general public use, a factual conclusion that likely would not be true today. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 539 (2007) (explaining that the Supreme Court decides only a handful of cases under its reasonable expectation of privacy test and that lower court decisions involving factual variations tend to be authoritative).

103. *See* Hafner, *supra* note 3.

104. *See* BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, CHARACTERISTICS OF DRIVERS STOPPED BY POLICE, 1999, at 1, 4 (2002) (estimating that in 1999, "19.3 million drivers age 16 or older, or 10.3% of all licensed drivers were stopped by police" and that because some drivers were stopped more than once, a total of 27 million traffic stops occurred).

105. *See id.* at 10.

106. *See id.* at 12.

107. I will concede, however, that good police officers conducting a standard traffic arrest might be reluctant to spend significant time searching an iPhone because they simply have no idea what to look for or where incriminating information might be hidden. Drugs can be held in only a few areas and are relatively easy to uncover during a search incident to arrest. In contrast, when searching an iPhone officers would likely have no idea which emails or websites to browse to find incriminating information. Of course, it is not just the "good" police officers, but also the overly aggressive officers with which the Fourth Amendment must be concerned. I am grateful to Professor Orin Kerr for making this point to me.

The iPhone drastically changes the amount of private information that can be accessed during a search incident to arrest. And unlike thermal imaging devices or airplane flyovers, iPhone searches could potentially affect millions of people. The stakes are higher and it is worth considering whether the search incident to arrest doctrine might be amended to fit this problem.

B. Change Everything: Limiting the Search Incident to Arrest Doctrine in All Police Interactions to a Search Related to the Crime of Arrest

The most drastic change to the search incident to arrest doctrine—short of abolishing it altogether—would be to limit officers to searching for evidence of the crime for which the suspect was arrested. Thus, if the driver were arrested for drug possession, police could search anywhere drugs might be found. But if the driver were arrested for failure to wear a seatbelt, a search for drugs would be impermissible. Justice Antonin Scalia advocated this revision to the search incident to arrest doctrine in his 2004 concurring opinion in *Thornton v. United States*,[108] in which the Supreme Court upheld the search of the passenger compartment of a "recently" occupied car.[109] Joined by Justice Ruth Bader Ginsburg, Justice Scalia argued that searching a vehicle incident to arrest should only be permitted when "it is reasonable to believe evidence related to the crime of arrest might be found in the vehicle."[110] Justice Scalia's view departs from the traditional rationale for the search incident to arrest doctrine. Instead of conducting the searches to prevent the arrestee from harming the officer or destroying evidence, such searches would be justified as "evidence-gathering" exercises that can be conducted because of "a reasonable belief that evidence [will] be found."[111]

Justice Scalia wrote for only himself and Justice Ginsburg in expressing this view, so we might be inclined to dismiss this approach as simply unlikely to be adopted. However, as Professor James Tomkovicz has recently explained, it is not altogether implausible to assume that Justice Scalia's position may some day command a majority: Chief Justice Roberts and Justice Alito have not yet had a chance to address this approach, and Justice Stevens and Justice

108. 541 U.S. 615 (2004) (Scalia, J., concurring in the judgment).
109. *See id.* at 623–24, 632 (Scalia, J., concurring in the judgment).
110. *Id.* at 632.
111. *Id.*

Souter are on record as being very dissatisfied with the current state of the search incident to arrest doctrine.[112]

Besides its unlikely adoption, perhaps a stronger objection to Justice Scalia's approach is that the evidence-gathering approach lacks doctrinal justification. Searching to gather evidence during a search incident to arrest is troubling because it would permit searches based on suspicion—rather than officer safety—that involve less than probable cause.[113] Likewise, such an approach would offer no justification for permitting searches of the passenger compartment incident to arrest but not the trunk of the vehicle.[114]

On the plus side, Justice Scalia's approach would solve the iPhone dilemma by reconceptualizing the entire search incident to arrest doctrine, without requiring a special rule for particular new technology.[115] If police could only search for evidence related to the crime of arrest, most traffic stops would not permit searches of an iPhone's contents. And even when police were permitted to search an iPhone incident to arrest, the scope of the search would be limited. If an officer arrested a driver for possession of drugs with intent to distribute, it would make sense to search his text messages for further evidence of the crime, since that function is commonly used in conjunction with drug sales.[116] But it would not seem to be permissible for the officer to search through the arrestee's pictures under the iPhoto function or the history section under his internet browser because such applications likely have nothing to do with drug sales. A rule limiting the search incident to arrest exception to the crime of arrest would prevent police from roaming at large among the thousands of pages of data held in the iPhone.

