CONSTITUTIONAL LAW—PROACTIVE CELL PHONE SECURITY POLICIES IN THE WORKPLACE: AVOID LIABILITY AS HI-TECH DEVICES *HACK* THE FOURTH AMENDMENT

I. INTRODUCTION

If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner.[1]

You are an attorney. Your practice focuses on helping doctors avoid malpractice liability. One of your clients is a family doctor who integrated smartphones in the workplace to facilitate accessing patient charts,[2] dictating notes, and storing client contact information. A few months after the upgrade, the doctor visits your office and is concerned that she may have compromised her patients' confidential medical information.

The doctor explains that while driving to work one morning, a police officer stopped her for displaying an expired registration sticker. After approaching the vehicle, the officer recited the standard request for documents: "License, proof of insurance, and vehicle registration, please." After receiving the documents, the officer said, "I am also going to need to see your cell phone."[3] Confused with the peculiar request, the doctor replied, "Why do you need to see my phone? Do I have to let you see it?" Responding, the officer took a serious tone and said, "Yes, I need to see your phone. What are you trying to hide, anyway? If you are not doing anything illegal, what are you worried about?" The doctor, complying with the request, then said, "Fine, here it is. I won't give you my password, though." Smiling, the officer took the phone.

While the officer entered the license and registration information into the police database, he also connected the doctor's smartphone to a seemingly innocuous gadget: a Universal Forensic Extraction Device (UFED), one of the station's new cell phone surveillance tools.[4] The UFED allowed the officer to bypass the doctor's password and quickly download every

---

1. *See* BRIAN J. S. CHEE, CURTIS FRANKLIN, JR., CLOUD COMPUTING: TECHNOLOGIES AND STRATEGIES OF THE UBIQUITOUS DATA CENTER 145 (2010) (quoting General Omar N. Bradley).

2. AmazingCharts Inc., an electronic health record software provider, announced a new software "App" that gives medical practitioners mobile access to their Amazing Charts Electronic Health Records from an iPhone, iPod Touch, and iPad. *Amazing Charts EHR Now Has An IPad/Iphone Mobile Application*, THE MEDICAL QUACK (Jan. 29, 2011), *available at* http://ducknetweb.blogspot.com/2011/01/amazing-charts-ehr-now-has-ipadiphone.html

3. *The price of privacy*, THE TIMES (Apr. 26, 2011), *available at* 2011 WLNR 8100431.

4. *See infra* Part II.

email, text message, picture, calendar appointment, contact entry, stored GPS location, as well as other passwords stored on the phone[5]—in just under two minutes.[6] When the officer returned with the cell phone, he informed the doctor that he found no contraband and that the phone was "clean." Puzzled, the doctor asked how the officer was able to bypass the password and access the phone. The officer replied, "We have some pretty neat gadgets." Immediately after this incident, the doctor drove to your office to discuss potential Health Insurance Portability and Accountability Act (HIPPA) liability for exposing her patient's confidential information.

In just two minutes, the hypothetical client presented above compromised the security of her information system, while increasing her liability. This problem is not an Orwellian fiction or academic creation: it is a reality.[7] In Michigan, for example, police agencies are deploying UFEDs in everyday traffic stops,[8] gaining access to highly sensitive information without a warrant.[9] Like the hypothetical, the Michigan State Police bypass the warrant requirement of the Fourth Amendment by obtaining consent from drivers, even if the driver believes the password on their phone will prevent the police from performing any meaningful search. Alternatively, if a driver is arrested for even some minor traffic violations, the police may perform the same search without a warrant, under the search-incident-to-arrest exception to the Fourth Amendment.

This issue underscores many modern challenges to the Fourth Amendment. From a world constructed of brick and mortar to the virtual world built of RAM and gigabytes, many Fourth Amendment principles fail to *transmit* across the digital divide between the new and old worlds.[10] Alt-

---

5. Many smartphones use internal applications generally referred to as "keychains," which automatically store passwords once used on a device. *See* William Dalsen, *Civil Remedies for Invasions of Privacy: A Perspective on Software Vendors and Intrusion Upon Seclusion*, 2009 WIS. L. REV. 1059, n. 35 (2009) (citing APPLE INC., *Mac OS X Security: Keeping Safety Simple* 3–4 (2007)).

