There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones

by DANIEL ZAMANI*

Introduction

We live in a changing world. Communication is increasing at unprecedented rates. The sharing of information over massive worldwide networks has reached proportions once unimaginable. While a 1993 *New York Times* article describing the "staggering growth rate" of the Internet referenced a figure of "200 billion bytes a month" (roughly 2.18 terabytes per year),[2] new estimates suggest that by 2013, this number will reach roughly 700 million terabytes per year.[3]

The growing ubiquity of "smart phones" has assisted this dramatic increase in the transfer of information. While there is no precise demarcation line between an early generation cellular phone and a "smart phone," for the purposes of this Note, a "smart phone" is defined as any phone with the ability to engage in non-voice, non-

* Juris Doctor Candidate 2011, University of California, Hastings College of the Law; Bachelor of Science 2006, University of California, Los Angeles. I would like to thank my family for their love and support, Professor George Bisharat for his guidance throughout the drafting process, Matt O'Neal for reviewing and commenting on early drafts, Ian Ellis for his painstakingly thorough editing of my later drafts, and the *Quarterly's* Volume 38 staff for all of their hard work and dedication.

2. John Markoff, *Business Technology; Jams Already on Data Highway*, N.Y. TIMES, Nov. 3, 1993, at D1, *available at* http://www.nytimes.com/1993/11/03/business/ business-technology-jams-already-on-data-highway.html.

3. *A Special Report on Managing Information: Data, Data Everywhere*, THE ECONOMIST, Feb. 27, 2010, at 71.

SMS (also known as "texting") communication.[4] In order to do so, these phones must have the ability to connect to remote computers.[5] These include web servers to access the World Wide Web, email servers to check correspondence, proprietary servers used to download third-party applications (*e.g.,* the iPhone's App Store, the Android operating system's Market, or the Blackberry App World), and even computers in one's home, from DVRs to a home desktop or laptop.

The focus of this Note will be on the search and seizure of the data that is both contained within and accessible by these devices. The sheer amount of information that a law enforcement officer may glean from these becomes apparent when one considers that the applications that can be installed offer the ability to do everything from connecting to one's home computer to signaling warnings when nearing speed traps to "nearly every imaginable function of the office and home entertainment center."[6] These myriad uses have appealed to a growing number of users, with estimates suggesting that by 2013, roughly half of the mobile phone market (currently around 173 million units) will be smart phones.[7]

For those that own one, their smart phone has been described as a "concierge," a "lifeline," or more broadly, "the remote control of our lives."[8] These anecdotal descriptions seem hyperbolic, but global mobile phone data traffic continues to increase—with rates greater than 200 terabytes per month expected in 2010 (six times the amount in 2009).[9] The quantity of data being passed through these devices, coupled with their constant presence at their users' sides, means that access to one's smart phone can potentially reveal more information about a user than even a search of one's home computer might.[10]

4. This usually entails having a separate data plan to connect to the World Wide Web, e-mail servers, and the like. While this definition may seem a bit unwieldy, this directly addresses the differences that make a smart phone "smart" as most cell phones have the ability to use voice and SMS (short message service or "text") communication.

5. *Id.*

6. John Boudreau, *Your Phone, Your Life: Applications For Your iPhone, Blackberry or Other Mobile Device Are Changing How You Navigate Your World*, SAN JOSE MERCURY NEWS, Mar. 15, 2009, at 1A, *available at* 2009 WLNR 5010619.

7. *Id*.

8. *Id*.

9. Jon Fortt, *iPhone Overload!*, FORTUNE, Sept. 14, 2009, at 37.

10. Boudreau, *supra* note 6 ("Because their smart-phone is with them everywhere they go, people develop far closer attachments to the devices than to their home PCs or laptops . . . . Nothing is as close to us all the time—not even your spouse or partner.").

A problem arises when one considers that while a search of a "regular" computer will often require a warrant simply due to its location within a home, a smart phone's portability makes it more susceptible to exceptions to the Fourth Amendment's provision that "no Warrants shall issue, but upon probable cause."[11] The exigency exception and the search incident to arrest exception are two ways by which law enforcement officers can get access to the massive data stores from an individual's smart phone.[12] Some courts have held that the mere fact that the item to be searched was a cellular phone provided an exigency that justified a warrantless search,[13] while others have defended searches incident to arrest because the cellular phone was no different from any other closed container.[14] Nearly all jurisprudence on this subject deals with cellular phones but currently it seems that the same standards would be applied to smart phones.[15] Yet, as discussed above, both the quantity and quality of the information stored on a smart phone, coupled with its constant presence at its user's side, seem to indicate that new standards are needed.

While scholars have discussed various methods to address these problems and update search and seizure doctrine for the Information Age, nearly all have done so by treating smart phones as immense and complex file cabinets.[16] While this comports with decades of

11. U.S. CONST. amend. IV.

12. *See, e.g.,* United States v. Lottie, No. 3:07-cr-51-AS, 2007 WL 4722439, at *2–*5 (N.D. Ind. Oct. 12, 2007).

13. *See, e.g.,* United States v. Zamora, 2006 WL 418390, at *4 (investigating agents' "reasonable beliefs . . . [regarding] the function and limitation of the cell-phone technology" provided an exigency that justified the warrantless search); United States v. Parada, 289 F. Supp. 2d 1291, 1304 (D. Kan. 2003) (law enforcement agents were justified in searching cell phone's call log by exigency of preventing potential destruction of evidence).

14. *See, e.g.,* United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1277–78 (D. Kan. 2007) (justifying search of a cell phone's contents because scope of search incident to arrest extends to "containers found on the arrestee's person" in order to preserve evidence of the arrestee's crime).

15. Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27, 45 (2008) ("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.").