---

112. *See* Tomkovicz, *supra* note 9, at 1451–52 ("It is not hard to imagine at least three of these Justices endorsing the 'evidence-gathering' rationale that Justice Scalia relied upon to sustain the search in *Thornton* itself.").

113. *See* David S. Rudstein, Belton *Redux: Reevaluating* Belton*'s Per Se Rule Governing the Search of an Automobile Incident to Arrest*, 40 WAKE FOREST L. REV. 1287, 1345–46 (2005); *see also* Dripps, *supra* note 14, at 404 ("The police, incident to arrest, must have some reason—but not probable cause—to suspect evidence, contraband or weapons. That's a standard, not a rule, and a fairly vague standard at that."); Tomkovicz, *supra* note 9, at 1464 ("[Justice Scalia] never asserts, because it would not be defensible to do so, that an arrest for an evidentiary offense will always, or nearly always, satisfy the *constitutional* standard—probable cause to believe that an item of interest to the government will be found in surrounding areas . . . ."). *But see* Edwin J. Butterfoss, *Bright Line Breaking Point: Embracing Justice Scalia's Call for the Supreme Court to Abandon an Unreasonable Approach to Fourth Amendment Search and Seizure Law*, 82 TUL. L. REV. 77, 107–08 (2007) (downplaying this concern).

114. *See* Tomkovicz, *supra* note 9, at 1471 ("Why is it not logical to believe that evidence located in the arrestee's vicinity might be found inside her trunk?").

115. *See* Kerr, *supra* note 7, at 858–59 (cautioning against courts generating new and individual rules each time new technology raises unforeseen issues).

116. *See, e.g.*, United States v. Slater, 971 F.2d 626, 637 (10th Cir. 1992) (explaining that a cell phone is a "recognized tool of the trade in drug dealing").

C. Change By a Different Sovereign: Encouraging State Legislatures to Adopt a More Protective Rule

Scholars dispute the ability of state courts to provide greater protection of constitutional rights than federal courts.[117] Although the debate rages, it is undisputed that, in the criminal procedure context, a number of states have imposed greater restrictions on searches and seizures under the Fourth Amendment and state constitutional equivalents.[118] Notably, numerous state courts have cabined the search incident to arrest exception under state law to narrower circumstances than authorized by the Supreme Court.[119]

One approach states courts might take is the one advocated by Justice Scalia and discussed in Part IV.B. If the Supreme Court refuses to limit the search incident to arrest doctrine to searches of the arrestee for weapons and evidence of the crime for which he has been arrested, then the state courts could look to their own constitutions to do so. To date, a handful of state courts have adopted this approach.[120]

Moreover, we should look beyond state courts to consider the role of state legislatures in crafting statutory protections. While new criminal procedure rules typically come from courts, it would be a mistake to ignore possible legislative solutions.[121] And, indeed, legislatures have taken action in the past to narrow what they believe to be an overly broad search incident to arrest doctrine.

In the wake of the Supreme Court's expansive 1973 decision in *United States v. Robinson*[122] permitting police to open all containers on a person

---

117. The literature on this subject is vast. For two prominent and contrasting viewpoints, compare James A. Gardner, *The Failed Discourse of State Constitutionalism*, 90 MICH. L. REV. 761 (1992) (documenting the failure of state constitutionalism), with William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489 (1977) (advocating that state courts can provide greater protection of liberties under state constitutions).

118. *See* Barry Latzer, *Toward the Decentralization of Criminal Procedure: State Constitutional Law and Selective Disincorporation*, 87 J. CRIM. L. & CRIMINOLOGY 63, 92 (1996) ("A good chunk of Fourth Amendment doctrine, or some more protective variant of it, is now a part of the state constitutional jurisprudence of most states.").

119. *See id.* at 94 nn.131, 133 (collecting nearly twenty cases from numerous states that limit the search incident to arrest exception).

120. *See, e.g.*, State v. Ringer, 674 P.2d 1240 (Wash. 1983) (en banc); State v. Caraher, 653 P.2d 942 (Or. 1982) (en banc).

121. *See, e.g.*, Douglas A. Berman, *Foreword: Addressing Capital Punishment Through Statutory Reform*, 63 OHIO ST. L.J. 1, 10 (2002) ("[W]e turn to legislatures to find some hope within an otherwise discouraging story about the reform of capital systems . . . ."); Ronald F. Wright, *Parity of Resources for Defense Counsel and the Reach of Public Choice Theory*, 90 IOWA L. REV. 219, 223–24 (2004) (arguing that indigent defense funding is more likely to improve if the reform comes from legislatures rather than the judiciary).