6. *A Sneaking Suspicion Privacy is Being Invaded: High-Tech Devices Grab Personal Info From Cell Phone – Without You Knowing*, THE STAR LEDGER (Apr. 23, 2011), *available at* http://blog.nj.com/njv_editorial_page/2011/04/a_sneaking_suspicion_that_priv.html.

7. *Id.*

8. Ed Walters, *Smartphones: Searchable by Police?*, FASTCASE (May 4, 2011), *available at* www.fastcase.com/smartphones-searchable-by-police/ ("[I]n Michigan, state police are using a customized piece of hardware to extract cell phone data from drivers during traffic stops.").

9. The Michigan State Police disavow these reports, stating that the UFED is only used if a search warrant is obtained or if the person possessing the mobile device consents; however, they refuse to grant the American Civil Liberties Union's Freedom of Information Act requests. Kathy Barks Hoffman, *Cell phone data extraction questioned by ACLU*, ASSOCIATED PRESS (Apr. 22, 2011), http://sg.news.yahoo.com/cell phone-data-extraction-questioned-aclu-151808893.html.

10. *See infra* Part IV.

hough "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,"[11] a circuit split has caused many judges to question whether a person's cell phone is subject to a warrantless search.[12] While this split has existed for some time,[13] the Supreme Court of the United States very recently denied certiorari to rule on the issue and resolve the conflict amongst the lower courts.[14] Instead, the Court's position is that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[15] This approach, however, fails in an age of rapid technological expansion, where new technologies like cell phones are becoming so prevalent in modern society. [16]

The rapid growth of technology has also overcome the business world. Many businesses even provide their employees with cell phones and have handbook policies regulating use and security.[17] A typical policy requires an employee to use a software password program to block unwanted access to their phones.[18] Such practices, however, fail when confronted with the government's modern surveillance technology.[19] Even the most sophisticated password would not stop the UFED.[20] Nor will any handbook policy. Our

---

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

12. If the courts find that a reasonable expectation of privacy exists in a cell phone, then police generally need to acquire a warrant to search it, unless one of the many exceptions to the Fourth Amendment applies. *See* United States v. Finley, 477 F.3d 250 (5th Cir. 2007) (reasonable expectation of privacy in the call records and text messages on the cell phone); United States v. Jones, 149 F. App'x 954 (11th Cir. 2005) (no reasonable expectation of privacy in text message pager).

13. *See infra* Part IV.

14. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds*, City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010) (declining to rule directly on the issue). Additionally, two state supreme Courts have considered the issue and reached divergent results. State v. Smith, 124 Ohio St.3d 163, 2009-Ohio-6426, 920 N.E.2d 949 (Ohio 2009) (cell phone search not permissible without a warrant); People v. Diaz, 244 P.3d 501, 1199 (Cal. 2011), *cert. denied* Diaz v. California, 132 S. Ct. 94 (2011) (warrantless cell phone search acceptable).

15. *Quon*, 529 F.3d 892 (9th Cir. 2008);*City of Ontario, Cal.*, 560U.S. at 746.

16. "Moore's Law," for example, is a theory that forecasts the doubling of computer processing speeds every eighteen months. *10 things you never knew that your mobile could do*, IRISH INDEPENDENT (Feb. 1, 2012), *available at* 2012 WLNR 2146847; *see* Jonathan H. Lemberg, note, *Semiconductor Protection: Foreign Responses to a U.S. Initiative*, 25 COLUM. J. TRANSNAT'L L. 345, n. 27 (1987) (citing Robert Noyce, *Microelectronics*, 237 SCIENTIFIC AMERICAN 65 (Sept. 1977)); *see* Jim Stafford, *Moore's Law still the industry standard for computers*, DAILY OKLAHOMAN (Oct. 10, 2006), *available at* http://newsok.com/moores-law-still-the-industry-standard-for-computers/article/2953869 .