16. *See, e.g., id*., at 40–41, 43 (noting that the container analogy is strained and inadequate, Gershowitz distinguishes between a regular cell phone and an iPhone by stating that "the former stores tremendously more information and in a very different way"); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 549 (2005) (Kerr states that the starting point for analyzing how the Fourth Amendment

Fourth Amendment precedent, it doesn't take into account three important factors: (1) the characteristic of files stored on smart phones to contain information beyond the actual content of the file (broadly referred to as metadata) and (2) the ability to access distant computers remotely from smart phones and (3) vice versa, the ability to access the smart phone remotely from a distant computer. If one were to analogize to a piece of property accurately, it might behoove one to delve into fantasy. An accurate analogy for a smart phone's capacity might be Mary Poppins' carpetbag or Hermione's handbag from *Harry Potter*, both of near infinite proportions. Yet, even those analogies do not describe a smart phone completely accurately as those items cannot access remote places. Continuing with this exercise, we would need to borrow from science fiction, adding some sort of wormhole or tunneling device allowing the smart phone owner to reach distant places from the phone and, conversely, to reach into the phone from those distant places. Yet, this only describes the smart phone's abilities; we must also consider the data contained therein. Metadata can be thought of as the interior of Russian *matryoshka* dolls, with layers of information nested within each other, but this analogy is insufficient as well because the content and its metadata are rarely, if ever, similar. In order to accurately describe metadata, one must delve even deeper into mythology and search for examples of inanimate objects describing the activities and whereabouts of their holders; in this case, the *matryoshka* dolls would have to be able to talk.

Though these attempts at analogy are deliberately ludicrous, they serve to illustrate the deficiencies of property analogies in the context of smart phones. It has been said that, "[a]ny sufficiently advanced technology is indistinguishable from magic"[17] and at the time the Fourth Amendment was drafted, smart phones might well have been considered magical. This is only relevant because courts have shown reluctance to rule on Fourth Amendment issues without analogies to past jurisprudence, which is nearly entirely based on tangible property principles.

This Note attempts to describe the current state of Fourth Amendment policy and show that its current trajectory will lead to untenable results as smart phones become even more prevalent and

should apply to a search of a computer is to "compare computers to homes and sealed containers.").

17. ARTHUR C. CLARKE, PROFILES OF THE FUTURE: AN INQUIRY INTO THE LIMITS OF THE POSSIBLE 36 (Harper & Row 1962).

people begin to use them to their full potential. Part I is a history of Fourth Amendment jurisprudence which establishes the importance of seeking property analogies in developing new search and seizure tests by examining the history of courts' treatment of new technology. Part II distinguishes the different types of information accessible via smart phones, focusing on the metadata that is not readily apparent to the user. It describes the difference between "content" and "coding" information and divides these categories even further. "Content" information is divided into the data stored on the phone and data stored in the "cloud" (a technical term used to refer to data on remote servers) and "coding" information is split into coding data that is visible to the user and the nonvisible "metadata." Procedures for dealing with these overlapping areas are proposed. Part III briefly discusses the ability to access smart phones remotely and the potential implications this has on searches and seizures pursuant to a warrant.

I. Fourth Amendment Jurisprudence and the Importance of Property Analogies in Establishing New Tests

Since its drafting, the Fourth Amendment's proscription against "unreasonable searches and seizures" has been a slowly changing doctrine. While courts have refined their analyses over the years, the pace at which they have progressed has been glacial relative to changes in society and technology. This disparity has become even more apparent with the advent and rapid integration of computers into nearly every facet of society.

However, the inertia of the Supreme Court has been apparent since the early years of Fourth Amendment jurisprudence. The initial focus of the Court was on the search and seizure of tangible items and thus was based primarily on an analysis of property rights.[18] This was in line with the Framers' intent to combat the abuses of the colonial era such as the infamous writs of assistance, which allowed officials to conduct virtually unlimited searches.[19] In *Olmstead v. United States*,

18. *See* Boyd v. United States, 116 U.S. 616, 622 (1886) (construing a law requiring the production of books and papers as an unconstitutional search and seizure); Olmstead v. United States, 277 U.S. 438, 465–66 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967) (holding that Fourth Amendment protection is confined to the protection of tangible items and the physical invasion of real property as opposed to interception of information via wiretaps).

19. THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 48–50 (2008).

one of the first cases dealing with the application of the Fourth Amendment to technology, the Court construed protection of people's "houses, papers, and effects" quite literally and held that conversations intercepted via wiretaps placed on phone lines located outside Olmstead and his codefendants' homes did not constitute a search or seizure because the conversations were not tangible and because government officials had not physically invaded the home.[20]

It took thirty-nine years for the Court to overturn *Olmstead* and shift the focus of its analysis from property to privacy rights. In *Katz v. United States*, a wiretap scenario similar to that of *Olmstead* was held to be a search and seizure because Katz had a reasonable and legitimate expectation of privacy in his conversation in an enclosed phone booth.[21] The shift from a property to a privacy analysis is apparent in the Court's oft-quoted adage: "the Fourth Amendment protects people, not places."[22]

Yet, though the focus has shifted to determining whether a person has a reasonable expectation of privacy in what is searched or seized, the Court still continues to use property principles in making those decisions, often focusing on the sanctity of the home.[23] It distinguishes between information transmitted from a police "beeper" located within a home[24] and one transmitting from a car;[25] between the curtilage of a home and open fields that may be on the same property;[26] and even between technology that can detect activity around homes and that which can detect activity within homes.[27]

20. *Olmstead*, 277 U.S. at 464–66.

21. Katz v. United States, 389 U.S. 347, 353 (1967).

22. *Id.* at 351.

23. *See, e.g.,* United States v. Karo, 468 U.S. 705, 712–13 (1984); United States v. Knotts, 460 U.S. 276, 285 (1983).

24. *Karo*, 468 U.S. at 712–13.

25. *Knotts*, 460 U.S. at 285.

26. United States v. Dunn, 480 U.S. 294, 301 (1987). Note that the "open field" doctrine dates back further than contemporary jurisprudence, but the emphasis on the sanctity of the home existed even in common law. Hester v. United States, 265 U.S. 57, 59 (1924) ("[T]he special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields. The distinction between the latter and the house is as old as the common law.").

27. California v. Ciraolo, 476 U.S. 207, 215 (1986) (allowing evidence of a patch of marijuana detected from a plane flying over the property); Kyllo v. United States, 533 U.S. 27, 37–38 (2001) (forbidding the use of thermal imaging technology to explore details of the home that would previously have been unknowable without physical intrusion; Justice Stevens, writing for the four dissenters, also hinged his argument on property principles, stressing that there was no "physical penetration" of the home).