122. 414 U.S. 218 (1973).

incident to a lawful arrest, the Massachusetts legislature adopted statutory language specifically designed to narrow the search incident to arrest doctrine.[123] For over thirty years, that statute has provided that

> [a] search conducted incident to an arrest may be made only for the purposes of seizing fruits, instrumentalities, contraband and other evidence of the crime for which the arrest has been made, in order to prevent its destruction or concealment; and removing any weapons that the arrestee might use to resist arrest or effect his escape. Property seized as a result of a search in violation of the provisions of this paragraph shall not be admissible in evidence in criminal proceedings.[124]

Other state legislatures could revise their codes to follow the Massachusetts model. Or those legislatures could take a different approach and authorize the seizure of iPhones or other wireless devices incident to arrest but prohibit warrantless searches of those devices without a warrant.[125]

The key question is, how likely are legislatures to take action to protect iPhones from warrantless searches? Legislatures are not typically in the business of limiting police officers' ability to conduct criminal investigations.[126] To the contrary, legislators' interests are typically in line with those of law enforcement and they therefore enact statutes that favor expansive police authority.[127] Yet, when it comes to iPhones the situation might be different. Unlike the faceless backdrop in which legislators typically award police great investigatory powers, the scenarios in which an iPhone can be searched incident to arrest are likely to resonate with legislators.

As typically middle- or upper-class individuals with teenage or young adult children, legislators are one of the demographic groups likely to

---

123. *See* Commonwealth v. Madera, 521 N.E.2d 738 (Mass. 1988) (discussing the reason for passing the statute); Commonwealth v. Toole, 448 N.E.2d 1264 (Mass. 1983) (same).

124. *See* MASS. GEN. LAWS ANN. ch. 276, § 1 (West 2004).

125. Justice John Paul Stevens has long advocated a similar approach permitting police to search the passenger compartment of an automobile incident to arrest but not open any of the containers found therein. *See* Robbins v. California, 453 U.S. 420, 451–52 (1981) (Stevens, J., dissenting); Thornton v. United States, 541 U.S. 615, 634 (2004) (Stevens, J., dissenting); *see also* Rudstein, *supra* note 113, at 1340–41 (discussing but ultimately rejecting this approach because it does not eliminate the problem of pretextual arrests).

126. *See* Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or, Why Don't Legislatures Give a Damn About the Rights of the Accused?*, 44 SYRACUSE L. REV. 1079 (1993); *see also* William J. Stuntz, *The Uneasy Relationship Between Criminal Procedure and Criminal Justice*, 107 YALE L.J. 1, 12 (1997) ("Perhaps more so than anywhere else in constitutional law, in criminal procedure the broad exercise of judicial power tends to be justified precisely by the legislators' unwillingness to protect constitutional interests.").

127. *See* Stuntz, *supra* note 13, at 539 ("[P]olice benefit from laws that criminalize street behavior that no one wishes actually to punish . . . cheaper policing should be a boon to police and legislators alike.").

purchase iPhones.[128] And while legislators rarely commit the crimes of murder or rape,[129] as mostly middle-class white men they are statistically more likely to be involved in computer crimes such as financial misconduct or fraud.[130] It is evidence of these crimes that is most likely to accidentally turn up during a search of an iPhone incident to an arrest, whether for running a stop sign or driving while intoxicated. Moreover, while legislatures are unlikely to have illegal child pornography on their computers or iPhones, it is reasonable to assume many male legislators have downloaded "run-of-the-mill" pornography.[131] While this material is not illegal, its discovery would be embarrassing and politically devastating.[132]

And as Professor Craig Lerner has demonstrated, significant legislative protections for criminal defendants often arises in response to a particular legislator being put through the criminal justice process.[133] Thus, while legislators are tough on crime and reluctant to reduce punishments or remove old crimes from the books, it is reasonable to expect that legislators will create criminal procedure protections that track their own self-interest.[134]

---

128. At least at this time, it is likely that legislators' children are the primary demographic group that Apple and its competitors are targeting. *See* Devona Walker, *In Southwest Florida, Apple Geeks Aren't Sold*, SARASOTA HERALD TRIB., June 27, 2007, at D1 ("[T]he iPhone's ideal demographic: a young, professional, tech-savvy gadget kind of guy who came into adulthood with an affinity for everything Apple."). As the devices become more ubiquitous however, middle-aged men and women will increasingly own them personally rather than purchasing them as gifts for children.