17. *See infra* Part IV.

18. *See infra* Part IV.

19. *See infra* Part IV.

20. The Cellebrite UFED is one of the more popular cell phone data extraction devices, but it is not the only data extraction device on the market. Martha McKay, *Why cops love it*,

technology has grown so rapidly that even our most sacred constitutional rights cannot keep pace.[21]

This problem exposes law-abiding businesses to unnecessary liability. One thing is certain: workplace password-protection policies are ineffective in the age of government data mining[22] with UFEDs. Until the Court or Congress ensures that the Fourth Amendment's protections extend into the twenty-first century, citizens and businesses that may otherwise want to cooperate with police cannot in fear of breaching client confidences. In the interim, businesses must rewrite cell phone security policies to protect confidential client information.

Cellular phones in the business setting have many uses, and this Note will demonstrate why businesses must respond appropriately to safeguard sensitive information contained on cell phones, in light of the UFED and other forthcoming surveillance technologies. Part II will provide an overview of current cell phone technology, as well as emerging mobile forensic technology used to extract mobile device data. Part III considers Fourth Amendment jurisprudence regarding warrantless cell phone searches, the two approaches courts have taken in the circuit split, and recent issues of technology and the Fourth Amendment considered by the Supreme Court.

---

and suspects hate it, NEW JERSEY RECORD (Feb. 14, 2008), *available at* 2008 WLNR 2872420. Other products, such as the "Mobiledit! Forensic" and "Cell Seizure," which use different methods to extract and analyze data, exist as well. *Id.* Cellebrite has 'a big advantage in the forensics world,' however, because it has access to new cellular handsets before they are launched commercially. *Id.* Cellebrite's commercial customers, such as Verizon Wireless, AT&T, Sprint/Nextel, T-Mobile UK, and Orange France, send their handsets to Cellebrite prior to commercial launch to make sure Cellebrite's synchronization boxes work with every phone. *Id.*

21. For instance, the major federal statute on technological surveillance was written in 1986, before the World Wide Web even existed. *See* 47 U.S.C. § 1002(a)(1) (West 2011).

22. "Data mining" is a broad term with varying definitions depending on the context in which it is used. *See* Informatica Corp. v. Bus. Objects Data Integration, Inc., 489 F. Supp. 2d 1060, 1071 (N.D. Cal. 2007). One court has accepted a definition of data mining in a government-search context as "searches of one or more electronic databases of information concerning U.S. persons, by or on behalf of an agency or employee of the government." *Elec. Privacy Info. Ctr. v. Dep't of Def.*, 355 F. Supp. 2d 98, 101 n. (D.D.C. 2004). Similarly, the Federal Agency Data Mining Reporting Act of 2007 defines "data mining" as "a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where" a federal agency conducts:

> [Q]ueries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals, the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and the purpose of the queries, searches, or other analyses is not solely the detection of fraud, waste, or abuse in a Government agency or program; or the security of a Government computer system.

42 U.S.C. § 2000ee-3 (West 2012). This Note construes the term "data mining" as describing the accumulation of personally identifiable information by a government agency.

Part IV considers typical cell phone security policies in the workplace, providing practical recommendations to reduce liability while the Court and Congress remain silent. Then, it examines how the Court's lack of guidance on the issue, as well as Congress's legislative inaction, exposes employers with a cell phone-equipped workforce to unnecessary liability. Part V will argue that the Court's refusal to accept the *virtual* reality of the Fourth Amendment is a dereliction of its sacred obligation.

II. MOBILE TECHNOLOGY AND SURVEILLANCE

The ubiquity of cell phones is a worldwide phenomenon.[23] The International Telecommunications Union, a United Nations agency for information and communication technologies,[24] estimates that by the end of 2011 5.9 billion mobile-cellular subscriptions will exist worldwide.[25] American workplaces have embraced this technology, but as it has developed, so too have their security policies.[26] To begin a discussion of cell phone security policies in the workplace, this section will provide an overview of current cell phone technology, the types of data stored by and on mobile phones, and the surveillance technology the government uses to obtain the data stored on cell phones.

