The John Marshall Journal of Information Technology & Privacy Law

Volume 30
Issue 1 *2013*

Article 1

2013

My iPhone is My Castle: One Aspect of Protecting Privacy in a Digital Age, 30 J. Marshall J. Info. Tech. & Privacy L. 1 (2013)

Joan Catherine Bohl

ARTICLES

MY IPHONE IS MY CASTLE:* ONE ASPECT OF PROTECTING PRIVACY IN A DIGITAL AGE

JOAN CATHERINE BOHL+

INTRODUCTION

The legal system has always operated, with reasonable success, by employing analogies. *This,* of course, is never really exactly like *that,* but law often requires us to make some sort of comparison, and thus to give some sort of predictability to human affairs. Generally, we can find common ground that makes a modicum of sense. A tent may look nothing like a mansion, but both are used for human habitation. If you peer into my tent and inventory my stuff, in a sense you have peered into my mansion. We can parse the details, measure value in terms of money, and find disparities galore, but at least we have a workable analogy. Absent a warrant, both searches are, in fact, searches within the meaning of the Fourth Amendment. Absent a warrant, both are impermissible searches of a home.

The earliest rumbles of technology created cracks within this system.[1] It was particularly problematic for the time-honored process of analogizing one item or one interaction with another. Technology made possible devices for communicating, and for storing and accessing information unknown in the centuries before.[2] So different, in fact, that

---

* This term, embodying the idea that a home is a uniquely private space that must be secure from intrusions of the government is found in John Adam's earliest writings. *See* JOHN ADAMS, LEGAL PAPERS OF JOHN ADAMS 137 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965) (describing a man's dwelling as his "[c]astle").

+ Prof. Bohl currently teaches Legal Writing at Stetson University College of Law. Her legal writing course focuses on the impact of technological advances on the law, particularly with reference to privacy issues. Prior to joining the Stetson faculty, she visited for a year at Santa Clara Law School, and taught at Southwestern University College of Law for thirteen years.

1. Kyllo v. United States, 533 U.S. 27, 33 (2001).

2. GERALD GOGGIN, CELL PHONE CULTURE 29-30 (2006); *see generally* CLARICE SWISHER, THE TECHNOLOGICAL REVOLUTION (2002) (examining important advances in

attempts to draw analogies to items long part of the "known world" were not only conflicting, but, in the hands of different courts, sometimes wildly inconsistent.[3] Starring in this largely unexamined twenty-first century drama: the smartphone. What is it? To what is it comparable? This Article is intended to answer these questions and to suggest that analogizing a smartphone to a home, unlikely as it appears at first blush, is appropriate, workable, and even necessary. It is also an analogy that can survive the ever-accelerating pace of technological innovations to smartphones.

Although the Fourth Amendment is generally fact specific and may often require a developed factual record, this is not always the case. A defendant can trigger the protections of the Fourth Amendment if he can establish that he has a reasonable expectation of privacy in an area that is searched.[4] For example, a suspect who stays at a particular apartment only occasionally can claim a reasonable expectation of privacy in that apartment, even though he often lives elsewhere. The suspect's use has rendered it one of his residences under the law.[5] As a matter of law, then, we could analyze all part-time apartment dwellers as being residents of those apartments for Fourth Amendment purposes. Similarly, since all smartphones contain at least some private information, the constitutionality of a smartphone search incident to an arrest can be analyzed under Fourth Amendment principles without delaying analysis until after the search has occurred. For reasons discussed further below, the requirements of standing are met. Indeed, reaching such an analysis in this manner is a constitutional necessity if Fourth Amendment rights are to be preserved in the face of technological advances.[6]

---

computer science and the resulting impact on civilization); State v. Patino, 2012 R.I. Super LEXIS 139, at *73-74 (R.I. Super. Ct. 2012) (noting that "[e]ven the United States Supreme Court has struggled with legal challenges raised by emerging technology" (citing City of Ontario v. Quon, 130 S.Ct. 269 (2010))).

3. *Cf., e.g.*, United States v. Park, 2007 U.S. Dist. LEXIS 40596 (N.D. Cal. May 23, 2007) (analogizing a smart phone to an "access point" with United States v. Finley, 447 F.3d 250 (5th Cir. 2007) (analogizing a cell phone to a container)).

4. *See*, *e.g.*, United States v. Lipscomb, 539 F.3d 32 (1st Circuit 2008).