129. *See* Craig S. Lerner, *Legislators as the "American Criminal Class": Why Congress (Sometimes) Protects the Rights of Defendants*, 2004 U. ILL. L. REV. 599, 622–23 (2004) (explaining that most indictments of federal legislators have been for nonviolent offenses, particularly financial crimes).

130. *See id.* at 623–24 (explaining that in addition to financial crimes, between 1970 and 2000 "six members of Congress were indicted for sex-related offenses, and several others have been investigated by their colleagues for sexual improprieties").

131. *See* Meghan Daum, *Porn's Lost Sex Appeal*, L.A. TIMES, Oct. 20, 2007, at A19 ("[N]umbers suggest that 20% of men and 13% of women look at pornography at work . . . .").

132. *See* Alan Bernstein, *County GOP Nervous About Fallout From Email Scandal—Two Republicans Hoping to Replace DA Say a Housekeeping Is Needed to Return Integrity to the Office*, HOUSTON CHRON., Jan. 10, 2008, at B1 (describing the uproar when pornography was found on the office computer of the elected District Attorney of Harris County); *see also* Scott Glover, *The U.S. 3rd Circuit Names a Special Panel to Investigate Possible Misconduct of Federal Jurist Alex Kozinski*, L.A. TIMES, June 17, 2008, at 1 (describing how Judge Alex Kozinski declared a mistrial in an obscenity trial he was presiding over and called for an investigation of himself following the disclosure that sexually explicit material was posted on his personal website).

133. *See* Lerner, *supra* note 129, at 632–61. For a recent and excellent argument challenging the view that criminal legislation tends to be entirely one-directional and that legislators never decriminalize conduct, see Darryl K. Brown, *Democracy and Decriminalization*, 86 TEX. L. REV. 223, 265–74 (2007).

134. *See* William J. Stuntz, *The Political Constitution of Criminal Justice*, 119 HARV. L. REV. 781, 796 (2006) ("[L]egislatures have been a good deal quicker to expand criminal procedure protections than to contract criminal liability.").

It is therefore possible that legislators will enact laws limiting the search of iPhones incident to arrest.

Moreover, legislators have incentive to enact such restrictions to please constituents. While it is unlikely that a lobby will form to press for a law exempting iPhones from the search incident to arrest doctrine, it is entirely possible that in the near future a prominent business executive or other powerful and connected individual will be embarrassed when his iPhone is searched at a traffic stop. And when those middle- and upper-class individuals—the type who vote and, more importantly, have money to make campaign contributions—press for some legislative action, lawmakers will have little reason to refuse them. The soft-on-crime label tends not to stick when the new law benefits a considerable majority and protects the middle-class right to privacy.[135]

D. Change at the Margins: The Open Application Test

A more modest revision to the search incident to arrest doctrine, but one that nevertheless would eliminate the current bright-line rule, would be for courts to adopt an open application test. Under an open application approach, police would be permitted to search any open application on the iPhone incident to arrest but would not be authorized to look through applications that are closed when the arrest is made. Thus, an individual who took steps to close the iPhoto application could expect the pictures contained therein to remain private. More significantly, an individual who kept her iPhone off entirely could avoid any search of its contents.

There are at least two problems with this approach: First, it would be very difficult to know if officers are telling the truth when they say an application was open. Because an iPhone can be turned on simply by tapping the touch screen and applications can be activated simply by touching an icon, it would be easy for officers to testify that an application was open at the time of arrest, even if it was in fact closed.[136] Of course, the prospect of police

135. *See* Marc Mauer, *Why Are Tough on Crime Policies So Popular*, 11 STAN. L. & POL'Y REV. 9, 16 (1999) ("[T]he conclusion that crime policy has shifted toward a 'get tough' strategy needs to be tempered with the recognition that when the perceived offenders are white and/or middle class, policymakers appear to be more receptive to rational policy considerations.").

136. Unfortunately, many experts believe that officers lie or, at best, fudge facts to ensure that guilty defendants are convicted. *See* Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1041 (1996) ("[T]he existing literature demonstrates a widespread belief that testilying is a frequent occurrence . . . ."); Myron R. Orfield, *The Exclusionary Rule and Deterrence: An Empirical Study of Chicago Narcotics Officers*, 54 U. CHI. L. REV. 1016, 1050 (1987) (concluding that more than 75 percent of officers surveyed believed that police shade the facts regarding probable cause, and that 19 percent of those who so believed also believed perjury was

lying runs throughout Fourth Amendment jurisprudence. Police could just as easily lie and say they received consent to search the trunk of a vehicle when they in fact did not, or that they smelled marijuana when in fact there was no such smell.