Even though these decisions were ostensibly based on a person's reasonable expectation of privacy in his home, the Court approvingly quotes pre-*Katz* case law in *Kyllo v. United States*, stating, "'[a]t the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[28]

Even outside the home, the location of a potential piece of evidence is regarded as quite important. Courts have held that vehicles can be searched with probable cause sans warrant, even if the vehicle is used as a home.[29] Nowadays, if a closed container turns up during the search of the vehicle, the police can open the container if it is capable of containing the object of the search but from 1977 to 1982,[30] the "Court [drew] a curious line between the search of an automobile that coincidentally turns up a container and the search of a container that coincidentally turns up in an automobile."[31] Contrary to the relative inviolability of the home, here the simple placement of a container in a vehicle can make it more readily subject to search and seizure.

Use of these property analogies continues in dealing with intangibles, such as computer data. For example, many courts have taken an approach that classifies data stored in a computer as a form of "writing" or "record" and the computer itself as a "container."[32]

28. *Kyllo*, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

29. California v. Carney, 471 U.S. 386, 393–95, 406 (1985) (Stevens, J., dissenting) ("The motor home in this case, however, was designed to accommodate a breadth of ordinary everyday living. Photographs in the record indicate that its height, length, and beam provided substantial living space inside: stuffed chairs surround a table; cupboards provide room for storage of personal effects; bunk beds provide sleeping space; and a refrigerator provides ample space for food and beverages. Moreover, curtains and large opaque walls inhibit viewing the activities inside from the exterior of the vehicle. The interior configuration of the motor home establishes that the vehicle's size, shape, and mode of construction should have indicated to the officers that it was a vehicle containing mobile living quarters.").

30. United States v. Chadwick, 433 U.S. 1, 13 (1977) (holding warrantless searches of luggage/closed containers unconstitutional); California v. Acevedo, 500 U.S. 565, 580 (1991) (eliminating the warrant requirement for closed containers in a motor vehicle).

31. *Acevedo*, 500 U.S. at 580.

32. *See* United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998) (As most data is stored on "computers and computer disks . . . . [p]robable cause existed to search for and seize the computer-related property because probable cause existed to search for the records concerning the individuals and entities listed in the [warrant]."); United States v. Musson, 650 F. Supp. 525, 531–32 (D. Colo. 1986) (scope of search warrant for "'all records'" includes computer diskettes and the data therein); Frasier v. State, 794 N.E.2d 449, 454–55, 460 (Ind. Ct. App. 2003) (scope of search warrant for "'notes and records

Other courts have followed the lead of *United States v. Carey*, which acknowledged that "the file cabinet analogy may be inadequate" and ruled that law enforcement officers should take a "special approach" to the search and seizure of computer data.[33] This "special approach" entails a targeted search for the files that are the object of the warrant and instructions to law enforcement officers to not stray outside the scope of the warrant.[34] However, while this "special approach" purports to distinguish between a container and a computer storage system, courts generally treat the difference between the two as one of scale and not of inherent difference.[35] The *Carey* court attempted to explain the inadequacy of the "file cabinet" analogy by explaining that computers can store massive quantities of data and usually contain "intermingled" documents.[36] In other words, computer systems are still like file cabinets, just massive file cabinets containing a wide variety of files. The court in *United States v. Williams* acknowledged this while disagreeing with the *Carey* court, holding that "the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of

related to the sale of marijuana'" allowed search of computer files as well as physical records); People v. Loorie, 630 N.Y.S.2d 483, 485–86 (County Ct. 1995) (refusing to require a second warrant for the data contained in a seized computer by drawing analogies between the examination of the computer data located on the seized drives and "the removal of documents from an envelope; from the breast pocket of a nylon jacket; and from a locked briefcase.") (internal citations omitted); People v. Gall, 30 P.3d 145, 153 (Colo. 2001) ("computers found in the defendant's closet were reasonably likely to serve as 'containers' for writings, or the functional equivalent of 'written or printed material'" for purposes of the scope of the warrant); United States v. Lucas, No. 3:08CR-26-C, 2008 WL 4858197, at *6 (W.D.Ky. Sep. 23, 2008) ("[T]he electronic storage of such information is sufficiently widespread that a reference to 'records' in a consent to search form naturally may be assumed to include electronic versions of records, as well as hard copies thereof.").

33. United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); *see also* In re Search of 3817 W. West End, 321 F. Supp. 2d 953, 955, 957–58 (N.D. Ill. 2004) (holding that the "particularity" requirement for warrants and the potential of "intermingling" of documents on a computer allows a court to impose a requirement that the "government . . . provide a protocol outlining the methods it would use to ensure that its search was reasonably designed to focus on documents related to the alleged criminal activity."); People v. Carratu, 755 N.Y.S.2d 800, 807 (Sup. Ct. 2003) ("[A] warrant authorizing a search of the text files of a computer for documentary evidence pertaining to a specific crime will not authorize a search of image files containing evidence of other criminal activity.").

34. *Carey*, 172 F.3d at 1275.

35. *See id*.

36. *Id*.

documents."[37] Thus, regardless whether or not the "special approach" is used, courts still view computers as little more than containers or, at best, immense file cabinets.

These examples are not provided to disparage current analyses, but to provide a background for the methods that courts use in dealing with novel problems and their continued emphasis on analogies to physical objects. While *Katz* may have signaled an acknowledgment of the importance of intangible information as something that should be protected by the Fourth Amendment, this information is still treated as something tangible—something which can be seized and searched similar to one's "papers" or "effects." Application of *Katz*'s "reasonable expectation of privacy" test can be conducted by analogy to closed containers. In the United States Department of Justice manual regarding protocols for dealing with the search and seizure of electronic evidence, law enforcement personnel are instructed to "treat the computer like a closed container such as a briefcase or file cabinet."[38] While there is some debate over whether a computer is a single closed container or each file is a separate closed container,[39] the analogies to tangible property remain.

Suffice it to say that any attempt to formulate a new approach to Fourth Amendment jurisprudence for applications to new technologies must at least have its roots in property analogies. Professor Orin Kerr refers to computers as "virtual warehouses" and writes that "[t]he first step [in applying the Fourth Amendment to computers] should be to compare computers to homes and sealed containers."[40] In his article "The iPhone Meets the Fourth Amendment," Professor Adam Gershowitz acknowledges that the shift from early-generation cellphones to smart phones "drastically change[d]" the landscape, but also observes that courts continue to

37. United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010).

38. H. MARSHALL JARRETT ET AL., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 2–3 (2009), http://www.cybercrime.gov/ ssmanual/ssmanual2009.pdf.