5. *See, e.g.*, State v. Simmons, 714 N.W.2d 264 (Iowa 2006).

6. *See, e.g.*, *In re* Application of the U.S. of Am. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 532 (D. Md. 2011) (noting that cell phone operation and tracking issues "will certainly arise again, most likely in urgent situations that do not allow an opportunity for deliberate consideration"); *see also* Opulent Life Church v. City of Holly Springs, Miss., 697 F.3d 279, 287-88 (5th Cir. 2012) (holding "cases are fit for judicial decision [when] they raise pure questions of law . . . [and when the plaintiff] would suffer hardship if review were delayed").

THE LEGAL SYSTEM'S TAKE ON "HOME SWEET HOME"

The home is the "first among equals"[7] in Fourth Amendment jurisprudence.[8] At the Fourth Amendment's "very core" stands "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[9] Whether or not a place qualifies as a home is not a matter defined by property laws,[10] but rather by use, by both the physical and psychological connections the premises has to those who live there.[11] Perhaps paradoxically, it *does* require some sort of boundary; this provides notice to the world and information as to what is or is not included in your home. Thus, you cannot sleep in the shifting shade of a tree and claim the area of shade as your home. Considering the importance the common law assigns to the home, this is a reasonable limitation. When the protection is so emphatically defined, the space protected must be too.

The touchstone of a warrantless Fourth Amendment search is reasonableness;[12] but its heart and soul was – and is – the framers' desire to protect the home from government.[13] A person's highest and most revered expectation of privacy lies in his or her home. For example, technology is capable of seeing through the walls of a home with infrared cameras.[14] This process does not require any physical intrusion into the home. It does not even require those wielding the camera to set foot on the homeowner's land.[15] But such a search, absent a warrant, is not permitted. All details within the home are private, simply because they are within the home.[16] The mere possibility that the government surveillance *could* expose private activities within the home to law enforcement examination is sufficient.[17] Explaining its ruling, the court in *Kyllo v. United States* noted with some indignation, that warrantless infrared surveillance of a suspect's home could expose "the lady of the

---

7. Silverman v. United States, 365 U.S. 505, 511 (1961).

8. The Fourth Amendment provides that:

> [the] right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

9. *Silverman*, 365 U.S. at 511.

10. Soldal v. Cook Cty., 506 U.S. 56, 64 (1992); Katz v. United States, 389 U.S. 347, 351 (1967).

11. California v. Ciraolo, 476 U.S. 207, 213 (1986).

12. Cooper v. California, 386 U.S. 58, 59 (1967).

13. *Silverman*, 365 U.S. at 511.

14. *Kyllo*, 533 U.S. at 37.

15. *Id.* at 29-30.

16. *Id.* at 37.

17. *Id.*

house in the bath."[18] Such an intrusion is unreasonable when we are considering the search of a home.

THE PARAMETERS OF THE FOURTH AMENDMENT PROTECTION OF CELL PHONES IN THE CONTEXT OF ARREST

Let's assume you are arrested. As a general matter, the Fourth Amendment protects information in which you have a subjective expectation of privacy, as long as the expectation is one society considers objectively reasonable.[19] This concept is subject to two narrowly defined exceptions[20] in the context of your arrest. One exception is the need to ensure officer safety.[21] This allows an officer to search your person at the time of arrest. The other exception arises from society's interest in the preservation of evidence.[22] This allows an arresting officer to search the area within your immediate control, the area colloquially known as your "grab zone." Once the officer has secured you, for example, by putting you in a patrol car, and thus has assumed control of the immediate area around you, both exceptions cease to exist.[23] Any further search must be authorized by a warrant. Furthermore, application of this test does not turn on what the police officer knew at the time of the search incident to arrest "but rather the objective, ex post facts as known to the court when considering the motion to suppress."[24]

Two different, and completely contrary, analogies have dominated judicial decision making with regard to smartphone searches performed incident to a subject's arrest. The elder of the two analyses takes the position that a smartphone can be categorized as a container.[25] When police search a suspect incident to an arrest, the process properly includes opening and searching any containers found on the suspect's person.[26] If you chose to lock your briefcase, or password protect your smartphone, the police are free to check your key ring for the appropriate key,[27] or take a guess at your password. Although officers may not

---

18. *Id.* at 38.