A. Mobile Phone Technology

There is a sharp divide between "cell phones" and "smartphones";[27] however, there is no precise demarcation line between the two.[28] A modern smartphone can hold "hundreds or thousands of messages, photographs, videos, maps, contacts, financial records, memoranda and other documents,

23. City of Ontario, Cal. v. Quon, 560 U.S. 746, 760 (2010) (ubiquity of cell phones made them affordable); *ICT Facts and Figures*, INTERNATIONAL TELECOMMUNICATIONS UNION, http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf (last visited Feb. 25, 2012).

24. INTERNATIONAL TELECOMMUNICATIONS UNION, *supra* note 23.

25. *Id.*

26. Perkins Coie, *Electronic Workplace*, OREGON EMPLOYMENT LAW LETTER 12 NO. 4 OR. EMP. L. LETTER 6 (Dec. 2005).

27. Sprint Nextel Corp. v. AT & T Inc., 821 F.Supp.2d 308, 320 n.20(D.D.C. 2011) ("The 'most innovative handsets' are smartphones, 'which integrate computer operating systems with phone capabilities and high resolution cameras' ").

28. Daniel Zamani, *There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones*, 38 HASTINGS CONST. L.Q. 169 (2010).

as well as records of the user's telephone calls and Web browsing."[29] A smartphone is "essentially a small computer."[30] Additionally, most mobile phone handsets, in compliance with the Federal Communications Commission's "E9-1-1" regulations,[31] are equipped with location-identifying technology designed to assist emergency responders locate individuals.[32] Indeed, the list of smartphone capabilities is growing, from the ability to "chat with friends, update social network profile[s], blog, tweet, prepare a presentation, prepare official reports, route your way through treacherous trails, see weather reports, [and] book plane tickets,"[33] to even opening garage doors, turning off your home lights remotely, and monitor home security cameras.[34]

The difference between cell phones and smartphones is the presence of robust operating systems in the latter.[35] The software integration of operating systems like those found on desktop or laptop computers provides increased utilization of typical computer functions, including the ability to install third-party software suites,[36] commonly referred to as "apps."[37] For example, the hypothetical client used HIPAA compliant software called "AmazingCharts."[38] AmazingCharts, a $24.99 smartphone app, allowed the doctor to access and review patient charts while away from the office.[39] One commentator observed, "[t]he beautiful thing about computers,

---

29. People v. Diaz, 244 P.3d 501, 513 (2011) *cert. denied,* 132 S. Ct. 94 (2011) (Werdegar, J., dissenting) (citing http://www.pcmag.com/encyclopedia_term/0,2542,%20t=Smartphone&i=51537,00.asp [as of Jan. 3, 2011].).

30. People v. Nottoli, 130 Cal. Rptr. 3d (Cal. App. 6th Dist. 2011).

31. 47 U.S.C. § 1002 (West 2011).

32. 47 U.S.C. § 1002 (West 2011).

33. *A world on your palms*, SKILLS AHEAD (Aug. 5, 2011), *available at* 2011 WLNR 15593196.

34. Many home automation providers now offer iPhone and iPad apps, bringing smart homes into the twenty-firstcentury. *See* Lisa Shearon, *smart HOMES*, SUNDAY TIMES (July 10, 2011), *available at* 2011 WLNR 13598611.

35. For a discussion of nomenclature and some of the nuances between cell phones and smartphones, see Vangie Beal, *The Difference Between a Cell Phone, Smartphone and PDA*, WEBOPEDIA.COM, http://www.webopedia.com/DidYouKnow/Hardware_Software/2008/smartphone_cell phone_pda.asp (last updated Aug. 31, 2010).