A second and more compelling reason to reject the open application test is that it runs afoul of one of the original justifications for the search incident to arrest doctrine: preventing the destruction of evidence.[137] Just as police could quickly open a closed application on the iPhone, so too could a suspect. An arrestee skilled at using his iPhone might be able to turn on the device, select an application, and destroy text messages, emails, photos, or other evidence in a matter of seconds.

Given that the Supreme Court has adopted a fiction that almost any physical evidence—whether in a closed or open container—in the arrestee's grasp could potentially be destroyed (even if the arrestee is handcuffed[138]) it would make little sense to draw a line forbidding searches of closed applications on an electronic device that an arrestee could easily open and destroy.[139]

E. Changing the Bright-Line Rule: Limiting the Search Incident to Arrest Doctrine to Five Steps of Searches

Another solution would be to limit police to only a fixed number of steps when searching the contents of an iPhone incident to arrest. For instance, courts could set a bright-line rule that police can take five steps, but no more, when rummaging through an iPhone's contents. As with the open application test, this solution likely causes more problems than it would solve, but is worth exploring briefly.

The primary virtue of the search incident to arrest doctrine is that it provides bright-line rules that are easily understood and applied. Thus, police

---

reasonably common). For the classic statement, see ALAN M. DERSHOWITZ, THE BEST DEFENSE, at xxi (1982) ("Almost all police lie about whether they violated the Constitution in order to convict guilty defendants.").

137. *See* Chimel v. California, 395 U.S. 752, 763 (1969) ("[I]t 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.").

138. *See* Carol A. Chase, *Cars, Cops, and Crooks: A Reexamination of* Belton *and* Carroll *With an Eye Toward Restoring Fourth Amendment Privacy Protection to Automobiles*, 85 OR. L. REV. 913, 918 n.31 (2006) ("Several courts have approved the search incident to arrest of an automobile notwithstanding that the suspect has been handcuffed and placed inside a police cruiser.").

139. *See* Tomkovicz, *supra* note 9, at 1427 (explaining that while the pre-*Chimel* era was marked by drastic changes in the scope of the search incident to arrest doctrine, "during the more than thirty-five years since its radical, contractive swing in *Chimel*, the search incident pendulum has moved slowly, yet steadily, in the opposite direction").

know that they can open an arrestee's wallet but cannot search the trunk of his car. The primary detriment of the search incident to arrest doctrine is that it permits the police to rummage through numerous layers of enclosed materials, even if there is no probable cause to believe contraband is buried beneath. This problem is particularly vexing with respect to the iPhone because it contains layer upon layer of data. As previously discussed, police conceivably could (1) turn on the phone; (2) open an internet browser; (3) type in a web-based email account such as www.hotmail.com; (4) log into the account (if the user id and password are saved); (5) open a folder of messages; (6) open a particular message; (7) read the message; (8) open the attachment to the message; and so forth.

One compromise approach would be to create a bright-line "five-level deep" rule (or some other admittedly arbitrary number) limiting the search of iPhones to a total of five steps. Under such a rule, the police could search five levels deep into an iPhone's contents, but no further. Thus, for example, police could (1) turn on the phone; (2) open the internet browser; (3) type in a web-based email account such as www.hotmail.com; (4) log into the account (if the user id and password are saved); and (5) open a folder of messages. If the officer completes the fifth step without finding anything incriminating that could be destroyed, the officer would need to stop searching. To search further, the officer would need to procure a warrant.[140]

The main virtue to this approach is that it puts an outer limit on how far police may search electronic data while at the same time leaving intact a relatively bright-line rule that makes clear to police exactly how far they can go. On the other hand, whether police exceeded the five steps would certainly be debated in individual cases. Judges would have to make findings of fact ranging from the simple—whether the phone was already turned on when the search incident to arrest began, thus not counting as one of the five steps—to the more fuzzy inquiries. For instance, when police linked from one webpage to another, were they taking two steps, or just one? This sort of unguided fact-finding is exactly what courts have tried to avoid by advocating a bright-line search incident to arrest rule.