39. *See* United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001) (holding that the scope of a search was exceeded when the police examined "more items within a closed container than did the private searchers" who had originally discovered evidence of wrongdoing); *Carey*, 172 F.3d at 1273–75 (holding that examining additional image files to find evidence of child pornography did exceed the scope of a search meant to search for evidence of drug sales).

40. Kerr, *supra* note 16, at 539, 549.

treat smart phones as "digital container[s]," albeit large ones.[41] In a recent article focusing on warrantless searches of smart phones, Matthew E. Orso argues that smart phones should be treated as computers.[42] If courts adopted this approach, courts would likely invalidate warrantless searches of smart phones,[43] and if there *were* a warranted search of a smart phone it would still be treated as what Kerr calls a "virtual warehouse."

II. Distinguishing Between Types of Information Accessible on and Via Smart Phones and the Untenability of Maintaining a Coding/Content Dichotomy

To understand better the amount and variety of information that can be stored on or accessed via a smart phone, it helps to categorize the data. A good starting point is to separate the data into "coding information" and "content-based information." Content-based information is the "substance" of data whereas coding information is information about the parties to a communication.[44] These two categories shall serve as our basic grammar. This Note divides each of these categories as follows: Where content-based information is concerned, we distinguish between data stored on the phone and data stored on remote servers (so-called "cloud" data). For coding information, we shall distinguish between data visible to the user and data hidden from the user. These distinctions are important to not only understand the wealth of information that is stored on smart phones, but also to assist in conducting an analysis of users' reasonable expectations of privacy in this data.

Courts and commentators have generally concluded that content-based information ought to receive more protection than coding information.[45] Content-based information is analogous to the

41. Gershowitz, *supra* note 15, at 38–41.

42. Matthew E. Orso, Note, *Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence*, 50 SANTA CLARA L. REV. 183, 223–24 (2010).

43. *Id*. at 224.

44. Orso, *supra* note 42, at 187–88.

45. Orso, *supra* note 42, at 193–94 (citing Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) *rev'd,* City of Ontario v. Quon, No. 08-1332, 560 U. S. __, (June 17, 2010)). The *Quon* cases address a situation in which the Ontario Police Department searched a SWAT team member's text messages for evidence that he violated the city's policy against using them for personal matters. *City of Ontario v. Quon*, slip op. at 2–5. The search revealed personal messages to his wife—some with sexual content—and messages to another SWAT team officer with whom he reportedly was having an

protected conversation in *Katz*.[46] By contrast, coding information is analogous to the unprotected, dialed phone numbers captured by a pen register.[47] In *Quon v. Arch Wireless*, the Ninth Circuit used this analysis to find that there is a reasonable expectation of privacy in the content of text messages.[48] While the Supreme Court reversed that decision in *City of Ontario v. Quon*, the Court assumed throughout its opinion that Quon had a reasonable expectation of privacy in the contents of his messages.[49] Nevertheless, when one delves even further into these categories, the distinctions between the two begin to blur for the purposes of privacy analysis.

Imagine that Smart Phone User A snaps a picture of her friend, Smart Phone User B, and then e-mails the photo to B with the message, "You look good!" The content-based information created and transferred during this exchange is not limited to the picture stored locally on A's smart phone, but also includes a copy of the photo and the message stored on a cloud email server.[50] The

affair. *Id*. Note that while the Supreme Court reversed the Ninth Circuit's decision, it declined to reach the issue of distinguishing between different categories of information and instead decided the case based on an analysis of an employee's reasonable expectation of privacy. *Id*. at 11–12. The Court did mention in dicta that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *Id*. at 11.

Yet, it seems clear that the Court has ways to go in understanding how to deal with the wide variety of information that is exchanged electronically. In the oral arguments, Chief Justice Roberts and counsel for respondent Quon shared a colloquy in which the Chief Justice stated that one "can't have a reasonable expectation of privacy based on the fact that their communication is routed through a communications company" and counsel responded that one would "expect that some company, I'm sure, is going to have to be processing the delivery of the message." Transcript of Oral Argument at 48:22-24:1-5, *Id*. (No. 08-1332). The Chief Justice responded, "Well, I didn't—I wouldn't think that. I thought , you know, you push a button; it goes right to the other thing." *Id.* at 49:3-5. Earlier, he wondered what happened when "he [Quon] is on the pager and sending a message and they're trying to reach him for, you know, a SWAT team crisis? Does he—does the one kind of trump the other, or do they get a busy signal?" *Id*. at 44:1-5.

46. *Katz*, 389 U.S. at 353.

47. *See Smith v. Maryland*, 442 U.S. 735, 742 (1979); *see also Arch Wireless*, 529 F.3d at 904, *rev'd,*No. 08-1332, 560 U. S.__, (June 17, 2010) (quoting *Smith v. Maryland*, 442 U.S. 735, 742 (1979)).

48. *Arch Wireless*, 529 F.3d at 910, *rev'd,* No. 08-1332, 560 U. S.__, (June 17, 2010).

49. *City of Ontario*, No. 08-1332, slip op. at 13. For more on the Court's decision, *see* supra note 45.

50. Without delving too deeply into the technical details of e-mail transfer protocols, when sending an e-mail from a smart phone or any other computer, a copy will be stored on at least one intermediate remote mail server. *See generally* Steven Baker, *Serving up mail: POP and IMAP*, UNIX REVIEW, Nov. 1996, at 25.

difference between local and cloud data is important: While Smart Phone User A has a locally stored copy of the picture, Smart Phone User B can view the content of the picture without permanently storing anything locally. In other words, Smart Phone User B (or the law enforcement officer searching her phone[51]) is not actually looking at a file on her phone,[52] but rather using the phone to peer at a picture stored at a remote location.

In addition to the content-based information, coding data is also transmitted from A to B, or more accurately, B's cloud. This data is composed of information visible to the user, such as information about when and to whom the email was sent. Additional information about the picture, data that is not readily visible to the user, is also sent. Such information includes the smart phone model, the time that the picture was taken, whether the picture was edited, and in some instances, the latitude and longitude of where the picture was taken, and even the name of the phone owner.[53]

The simple content/coding dichotomy shows its deficiencies when applying current Fourth Amendment jurisprudence to it. In *Smith v. Maryland*, the Court stated that allowing warrantless searches of the numbers dialed on a phone was allowable because the user voluntarily exposed information that the phone company had "facilities for recording and that it was free to record."[54] Following this line of analysis, the Ninth Circuit held in *United States v. Forrester* that computer surveillance used to obtain e-mail to/from addresses as well as website IP addresses visited by the defendant were "constitutionally indistinguishable . . . from the pen register that the

51. Email servers require authentication, usually in the form of a user name and password, which in this scenario raises issues of consent and whether a person should have a reasonable expectation of privacy in information which that has been protected by a password. However, in order to constrain the scope of this Note, we will assume that email is being accessed through an application that saves this authentication information. For further analysis on the effects that passwords have on this information see generally David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205 (2009).