36. Wayne Jansen & Karen Scarfone, *Guidelines on Cell Phone and PDA Security*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (October 2008), https://www.nsi.org/pdf/reports/NIST%20Cell%20Phone%20and%20PDA%20Security.pdf .

37. *See* Juliana Hoyt, *Getting Up to Speed: Tech Savvy Tips for ADR Professionals A Mile Wide, Inch Deep Review of Online Resources for Your Business*, 36 VT. B.J. 44, 45 (2010) (discussing applications and calling them "apps").

38. *Amazing Charts EHR Now Has An IPad/Iphone Mobile Application*, THE MEDICAL QUACK (Jan. 29, 2011), *available at*http://ducknetweb.blogspot.com/2011/01/amazing-charts-ehr-now-has-ipadiphone.html .

39. *Id.*

smartphones, and electronic medical records is that [they make it] amazingly easy to store, access, and share information," yet, "[t]he terrifying thing about computers, smartphones[,] and electronic medical records is that [they make it] amazingly easy to store, access, and share information."[40] "Technology is a double-edged sword."[41] With the proliferation of mobile technology in society, many business settings have incorporated mobile devices into the workplace and must balance the *beautiful* against the *terrifying*.

B. Methods To Intercept Electronic Communications

Businesses are not alone in using cell phones to facilitate their productivity. Criminals also use cell phones to facilitate their *productivity*.[42] In response, mobile surveillance technology advanced to allow the government to obtain evidence in criminal investigations. These methods fall into two general categories: statutory requirements placed on service providers to allow the government to intercept electronic communications[43] and forensic processes to physically extract data from mobile handsets.[44] This section provides a brief overview of the statutory framework available to the government in intercepting electronic communications but focuses specifically on the physical extraction of data set forth in the hypothetical.

---

40. Jane Anderson, *Portable Electronic May Be Source of HIPPA Violations, Penalties*, INTERNAL MEDICINE NEWS, (Apr. 1, 2011) http://www.internalmedicinenews.com/single-view/portable-electronics-may-be-source-of-hipaa-violations-penalties/af89bd4ce5.html.

41. Maureen Minehan, *GPS Tracking: Big Brother or Big Benefit?*,28 NO. 1 EMP. ALERT 1 (2011) ("Technology is always a double-edged sword"); Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289, 1316 (2011) ("Technology is a double-edged sword.").

42. This Note does not attempt to hypothesize the endless possibilities of how criminals may use mobile technology to commit crimes, but the obvious uses include using mobile phones to communicate with other members of a criminal enterprise, to transfer sexually explicit contraband, or as tools in the commission of identity theft. *See United States v. Brown*, 2008 WL 2098070, at *3 (S.D. Ohio 2008) (possession of child pornography on cell phone); United States v. Park, 2007 WL 1521573, at *3 (N.D. Cal. 2007) (officer searched the address book of defendant's cellular telephone and recorded the names and telephone numbers of individuals whose information appeared in the cellular telephone); United States v. Chervin,, 2011 WL 4424297, at *5 (S.D.N.Y. 2011) (cell phone used in the commission of identity theft).

43. *See* 47 U.S.C. § 1002 (West 2011).

44. Physical extraction occurs when a mobile handset is connected to another device, physically, which creates a byte-for-byte copy of a disc image. EOGHAN CASEY ET. AL., DIGITAL EVIDENCE AND COMPUTER CRIME 26 (3d ed. 2011), *available at* http://www.elsevierdirect.com/companions/9780123742681/Chapter_20_Final.pdf (last visitedFeb. 25, 2012).