19. Smith v. Maryland, 442 U.S. 735, 740 (1979); 22A C.J.S. Criminal Law § 1066 (2006).

20. Some courts consider these categories of searches not only exceptions to the Fourth Amendment warrant requirement but . . . also [per se] "reasonable" search[es] under that Amendment. New York v. Belton, 453 U.S. 454, 459 (1981) (citing United States v. Robinson, 414 U.S. 218, 235 (1973)).

20. Chimel v. California, 395 U.S. 752, 762-64 (1969).

22. *Id.*; United States v. Zamora, 2006 WL 418390, at *4 (N.D. Ga. Feb. 21, 2006).

23. United States v. Gant, 129 S.Ct. 1710, 1719 (2009).

24. WAYNE R. LAFAVE, SEARCH AND SEIZURE 113 (5th ed. 2012).

25. United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007).

26. *Id.* (citing Unites States v. Johnson, 846 F.2d 279, 282 (5th Cir. 1988)).

27. United States v. Wurie, 612 F. Supp. 2d 104, 107 (D. Mass. 2009).

damage either the briefcase or the phone,[28] if the officers find the key,[29] or guess the password,[30] the search is on. This analogy is still widely recognized,[31] although it was certainly problematic from the start, since a "container" is usually considered a physical object capable of containing another physical object.

The other analogy, born shortly thereafter, rejects the idea that a smartphone can be analogized to a container at all given its virtually unlimited capacity to obtain and store information. In *People v. Diaz* the court chose instead to analogize a smartphone to an access point.[32]

With no principled analogy for the role cell phones play in twenty-first century life, some courts will continue to allow law enforcement to conduct ad hoc intrusions into the private information found on your smartphone. This Article will propose an analogy capable of surviving the continual and relentless evolution of smartphones. It is an analogy that will make sense to the 327.6 million cell phone users,[33] and probably would have resonated with the framers as well. In 1776 your home played a central role in your life; it housed personal items of all sorts, from writings that could reflect your most intimate thoughts to sensitive medical and financial information. It provided you a post from which to look out at the world. In 2013, you carry that personal information – and more – in your pocket or purse. Your smartphone allows you to look out on the world. Your smartphone has, in a real sense, become your home.

A PHONE, PERHAPS, BUT NOT YOUR GRANDDADDY'S "PHONE"

The struggle to somehow cabin the legal significance of a smartphone has resulted in twists and turns as lawyers and judges try

---

28. For example, an iPhone user may limit the number of inaccurate password entries so that when the number is exceeded, the iPhone's data is erased.

29. *See* United States v. Gamalier Concepcion, 942 F.2d 1170, 1172-73 (7th Cir. 1991).

30. In a June 2011 study of 204,508 smart phone passwords, the most common passwords were one of the following: 1234, 0000, 2580, 1111, 5555, 5683, 0852, 2222, 1212, 1998. *Cracking Smartphone Passwords*, ISS SOURCE (Mar. 30, 2012), http://www.isssource.com/cracking-smartphone-passwords/.

31. *See* United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1278-79 (D. Kan. 2007) (collecting cases upholding cell phone searches incident to arrest).

32. People v. Diaz, 244 P.3d 501, 505 (Cal. 2011).

33. This number exceeds the number of people living in the U.S., Puerto Rico, Guam and the U.S. Virgin Islands – 347.6 smart phones versus 315 million people. Cecilia King, *Number of Cellphones Exceeds U.S. Population: CTIA trade group*, WASHINGTON POST BLOG (Oct. 11, 2011, 7:54 AM ET), http://www.washingtonpost.com/blogs/post-tech/post/number-of-cell-phones-exceeds-us-population-ctia-trade-group/2011/10/11/gIQARNcEcL_blog.html.

to wrestle the concepts into submission: these struggles help illume what a smartphone *is*, as well as what it is *not*.[34]