52. This point may be disputed in that the picture is stored on the local cache during viewing, and may be stored locally for a short time thereafter. The local cache is an area within the memory storage of the phone to facilitate quick viewing of files. This illustrates yet another gray area in the classification of data, making it even more difficult to differentiate between local and remote data.

53. Johannes Ullrich, *Twitpic, EXIF and GPS: I Know Where You Did it Last Summer*, SANS INTERNET STORM CENTER (Feb. 10, 2010), http://isc.sans.org/diary.html?storyid=8203.

54. *Smith v. Maryland*, 442 U.S. at 745.

Court approved in *Smith,*" and that they "constitute addressing information and reveal no more about the underlying contents of communication than do phone numbers."[55] Using this line of reasoning, courts might reasonably conclude that much of the information discussed in the above example may be accessed by the government without triggering a Fourth Amendment analysis. Nevertheless, when the content-based and coding information categories are divided, it quickly becomes apparent that coding information can contain quite a bit of content and is more closely analogous to the *Katz* conversations than to the phone numbers in *Smith*.[56] Based on such an analogy, coding information is deserving of much greater Fourth Amendment protection than it has heretofore received.

A. Content-Based Information

1. Content-Based Information Stored on the Phone

United States v. Mercado-Nava

See *United States v. Forrester: An Unwarranted Narrowing of the Fourth Amendment*

. *Zamora*

Mercado-Nava

2. Content-Based Information Stored in the Cloud

Forrester *Smith v. Maryland*

Quon

. *Mercado-Nava*
. *Id.*
. *See Forrester*
. *See Arch Wireless,* *rev'd,*

Arch Wireless

See

City of Ontario

supra

How Privacy Vanishes Online
available at

supra

Arch Wireless

Live Folders

3. Overlap Between Local and Cloud Content-Based Information

e. Law enforcement can easily exceed the scope of the search without any sort of active wrongdoing on their part because the closed container[70] can seamlessly connect to remote virtual containers,[71] often without any clear demarcation between the two. To add to the ambiguity surrounding this area of law, the scope of the search will depend on whether it is conducted pursuant to a warrant or one of the exceptions to the warrant requirement. Each solution needs to balance both the needs of law enforcement on the one hand, and the protection of a person's *Katz*-prescribed "reasonable expectation of privacy,"[72] on the other.

a. Searches of Local and Cloud Data Pursuant to a Warrant

If a search is conducted pursuant to a warrant, the Fourth Amendment requires that the warrant shall "particularly describ[e] the place to be searched, and the persons or things to be seized."[73] When looking at the particularity requirement as applied to warranted smart phone searches, it is quite easy for a law enforcement officer to stray outside of "the place to be searched." This becomes quite important because if "officers' failure to realize the overbreadth of [a] warrant [is] objectively understandable and

developers.blogspot.com/2009/04/live-folders.html. Another example would be the "Dropbox" service that allows for the same functionality and has applications on the iPhone, Blackberry, and Android-based phones. DROPBOX, http://www.dropbox.com/anywhere (last visited Sept. 26, 2010).

70 , 486 F. Supp. 2d at 1277–78 (analogizing cell phones to closed containers).

71 United States v. D'Andrea, 497 F. Supp. 2d 117, 122 n.16 (D. Mass. 2007) (analogizing websites to a "file cabinet or other physical containers in which records can be stored").

72 , 389 U.S. at 360 (1967) (Harlan, J., concurring).

73. U.S. CONST. amend. IV.

reasonable," it doesn't invalidate the search.[74] This means that if a warrant specifies that a police officer can search a smart phone, he or she can venture far from the "place to be searched" with no negative consequences.

However, just because a law enforcement officer can enter into an area doesn't mean that they are operating within the constraints of the Fourth Amendment by doing so.[75] While scholars have not specifically addressed a warranted search of a smart phone and the difficulties in distinguishing those areas subject to a valid search, it stands to reason that allowing a search into any and all computers that may be connected to the phone can create an impermissibly broad search that violates a warrant's particularity requirement.

We need to create a framework whereby law enforcement may conduct smart phone searches but where the Fourth Amendment retains some teeth. If law enforcement is to remain within the bounds of a warrant to search a smart phone, the solution is to devise some way of demarcating between items that are stored on the phone and items that are stored remotely. There are features that allow a user to disable wireless access features of phones, thus preventing someone using the phone from delving into remote content.[76] If a smart phone does not have an "airplane mode" or something similar, other precautions can be taken to make sure that the scope of the search is not exceeded, such as manually disabling wireless connections.[77]

While it may seem hyperbolic at this juncture to compare the search of a smart phone to the general warrants that were one of the "important cause[s] of the American Revolution,"[78] as time passes and smart phones become more and more ubiquitous and widely connected to more and more computers, a search that is not confined to the local data on the smart phone could conceivably expand its

74. Maryland v. Garrison, 480 U.S. 79, 88 (1987).

75 , Garcia v. Dykstra, 260 F. App'x 887, 897-98 (6th Cir. 2008) (officers found a key by a padlocked storage unit and used it to enter and examine the premises, thus constituting an unwarranted search because by locking the unit, the owners retained a reasonable expectation of privacy in its contents).

76 , , http://support.apple.com/kb/ht1355 (last updated June 1, 2010) ("When airplane mode is on , . . . [n]o phone, radio, Wi-Fi, or Bluetooth signals are emitted from iPhone and Global Positioning System (GPS) reception is turned off, disabling many of iPhone's features.").