1. *Statutory Procedures to Obtain Mobil Phone Data*

As a preliminary matter, every telecommunications carrier is required to ensure that its equipment, facilities, and services that provide subscribers with the ability to originate, terminate, or direct communications enable the government, "pursuant to a court order or other lawful authorization," to intercept all wire and electronic communications.[45] Additionally, service providers must allow the government to access "call-identifying information that is reasonably available to the carrier before, during, or immediately after the transmission of a wire or electronic communication."[46]

The government can also use "pen registers" or "trap and trace devices" to intercept mobile phone communication data.[47] A "pen register" is a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.[48] The function of a pen register is limited because it cannot access the content of any communication.[49] A "trap and trace device" is a device or process that captures the incoming impulse that identifies the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.[50] These devices too cannot access the contents of any communications.[51] To intercept electronic and other types of communications, the government must follow a detailed statutory procedure.[52]

While the Fourth Amendment secures people "in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[53] it only constrains the government from such action.[54] Congress enacted statutory protections for communications in 1934[55] and further developed the statuto-

---

45. 47 U.S.C. §§ 1002(a)(2) (West 2011).

46. 47 U.S.C. § 1002(a)(2)(A) (West 2011). For an excellent discussion of the statutory privacy protections for electronic communications, see Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT L.J. 365, 370–81 (2010).

47. 18 U.S.C. § 3127(2)(B) (West 2011).

48. 18 U.S.C. § 3127(3) (West 2011).

49. 18 U.S.C. § 3127(3) (West 2011).

50. 18 U.S.C. § 3127(4) (West 2011).

51. 18 U.S.C. § 3127(4) (West 2011).

52. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, (2004).

53. U.S. CONST. amend. IV.

54. *See* Kerr, *supra* note 52, at 1209–13.

55. Sarah Salter, *Storage and Privacy in the Cloud: Enduring Access to Ephemeral Messages*, 32 HASTINGS COMM. & ENT L.J. 365, 371 n.19 (2010) (citing 47 U.S.C. § 605(a) (1934)) ("The Federal Communications Act, enacted in 1934, provided: No person not being authorized by the sender shall intercept any communication and divulge or publish the exist-

ry protections in 1968[56] and 1986.[57] These legislative enactments prohibit non-governmental interception of communications and also provide procedures for the government to follow in conducting electronic surveillance.[58]

2. *Forensic Data Extraction*

Forensic data extraction from mobile phones is a relatively new technology that evolved from a commercial device that transferred some data from one handset to another.[59] Cellebrite, an Israeli-based company with offices in New Jersey, is the leading provider of commercial data-transfer devices.[60] In 2006, the government approached Cellebrite and requested it to develop a device that would allow police, like the officer in the hypothetical, to extract data from mobile phones.[61] Since then, the company has become the leader in mobile forensics, [62] supporting over 6,800 handsets and GPS devices.[63]

Its core product, the UFED, enables operators to extract data from smartphones, legacy phones, and GPS devices, covering all major mobile operating systems, including the iPhone iOS, Android, BlackBerry, Symbian, and Palm.[64] The UFED Ultimate, what the company refers to as an "all-in-one" mobile forensic solution,[65] performs physical, logical, and file sys-

---

ence, contents, substance, purport, effect or meaning of such intercepted communication to any person.") (internal quotations omitted).

56. Salter, *supra* note 55, at 371 n.21 (citing Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197. 218-21) (Title III of the Act "outlined protection for electronic surveillance, providing for court supervision").

57. Salter, *supra* note 55, at 371.

58. *See generally*, 18 U.S.C. § 3127(4) (West 2011).

59. For example, when a consumer purchases a new phone, instead of manually inputting contact information, calendar appointments, and other types of data stored on an old handset, some carriers offer a service that involves connecting the old and new handsets to a device that operates as a switch-station, which extracts the data from one handset and copies it onto another. *See* Michael J. Tonsing, *New Techniques to Extract Evidence from Cellular Phones Create Dilemma for Courts, Prosecutors, and Criminal Defense Lawyers*, 55 FED. LAW. 12 (October 2008).

60. *Id.*

61. *Id.*

62. *See* McKay, *supra* note 19.

63. *Cellebrite UFED Extends Forensic Capabilities to Android Mobile Devices*, PR NEWSWIRE, http://www.prnewswire.com/news-releases/cellebrite-ufed-extends-forensic-capabilities-to-android-mobile-devices-132449788.html (Oct. 24, 2011).