First, a smartphone is not a beeper – a device that can be attached to a car or truck to track its movements. A smartphone can certainly provide real time location data, but it is not something affixed to something else. When a beeper is affixed to a car, for example, a trespass occurs. The application of the foreign, physical object to the suspect's car without his or her consent is a trespass onto his or her property. In contrast, no trespass occurs when law enforcement tracks a suspect by monitoring his or her smartphone. Nothing is attached to the phone. Law enforcement need never touch it. Instead, a smartphone constantly emits "pings," in an attempt to find the strongest signal from available cell towers.[35] The phone is simply doing what it has been designed to do and the police are simply taking note. When your cell phone is turned off, it is essentially placed in a state of "electronic hibernation."[36] Even at that point a federal court can order the wireless service provider to send a signal to defendant's cell phone prompting the phone to compute its current GPS coordinates and relay it back to the provider.[37] Furthermore, the service provider can remotely activate software that prompts the smartphone to continue to "ping" even when it is turned off. No physical contact has occurred between a police officer and the smartphone. Nothing has occurred that under traditional property rules might be a trespass. Once again, technology would jealously deny us a workable analogy. But as the limitations of a purely property-based concept of "trespass" became more constricting and unhelpful, however, the United States Supreme Court stuck a proverbial "toe in the water," to begin a process of abandoning this paradigm of trespass in favor of a broader conception of privacy interests.[38]

Further, the fact that a smartphone is in fact a *phone* is not a useful analogy either. The phones of yesteryear connected the caller with the number of the person being called. At the end of the month, a bill would arrive detailing "long distance" calls. Typically, no record of local calls was generated at all.[39] A smartphone, on the other hand, lists

---

34. Brian A. Stillwagon, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165, 1168 (2008) (noting that cell phone cases have forced "the judiciary to adapt the constitutional text [of the fourth Amendment] to modern situations").

35. *See generally In re Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d at 526.

36. United States v. Flores-Lopez, 670 F.3d 803, 808 (7th Cir. 2012).

37. *See* All Writs Act, 28 U.S.C. **§** 1651 (a) (providing authority to order this GPS data).

38. *In re Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d at 537-38 (citing *Katz,* 389 U.S. at 353).

39. *See generally In re* Application of the U.S. of Am. for Historical Cell Phone Data, 747 F. Supp. 2d 827 (S.D. Texas 2010).

every call made or received, either local or across a continent, color-coded to distinguish incoming calls from outgoing.[40] The touch of a finger on the smartphone reveals every contact. If the contact is in the owner's smartphone's address book, that gentle swipe will reveal names as well. If the smartphone owner is particularly thorough, the gentle swipe will reveal physical addresses, emails, and reminders of various sorts. Besides, as if some evil genie sought to render any useful comparison completely out of the question, a smartphone virtually always belongs to one person, not a household.[41] The landline of a bygone era was shared by an entire household, or even more. In contrast, if it is your smartphone, the contacts revealed are yours. It yields a record of your associates, contacts, activities, priorities – an outline of your life. The sheer number of smartphones of varying capabilities further muddies any analogy, rather than providing a staging ground for comparisons the law could use. Thirty years ago, for a nanosecond or so, cell phones were, in fact, analogous to landline phones; no one would accuse them of being "smart." These precursors of the smartphone, aptly called "car phones," operated off the car battery only, and were designed primarily for obtaining roadside assistance.[42] Cell phones evolved, of course, and became "smarter." Their increased capacities and functionalities, however, came at different paces. Soon, the sheer variety overwhelmed law enforcement, if not the ordinary citizen. Out of this explosive growth, one of the few generally accepted rules applicable to cell phones was born: all cell phones are to be considered equal. Law enforcement personnel need not ascertain how "smart" the smartphone seized actually is; as a matter of expediency, all are treated the same.[43]

One other legacy of the tenuous relationship between the landline phone and its "smart" progeny is the contested question of what legal significance attaches to the transmission of a message or call from one smartphone to another.[44] It is axiomatic that one can have no legitimate expectation of privacy in something one has knowingly exposed to the world.[45] When our proverbial Granddaddy placed a call with his landline (rotary, no doubt) he was aware that an operator was on the line as

---

40. *Park*, 2007 U.S. Dist. LEXIS 40596, at *22; *see also iOS: Using Messages*, APPLE (May 20, 2013), http://support.apple.com/kb/HT3529.

41. *Patino*, 2012 R.I. Super LEXIS 139, at *110.

42. Tom Farley, *The Cell-Phone Revolution*, AMERICAN HERITAGE OF INVENTION & TECHNOLOGY, Winter 2007.

43. United States v. Wall, 2008 WL 5381412, at *4 (S.D. Fla. Dec. 22, 2008) (noting that messages on pagers may be subject to automatic deletion as more are received but this is not true on cell phones collectively).