Perhaps more obviously troubling, selecting a certain number of searches—for instance, saying that police can search five levels deep into an iPhone, but not six—is terribly arbitrary. While courts could say the number of levels is correlated to the likelihood that the arrestee could reach that data and destroy it, selecting a level would still be beyond the institutional

140. Of course, a warrant would require probable cause, which is unlikely to be shown given the lack of any incriminating evidence found thus far in the search.

capacity of courts.[141] Moreover, no comparable five-step rule exists for searches of tangible evidence found during a typical search incident to arrest. If police can exceed five steps to discover drugs in a small bag hidden inside a box lying under some papers in the glove compartment of a car, it is difficult to justify a five-step rule only for iPhones.

F. Distinguishing Between Data on the Device and Remotely-Stored Data Accessible From the Device

Finally, courts could try to draw a conceptual line between data that is "on" or "in" the iPhone and data that is simply accessible via the iPhone. This would essentially be drawing a line between the iPhone's internet browser function and its other applications. An arrestee's pictures in his iPhoto application, his text messages, and his incoming call history would be considered contained "in" the phone. If internet service were cut off, the owner of the phone would still be able to access these features because the data has been downloaded to the phone. By contrast, web-based email accounts or other material that an individual accesses over the internet are not typically downloaded to the phone and are instead, for lack of a better phrase, simply floating around on electronic servers in cyberspace. Because such data is not physically present on the iPhone without proactively seeking it out, courts and legislatures could draw a line forbidding such searches incident to arrest while allowing police to search applications that have data permanently on the iPhone.

One wrinkle to this approach might be if the internet browser that allows the user to access information floating in cyberspace is open when the officer searches the iPhone. For instance, what if the officer conducting the search incident to arrest discovers that the internet browser is open to a web-based email account and the selected email has incriminating information in it? Surely it would not make sense to say that the officer could search the rest of the iPhone's applications but not the open web-based email. One solution to this problem would be to harken back to the original search incident to arrest jurisprudence that allows a full-scale search of some areas beyond the person of the arrestee if the area is in the immediate grabbing space.[142] For instance, the search incident to arrest doctrine typically does not allow a search of the trunk of a vehicle, but if the trunk is open and the

141. *See* Kerr, *supra* note 7, at 858–59.
142. *See Chimel*, 395 U.S. at 763.

arrestee is standing near it, then such a search is permissible.[143] In the hypothetical scenario outlined above, web-based email can be analogized to the trunk of a car. The web-based email, banking information, or MySpace page, would typically be considered to be outside the grabbing space of the suspect. However, when the webpage is open in the internet browser at the time of arrest it would be within the arrestee's immediate grabbing space.

Thinking in terms of physical tangible space, an approach that differentiates between material downloaded onto the iPhone and material that is simply accessible via the iPhone seems to make sense. Just as officers could search the cigarette pack in Mr. Robinson's pocket, they can also search the photos he is carrying on his iPhone. And just as the police could not search Mr. Robinson's medical records stored in his house (rather than on his person), the police also could not search electronic data not currently downloaded onto his phone.

Yet, the comparison with Robinson's medical records fails at a certain level when we consider that one purpose of the search incident to arrest doctrine is to prevent destruction of evidence. Of course, Mr. Robinson could not destroy the medical records in his house while being arrested at a traffic stop. Yet, he could quickly open his internet browser, log onto his web-based email account, and destroy incriminating evidence without ever leaving the traffic stop. Nevertheless, this approach is conceptually promising because it does not require a wholesale revision of the search incident to arrest doctrine, which has been framed with tangible physical evidence in mind.

CONCLUSION

At the end of the day, all six approaches appear to be somewhat unsatisfying. Permitting the police to search only for evidence related to the purpose of arrest would improve the doctrine for all cases, not just those involving iPhones, but it has recently been rejected by a majority of the Supreme Court. Asking state legislatures to limit police to search incident to arrest only for evidence related to the arrest is plausible, but highly unlikely to occur in many states. An open application test may encourage police deception and will likely create the types of factual disputes that the bright-line search incident to arrest doctrine was designed to avoid. A five-step limit will likewise raise factual questions that are best avoided. Finally, while

143. *See, e.g.*, State v. Alderman, No. 28991-1-II, 2003 WL 21965127, at *3 (Wash. App. Aug. 19, 2003) (upholding the search of a vehicle's trunk that was "partially open" under the search incident to arrest doctrine).

a rule that differentiates between data on the iPhone and data accessible via the phone is the most conceptually pure, it does not account for the possibility that arrestees could still destroy data that is merely accessible via the iPhone. Nevertheless, despite the flaws associated with each proposal, all are likely preferable to doing nothing and allowing police to search thousands of pages of electronic data without probable cause or a warrant.