77 ,

78. United States v. Parcel of Land, Bldgs., Appurtenances & Improvements, Known as 92 Buena Vista Ave., Rumson, N.J., 507 U.S. 111, 118–19 (1993) (observing, "the misuse of the hated general warrant is often cited as an important cause of the American Revolution").

scope to reach computers worldwide and, perhaps more importantly, computers located in the home.[79] Although property analogies may be insufficient to describe fully the breadth and scope of the reach of a smart phone, Fourth Amendment jurisprudence continues to respect the sanctity of the home.[80] To allow a warranted search of a smart phone to give access to these other computers is stretching the scope of a warrant into areas in which people certainly have reasonable expectations of privacy.

b. Searches of Local and Cloud Data Pursuant to a Warrant Exception

The two exceptions to the Fourth Amendment warrant requirement that would most likely affect searches of smart phones (and cell phones in general) are the "search incident to arrest" and "exigent circumstances" exceptions. Each raises its own concerns, but as a preliminary issue, the argument that "an exigency exists merely because information is stored on a cellular phone" is a legal fiction that should be replaced by a more coherent standard that comports with the policy reasons for the exception.[81] The exigency exception to the warrant requirement exists to deal with a certain type of situation. There are three basic situations in which an exigency is justified: "if lives are threatened, a suspect's escape is imminent, or evidence is about to be destroyed."[82]

The argument for exigent circumstances based solely on the fact that the item being searched is a cell phone attempts to use destruction of evidence as their justification. A court using the exigency exception reasons that if the owner of the phone receives a call, this may delete or overwrite an earlier stored number.[83] In , a good example of this type of case, the court justifies this "exigency" by claiming that law enforcement "had the authority to immediately search or retrieve . . . the cell phone's memory of stored numbers of incoming phone calls, in order to prevent the destruction of evidence."[84] The court's reasoning is faulty for two related reasons. First, the evidence of calls is not destroyed

79 notes 24–27.

80 , 533 U.S. 27 at 37 (discussing the "Fourth Amendment sanctity of the home").

81. Orso, note 42, at 196.

82. United States v. Ball, 90 F.3d 260, 263 (8th Cir. 1996) (citations omitted).

83 , 289 F. Supp. 2d at 1303–04.

84 at 1304.

because the cellular service provider stores this information.[85] Second, the service provider's storage makes this information available by warrant. While this may seem redundant, it is worth recalling that the Fourth Amendment evinces a "strong preference for searches conducted pursuant to a warrant"[86] and unless circumstances fall under one of the three "narrowly drawn" exigency exceptions, the search cannot be justified.[87] While courts afford some deference to the "reasonableness of the officer's belief that exigent circumstances existed,"[88] the Supreme Court has continually held that "the police bear a heavy burden when attempting to demonstrate an urgent need that might justify warrantless searches or arrests."[89] Unless there is some other exigency that can be demonstrated (and one in particular will be discussed in Part III), the mere fact that the item being searched is a cell phone should not be considered exigent circumstances that would allow a warrantless search.

However, one might suggest that a warrant exception in the case of a cell phone justifies an exigency in the case of a smart phone simply due to its ability to connect to remote computers. In other words, because a smart phone can access remote computers and these computers may have information on them which could be deleted or overwritten, the situation calls for a warrantless search to prevent the destruction of evidence. This is clearly outside the scope of the policy reasons for the exigent circumstances exception, especially if the safeguard of switching the phone to a mode which limits all wireless access is used.[90] Limiting wireless access protects both the privacy rights of the individual and allows law enforcement officers to prevent access to the remote computers for the duration of the search. If

85. Orso, note 42, at 199 n.68 ("A cellular phone user for the past nine years, the author has received a statement every month listing all incoming and outgoing calls and text messages. This experience has been consistent among three separate cellular phone companies—Verizon, U.S. Cellular, and TMobile—during this time period. Therefore, it seems safe to assume that cellular companies do, in fact, retain records of incoming and outgoing calls and text messages.").

86. Illinois v. Gates, 462 U.S. 213, 236 (1983).

87. United States v. Clement, 854 F.2d 1116, 1119 (8th Cir. 1988).

88 (citing United States v. Selberg, 630 F.2d 1292, 1295 (8th Cir. 1980)); United States v. Miller, 430 F.3d 93, 97-98 (2d Cir. 2005); United States v. Martins, 413 F.3d 139, 150 (1st Cir. 2005); United States v. Davis, 588 F. Supp. 2d 693, 702 (S.D. W.Va. 2008).

89. Welsh v. Wisconsin, 466 U.S. 740, 749–50 (1984).

90. Furthermore, even data that has been deleted can be recovered using certain forensic tools. Jeannine Heinecke, , LAW ENFORCEMENT TECH., Nov. 1, 2007, at 62.

there is a situation in which law enforcement believes that evidence is stored on remote computers, a warrant is the proper method for retrieving it.

The other important warrant exception in which smart phones might be implicated is when a search is conducted incident to arrest. In , the Supreme Court explained the rationale and scope of this warrant exception:

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction.[91]

In *New York v. Belton* *Chimel*

United States v. Finley

Belton

Finley

United States v. Park

Finley

Park

. *Id.*

supra

Finley *Finley*

Park
Chimel

Park

Ohio v. Smith
Finley *Park*

. *Id.*
. *Id.*
. *Id*
. *Id*
. *Id.*
. *Id.*
. *Id.*
Chimel

Park

Smith

Park *Smith*

cert. denied

Id.

See supra

Smith

Smith

Id.

Id.

. *Chimel*

supra

B. Coding Information

1. Visible to the User

See, e.g., *Completely Erase your iPhone's Data*

How to reset a Motorola Droid

How do I reset my BlackBerry?

BlackBerry%3F (last visited Sept. 10, 2010) (even a soft reset which merely "re-establishes communication between the Blackberry device and the computer" requires holding three keys simultaneously).