44. *Patino*, 2012 R.I. Super LEXIS 139, at *97 (discussing the analogies initially applied by the judiciary that, while easy to apply "in hindsight and given the evolution of technology from pagers to cell phones, appear inapt.").

45. State v. Quinlan, 921 A.2d 96, 109 (R.I. 2007).

well, routing the call to its intended recipient.[46] The fact of the call, the number dialed, and indeed, some of its content inevitably entered the public domain. Times changed, switchboard operators moved on to other pursuits, and computer systems of increasing sophistication connected caller with callee. In essence, however, the methodology did not change. The call or text from a smartphone had to be connected via a service such as Verizon or AT&T for the call or text to be received. Under established legal theory, this meant privacy had been compromised. Some courts cling to this undeniably serviceable analogy, taking the position that the cell phone user has forfeited his or her expectation of privacy.[47] Other courts and jurists reason that the smartphone user in the twenty-first century is unlikely to think that a call passed by satellite to its recipient has been exposed to the world.[48]

OTHER ANALOGIES *CANNOT* APPLY: SOME RED HERRINGS

In the search for a workable analogy, some commentators have seized upon the personal computer; it shares some characteristics with a smartphone, and so makes a tempting possibility. At first blush the comparison seems the most legitimate so far. Both are potentially filled with personal and financial data, records of thoughts, notes, and pictures. After this point, however, the similarities break down. First, and most obviously, people do not carry personal computers in their pockets; the intimate connection between owner and phone is lost. In this threshold sense, computers are one step removed from the ordinary, ongoing round of life – the ordinary life that the framers equated to life in the home - and valued so intensely.

Furthermore, a computer is more frequently shared and even compartmentalized and so becomes more a tool for use by several people than an extension of one person. Libraries and schools routinely provide computers to multiple users.[49] The mere login to a personal computer signals this difference by asking for both a user name and password. A smartphone may be able to perform the same tasks, but it is not shared.

---

46. *But see Smith*, 442 U.S. at 746-47 (Stewart, J., dissenting) (noting that a caller does not assume information from his or her call will be transmitted to government agents to use for their own purposes).

47. Reporters Comm. for Freedom of Press v. AT&T, 593 F.2d 1030, 1043 (D.C. Cir. 1978) (discussing the fact that, as a general proposition, when an individual conducts a relationship with others he or she must expect to leave behind some record).

48. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); Orin S. Kerr & Greg Jojeim, *The Data Question: Should the Third Party Records Doctrine be Revisited*, A.B.A. JOURNAL (Aug. 1, 2012), *available at* http://www.abajournal.com/magazine/article/the_data_question_should_the_third_party_records_doctrine_be_revisited/.

49. *Public Computer*, WIKEPEDIA (Aug. 19, 2013), http://en.wikipedia.org/wiki/ Public_computer.

Your smartphone is yours alone, no option exists for public use. The fact that a computer's files can be compartmentalized brands it a tool as well. Some files can be password protected while others are not.[50] This is contrary to the Fourth Amendment guarantees shielding the home. Indeed, even illegal activities that would subject the suspect to sanctions outside the home are protected as long as they are conducted within the confines of the home.[51] All areas are protected by virtue of being categorized as part of the home.

Another unworkable analogy is that text messages on a cell phone align with their older cousins, emails or even physical mail, because all reveal some sort of address. Routing information, like addresses on letters, obviously must be visible to the world. But although an email may also have a visible subject line, both physical mail and email "contain a package of content the sender assumes will be read only by the intended recipient."[52] Further, a paper letter and an email both tend to be a complete communication. Text messages, in contrast, embody brief back and forth exchanges of small portions of information, opinion, or comment.[53] Therefore one can scan a letter and get a writer's point, fully developed. Similarly, emails are usually complete communications.[54] Not so with a text. It is meaningless to see one text entry.[55] The back and forth exchange of text messages is more like oral communication.[56] A judicial order authorizing law enforcement to review and photograph one text message only would be both unlikely and unhelpful.