113. *See, e.g.*, United States v. McCray, No. CR408-231, 2009 WL 29607, *4 (S.D. Ga. 2009) ("In this case, the officers seized McCray's cell phone from his pocket after developing probable cause to believe that he had enticed a 14-year-old girl to engage in a sexual act. Initially, the phone was placed on the tail gate of [defendant] McCray's pickup truck. But after the discovery of the crack cocaine and the Polaroid photograph depicting a naked adult female, Officer Balmer concluded that the phone's camera function might contain evidence of either drug trafficking and/or molestation of a minor. Accordingly, he briefly reviewed the images stored in the phone's memory. After finding lewd images of J.W. on the phone, he secured the phone as evidence and for further review by SCMPD detectives, who secured a warrant before conducting a more comprehensive search of the phone.").

matter of that communication."[114] This encompasses "phone numbers, email addresses, pager numbers, and other labeling information that uniquely identifies an account"[115] in addition to the date/time information associated therewith. For the most part, the coding information visible to the user should be treated as similar to any of the data stored locally, because it is nearly always visible on the same screen as any content information. Nevertheless, because coding information is so readily analogous to the information that is aggregated by pen registers and trap and trace devices without it even constituting a search,[116] courts may attempt to leverage this into allowing a search of the phone. Recall that a smart phone's versatility poses a unique problem: whereas coding information in other contexts may be readily viewed or captured separate from its accompanying content,[117] in the context of both warranted and warrantless searches of smart phones, it often exists side-by-side with content-based information.[118]

2. Invisible to the User

The definition of coding information in this Note is a bit more expansive than that proposed by earlier commentators.[119] In addition to information about the parties to a given communication, our definition also encompasses data that may be invisible to the user of the phone. This data may include everything from information about the date and time a certain file was created or modified to the latitude and longitude of the user when they snapped a picture with their smart phone.[120]

As this data can generally only be accessed by savvy users and sometimes only if files are transferred to computers, it seems as if this data is relatively safe from governmental intrusion. However, due to

114. *See* Orso, *supra* note 42, at 187–88.

115. *Id.*

116. *See, e.g.*, *Smith v. Maryland*, 442 U.S. at 742.

117. *See* Orso, *supra* note 42, at 190 (comparing exposing dialed telephone numbers to the phone company and exposing address information on a letter to cell phone coding information).

118. For an excellent discussion of the patent deficiencies in upholding searches on grounds that the coding data in question was exposed for interception by service providers, see Orso, *supra* note 42.

119. *See* Orso, *supra* note 42, at 188 ("Coding information describes data that reveals only the identity of a party to a communication without disclosing the subject matter of that communication.").

120. Ullrich, *supra* note 53.

the probative nature of this information and its potential future use by law enforcement,[121] it is worth considering in this analysis. That said, due to its nature as "invisible" coding information, it is highly unlikely that this information would show up during a search conducted pursuant to any of the warrant exceptions. Instead, it would most likely be revealed during a warranted search.

The fact that this information will generally be viewed pursuant to a warrant, which must "particularly describ[e] the place to be searched, and the persons or things to be seized,"[122] means that many of the concerns of scope raised by warrantless searches are alleviated. Despite the foregoing, it is not entirely clear if the scope of a search warrant encompasses this "information about information." To demonstrate, consider a hypothetical warrant allowing law enforcement to search a smart phone for evidence of pictures of child pornography.[123] While police officers find no evidence of child pornography, they see what looks to be drug paraphernalia in some of the pictures. Having access to the location and date/time information about the photo can characterize the paraphernalia in many different ways, from identifying a residence (or any location) that law enforcement might believe they have probable cause to search or establishing that the picture was innocently taken at a police drug demonstration on a school campus. Here, suppose that the warrant clearly established that law enforcement was directed to look for pictures (content-based information, in other words), but instead discovered potentially damning information that is arguably outside the scope of the search (metadata). While the warrant did not specifically authorize a search of the location and time of the pictures,

121. At the beginning of 2010, an image containing what appeared to be lines of cocaine was posted to 4chan.org, a popular Internet message board with the message "Long day at the office, you would not BELIEVE where the office is [by the way]." The subsequent poster examined the EXIF ("exchangeable image file format"—"invisible" coding data) information of the image file and identified the location of the image as being taken at the White House. It was quickly picked up by various social networking sites and blogs, until many dismissed it as a hoax. While this particular incident may demonstrate the abilities of a savvy user to mislead with this information, it is most certainly illustrates the potential for extracting probative information from this data. *See* Sara K. Smith, *Exciting White House Scandal Was Just A Prank!*, WONKETTE (Jan. 15, 2010, 11:00 AM), http://wonkette.com/413200/exciting-white-house-coke-scandal-was-just-a-prank.

122. U.S. CONST. amend. IV.

123. The setup of this hypothetical is somewhat similar to the facts of *United States v. McCray*, No. CR408-231, 2009 WL 29607 (S.D. Ga. 2009), in which a search incident to arrest revealed some incriminating pictures of a minor and led to a warranted search of the phone.

the data was nonetheless revealed to law enforcement.[124] Does law enforcement simply get to use this information as a "bonus" even though the user may not have even been aware that the phone was recording this information?

Though this information will likely be revealed pursuant to a warrant, the "plain view" warrant exception is often used as the justification for straying outside the scope of the warrant.[125] The plain view doctrine is an exception to the warrant requirement, which allows officers to seize evidence found in plain view during a lawful observation.[126] It requires that the officer be (1) lawfully present at the vantage point from which the evidence is viewed, that he (2) have "lawful right of access to the object" and, (3) that the "incriminating character" of the object be "immediately apparent."[127] Professor Orin Kerr writes about the dilemma of "balanc[ing] the threat of general searches against the public benefit of recovering additional evidence."[128] While speculating on some of the potential solutions to this problem, he tentatively advocates abolishing the plain view exception for digital evidence searches.[129] He justifies this both in terms of public policy and practical concerns:

> Eliminating the plain view exception in digital evidence cases would respect law enforcement interests by granting the police every power needed to identify and locate evidence within the scope of a warrant given the particular context-sensitive needs of the investigation. At the same time, the approach would protect privacy interests by barring the disclosure of any evidence beyond the scope of a valid warrant in most cases . . . . In short, it would allow the police

124. It is likely that law enforcement will see this data, even if this is not the object of their search nor do they actively seek it out, as metadata is often used to, ironically enough, limit the scope of the search. *See* Derek Haynes, Comment, *Search Protocols: Establishing the Protections Mandated by the Fourth Amendment Against Unreasonable Searches and Seizures in the World of Electronic Evidence*, 40 MCGEORGE L. REV. 757, 772 (2009) ("Metadata is another valuable way to limit the scope of a search without unduly burdening the government's interests in effective law enforcement.").

125. *See, e.g.*, United States v. Adjani, 452 F.3d 1140, 1151 (2006) ("There is no rule . . . that evidence turned up while officers are rightfully searching a location under a properly issued warrant must be excluded simply because the evidence found may support charges for a related crime (or against a suspect) not expressly contemplated in the warrant.").

126. Horton v. California, 496 U.S. 128, 135–137 (1990).

127. *Id.* at 136–37 (quotations omitted).

128. Kerr, *supra* note 16, at 571.

129. *Id.* at 582–83.

> to conduct whatever search they needed to conduct (to ensure recovery) and then limit use of the evidence found (to deter abuses).[130]

This seemingly radical approach has been adopted in part by the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, in which it held that "the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it gained access only because it was required to segregate seizable from non-seizable data."[131] In other words, the use of electronic forensic tools[132] and/or methods designed to probe the data for illegality are precluded without specific authorization in the warrant.[133]

The situation that the Ninth Circuit addressed in *Comprehensive Drug Testing, Inc.* is distinct in that it deals with intermingled discrete documents,[134] instead of a piece of data that is attached to the file itself. Yet, the idea of forswearing the plain view doctrine is a useful one for "invisible" coding data, especially because this coding information can contain information that can reasonably be categorized as content. The rapid proliferation of smart phones may be the first step of the "new dynamics of digital evidence collection and retrieval" and may further justify doing away with the plain view requirement as a "sound doctrinal response to the new dynamics of digital evidence collection and retrieval."[135]

III. Remote Access of a Smart Phone's Contents

. *Id.*

Comprehensive I *rev'd en banc*

. *See supra*

. *Comprehensive I*

. *Id.* *cf.* *supra* *United States v. Tamura*

Comprehensive I

supra

. *See e.g.* *Inside iPhone 3.0's Remote Wipe Feature*

available at

. *See e.g.*

. *See supra*

See supra

Clement

. *See, e.g.,*

142. Evidence tampering is a statutory crime. *See* MODEL PENAL CODE § 241.7 (2001) (holding a person liable for a "misdemeanor if, believing that an official proceeding or investigation is pending or about to be instituted, he: (1) alters, destroys, conceals or removes any record, document or thing with purpose to impair its verity or availability in such proceeding or investigation; or (2) makes, presents or uses any record, document or thing knowing it to be false and with purpose to mislead a public servant who is or may be engaged in such proceeding or investigation").

criminal liability to wipe the phone, law enforcement can use the same precaution advised above to limit the scope of searches from straying needlessly into the "cloud"; namely, the police officer can put the phone in a mode that doesn't allow wireless communications.[143] Just as this method prevents law enforcement from accessing remote computers from the smart phone, it also will prevent access to the smart phone from remote computers.

The challenges in applying the Fourth Amendment to new and changing technologies are numerous and require a mix of precedent, policy, and pragmatism to address them thoroughly. However, getting the correct mixture of the three can be difficult. While courts may continue to rely upon property analogies in dealing with Fourth Amendment issues, they should take care to make sure that the analogies do not oversimplify the issue. Further, they should consider using the model proposed in this Note to assist with distinguishing among data that can be accessed in a search of a smart phone.

A smart phone, by virtue of its versatility, is distinct from its pager and cell phone predecessors. Likewise, a smart phone's mobility and peculiar social niche distinguish it from the common computer. Therefore, while Fourth Amendment jurisprudence for either may seem analogous, courts should recognize that smart phones have their own unique characteristics and contains a wealth of data that neither cell phones nor computers have.

Categorizing the data found on a smart phone both clarifies and confuses. While it helps to delineate between types of information and separately consider the privacy expectations in each, the demarcation is essentially artificial and may sometimes be quite blurry. To muddy the waters even further, each search should be separately considered in a warrant context and pursuant to a warrant exception.

In the context of a search pursuant to a warrant, the most important concern is that of scope. The scope of a warranted search is constitutionally confined by the particularity of the warrant.[144] Courts must be careful not to let law enforcement exceed the scope of a warrant to search a smart phone simply by virtue of the fact that the lines between different data are hard to discern. There are

143. *See supra* Part II.A.iii.a.

144. U.S. CONST. amend. IV.

techniques to prevent encroachment onto remote computers[145] and to prevent remote computers from encroaching onto the search.[146] It is even possible that smart phones may be the devices that usher in the abolishment of the plain view doctrine as applied to warranted searches.[147]

The scope of the search is also important when considering a search pursuant to a warrant exception. It is in light of this concern that an "exposure-based approach" seems useful.[148] Professor Orin Kerr defines a Fourth Amendment search as occurring "when [metadata] is exposed to possible human observation" and uses this to bridge the "physical world notions of searches to the context of computers."[149] This means that whenever government agents see a piece of information, whether it is content-based information or coding data, they must have a rationale for that search. While other commentators have posited different techniques for limiting the scope of an unwarranted search of a smart phone,[150] it seems parsimonious to simply limit a search incident to arrest to the presently exposed screen on the phone. The concerns regarding destruction of evidence can be eliminated, or at least reduced, by switching off the wireless connection.[151] Furthermore, if there is a great concern regarding evidence that might be on the phone and would help resolve an emergency, this would constitute exigent circumstances that would justify a warrantless search. Otherwise, law enforcement can obtain a warrant as the Fourth Amendment usually prescribes.

The full potential of smart phones has yet to be seen, but it seems certain that their popularity will only continue to grow. As they reach ubiquity, both in society and in people's lives, the expectation of privacy in them will increase. It is important that courts set standards that balance the needs of law enforcement with the peoples' reasonable expectations of privacy to arrive at a conclusion that comports with the Fourth Amendment and is readily administered.

145. *See supra* Part II.A.iii.a.

146. *See supra* Part III.

147. *See* Kerr, *supra* note 16, at 571, 582–84.

148. *Id.* at 551.

149. *Id.*

150. *See, e.g.*, Gershowitz, *supra* note 15, at 44–57.

151. While these two proposals may be seen as inherently contradictory in that a law enforcement official would have to go beyond the presently exposed screen to shut off the wireless connection, this would only be done in the case of an exigency, which would provide the justification for going beyond the presently exposed screen. *See supra* Part II.A.iii.a.

We are witnessing an explosion of technological growth. The issues that are now emerging do not conform to the tidy analogies to the rules that governed the comparably slow technological evolution encountered by previous generations. To the extent that the digital age has led us into uncharted waters, this Note represents a new cartographic method. While it certainly does not consider every eventuality, it maps out the contours of information in a way that should have some conceptual stability. Further, it is built on a premise that no one should reject—that the reasonableness of a search should derive from the pre-legal expectations of the people, rather than from the legal fictions that sometimes arise when recently minted round pegs are forced into outmoded square holes.

***