A LIMITED SEARCH OF A CELL PHONE TO PRESERVE DATA: OKAY OR NOT OKAY?[57]

A frequently advanced justification for a warrantless smartphone search is an exigent circumstance theory, arising out of the possibility that, in the time needed to obtain a warrant, the smartphone's owner could destroy any evidence on the phone. The exigent circumstance exception to the Fourth Amendment warrant requirement rests on the need to preserve evidence that will otherwise be destroyed.[58] First,

---

50. United States v. Cotterman, 709 F.3d 952, 958 (9th Cir. 2013).

51. *See, e.g.*, Ravin v. State, 537 P.2d 494 (Alaska 1975) (asserting that an adult's right to possess marijuana in the home is protected).

52. United States v. Forrester 512 F.3d 500, 511 (9th Cir. 2007).

53. *Patino*, 2012 R.I. Super LEXIS 139, at *77, *115; *see also What is the maximum length of text message?*, VERIZON WIRELESS (May 24, 2011, 2:33 PM), https://community.verizonwireless.com/thread/537870 (describing the limit on characters in a text).

54. *Patino*, 2012 R.I. Super LEXIS 139, at *132.

55. *Id.* at *131-32.

56. *Id.*

57. KATHY LEE AND HODA, www.today.com/klandhoda.

58. Mincey v. Arizona, 437 U.S. 385, 393-94 (1978).

destruction of any data on the phone[59] is a remote possibility because the police officers that seize the phone can secure it, and even if it is not secured, the chance of evidence destruction is remote. A lead box is an inexpensive way to freeze the phone and its content.[60] Even if it were not secured in that way, the chances that an accomplice would be aware of the arrest would require an extraordinarily alert accomplice and an arrestee focused on elimination of evidence. With an iPhone, for example, the person arrested would need to notify the accomplice in the seconds or minutes before he or she is searched and secured.[61] Even assuming virtually instantaneous notification, remotely "wiping" the phone requires multiple steps[62] and knowledge of the arrestee's Apple identification code.

Similarly, no distinction between data, pictures, or call records on a smartphone satisfies the Fourth Amendment's mandate, because no meaningful distinction exists. In a physical search, a police officer could not search a medicine cabinet for a flat screen TV.[63] No such bright line limitations exist in the virtual world of a smartphone. The picture "app" is no easier – and no more difficult – to touch than the text "app."

Similarly, although a smartphone search can reveal two general types of information: coding or address information and content information,[64] this distinction crumbles, too, under the weight of technological advances. Coding information discloses contact information, such as phone numbers.[65] It is the smartphone equivalent of the routing information on the envelope of a letter. Content information, on the other hand, includes pictures or the substance of messages[66] on a smartphone, or in the letter once it has been opened. As recently as

---

59. Dan Boone, *Materials That Affect Cell Signals,* EHOW TECH (Feb. 19, 2013, 6:20 PM), http://www.ehow.com/info_8113041_materials-affect-cell-signals.htm. This product is used by police and military to jam signals. The science behind it is called a Faraday Cage. Nathan Chandler, *How Faraday Cages Work*, HOW STUFF WORKS, http://science.howstuffworks.com/faraday-cage.htm (last visited Nov. 3, 2013).

60. Boone, *supra* note 59.

61. I use the iPhone as an example frequently because it dominates the United States market for smart phones. Lance Whitney, *iPhone wins 51 percent of U.S. smartphone sales, says report*, CNET (Jan. 22, 2013), http://news.cnet.com/8301-13579_3-57565106-37/iphone-wins-51-percent-of-u.s- smartphone-sales-says-report/.

62. *iCloud: Erase Your Device*, APPLE (Oct. 31, 2013), http://support.apple.com/kb/PH2701?viewlocale=en_US&locale=en_US (explaining that to accomplish a remote "wipe" of an iPhone, a person – here, an accomplice – would need to know the owner's – here, the arrestee's – apple I.D. and be able to sign in to iCloud.com and select the device).

63. *See, e.g.* United States v. Galpin, 720 F.3d 436 (2d Cir. N.Y. 2013) (making this point in the context of the search of a computer).

64. *Smith*, 442 U.S. at 741-42.

65. *Id.*

66. Matthew E. Orso, *Cellular Phones, Warrantless Searches and the New Frontier of Fourth Amendment Jurisprudence,* 50 SANTA CLARA L. REV. 183, 188 (2010).

2001, the Patriot Act [67] distinguished between "dialing routing and addressing" and *contents* of electronic communications in an apparent attempt to assuage fears that American citizens' privacy was at risk. In a very real sense, this distinction may be wholly inadequate under Fourth Amendment principles in a digital age.

For example, *State v. Patino* illustrates the fatal flaw in this distinction by explaining the reality of smartphone use, focusing specifically on text messages to demonstrate a simple "work around" of the Fourth Amendment. Text messages, the court noted, can be accessed from multiple places: "the sending phone, the receiving phone and, perhaps the service providers' records."[68] *Patino* involved the question of whether the defendant had abused and ultimately killed his girlfriend, Trisha's, biological child. Defendant Patino occasionally shared Trisha's apartment. Four smartphones were found in the apartment when the investigation of the child's death commenced.[69] One of the four smartphones had been purchased by defendant but was apparently used exclusively by Trisha.[70] Defendant used the other phones. Trisha was not implicated in the child's abuse. Indeed, upon finding the child unconscious and unresponsive, she left everything behind, including her cell phone, to accompany him to the hospital.[71]

A text message sent between these two people could obviously be read either from the phone Trisha used or the phones Defendant Patino himself used. The police could have confiscated and secured the defendant's phone and then sought a warrant to search it, leaving the plainly innocent Trisha's phone untouched and unobserved. Instead, the police apparently viewed incriminating text messages sent by Trisha to the defendant, and from the defendant to Trisha, all stored on Trisha's phone. The fact that the defendant's texts went to Trisha gave the police another lead. They were able to use the coding information in the contact list on Trisha's phone to link the incriminating texts to the defendant's phones. In effect, the police were able to conduct a warrantless search of the defendant's phones that, technically, did not violate the Fourth Amendment. The texts thus viewed were a smoking gun, documenting the child's growingly serious medical condition, [72] and implicating the defendant.

The "work around" begins with this unconstitutional expediency on the part of police. Trisha was never a suspect. Of course, a review of her text messages, pictures, and contacts violated her privacy as well as

---

67. The Electronic Communications Privacy Act of 1986 was later expanded through the Patriot Act. 18 U.S.C. §§ 3121-3125 (2012).

68. *Patino*, 2012 R.I. Super LEXIS 139, at *103-04.

69. *Id.* at *8.

70. *Id.*

71. *Id.* at *113 n. 50.

72. *Id.* at *5.

yielding overwhelmingly incriminating evidence against Defendant Patino. But since the phone was Trisha's, the defendant lacked standing to challenge the search under the Fourth Amendment.

Furthermore, Trisha, for all practical purposes, would also lack ability to challenge the search. To do so would require her to obtain an attorney, invest money in legal fees, and spend time in court.[73] Having suffered no injury herself, and having few material resources, the grieving mother would be unlikely to take any steps at all. Meanwhile, armed with the coding information to connect content of the texts on Trisha's phone to the defendant, police were in an excellent position to question the defendant. They could use phrases he himself had used and take advantage of the time frame the texts provided.[74] The "work around" was complete.

A WORKABLE ANALOGY FOR GOVERNMENT SEARCHES OF SMARTPHONES

The analogies reviewed above have all proved flawed. They necessarily yield inconsistent results, allowing some searches, forbidding others, toying with unworkable compromises that might allow a limited search. This disconnect may be unthinkably magnified as smartphone technology evolves.[75] If one can step just outside the spatial world, however, one can think of a person's smartphone as that person's home. The significance of "home" is already rooted in our country's origins. It represents an unyielding bright line, workable and adaptable, already untethered from property concepts. If the dramatic march of technology in the twenty-first century has provided any general lesson, it is that spatial and physical boundaries must not define us. The virtual world is coming into its own, and it is more than malleable enough to include another private space: the smartphone. Indeed, should some modern day doubting Thomas[76] take issue with this, let him simply visit a busy airport terminal. He will see smartphone users immersed in the content of their phones, oblivious to the ebb and flow of the crowd, secure in that private space, in that virtual home that their smartphones provide.

---

73. *Id.* at *26.

74. *Id.* at *103.

75. Some examples that one might see in the future may be seen at physics.org. *Future Mobil Phone Technology*, PHYSICS.ORG, http://www.physics.org/article-questions.asp?id=83 (last visited Nov. 3, 2013).

76. According to the Christian Bible, Jesus' disciple, later dubbed "Doubting Thomas," is known for questioning Jesus' resurrection when first told of it. *Thomas the Apostle*, WIKIPEDIA, http://en.wikipedia.org/wiki/Thomas_the_Apostle (last visited Nov. 3, 2013).