64. *Id.*

65. *UFED Ultimate*, CELLEBRITE.COM, *available at* http://www.cellebrite.com/images/stories/brochures/UFED-Ultimate-ENGLISH-Brochure-web.pdf (last accessed Feb. 25, 2012).

tem extractions.[66] It is a stand-alone hardware device designed to copy contact lists and address books, pictures, videos, music, ringtones, text messages, call history, and device identifying information onto a memory storage device.[67] Additionally, many smartphones store user passwords for email servers, wireless networks, and third-party software suites that allow users to access remote computers or servers, like the hypothetical doctor's chart software.[68] These saved passwords are prime targets for the UFED Ultimate.[69] Because the UFED performs logical and physical extractions, the government can recover deleted phone data that a user may not even be aware existed.[70] It communicates with a cell phone through a cable, infrared, or blue tooth connection.[71] The UFED also acts as a write blocker, which simply means that no information is written to the phone when an examination is conducted.[72] Put simply, if a phone is searched with a UFED, it surreptitiously leaves no trace behind.[73] The devices are not only highly mobile; they are also inexpensive.[74]

The expansion of cell phone functionality and availability pressures businesses to adopt technology in-step with their clients. Additionally, amazing cost-saving advantages can result from the use of technology in the workplace.[75] On the other hand, businesses are prime targets for data-system

---

66. Mobile forensic commentators observe that one important consideration in the evaluation of forensic devices is whether the tool performs a physical or logical analysis. Andrew Hoog & Katie Strzempka, *Independent Research and Reviews of iPhone Forensic Tools*, VIAFORENSICS.COM, *available at* http://viaforensics.com/education/white-papers/iphone-forensics/ (released Nov. 2010) (last visited Feb. 25, 2012). A physical acquisition creates a bit-by-bit copy of a memory disk image, and thus, can recover deleted data. *Id.* Accordingly, the physical acquisition of data is a time consuming process that is contingent on the amount of data stored on the mobile device. *Id.* Alternatively, a logical analysis rapidly extracts data in the form of binary code, which is then translated by a device and repopulated. *Id.*

67. Jeff Lessard & Gary C. Kessler, *Android Forensics: Simplyifying Cell Phone Examinations*, SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL, Vol. 4, No. 1, Sept. 2010, *available at* http://www.ssddfj.org/papers/SSDDFJ_V4_1_Lessard_Kessler.pdf (last visited Feb. 25, 2012).

68. *UFED 1.1.7.8 Release Notes*, CELLEBRITE.COM, *available at* http://www.cellebrite.com/releases/1178/release%20note-august-17-ROW.pdf (released Aug. 2011) (last visited Feb. 25, 2012).

69. *Id.*

70. Hoog & Strzempka, *supra* note 66.

71. Lessard &Kessler, *supra* note 67.

72. *Id.*

73. *Id.*

74. A standard kit costs about $4000. Martha McKay, *Why cops love it, and suspects hate it*, NEW JERSEY RECORD (Feb. 14, 2008), *available at* 2008 WLNR 2872420 ("[T]he $4,000 kit, which was first introduced in July, has already been sold to more than 1000 law enforcement agencies.").

75. For example, instead of sending telegrams or letters through the postal mail, businesses can quickly communicate through the use of email. Many companies are also provid-

attacks by hackers or foreign governments.[76] Even with robust software-security protections like passwords and firewalls, in the age of the UFED, such protections are *soft*. As businesses leave behind the age of brick and mortar for the new world, they must cautiously guard the confidences entrusted to them, whether their attackers wear the badge of *hacker* or *Michigan State Police*.

III. FOURTH AMENDMENT JURISPRUDENCE

Businesses should, in theory, take solace in the limitations placed on the government's ability to access or penetrate private data. Although the word "privacy" never appears in the text of the Constitution, "the privacies of life"[77] guaranteed by the Fourth Amendment are historically considered part of "the very essence of constitutional liberty and security."[78] The framers of the Constitution created the Fourth Amendment to limit the government's ability to intrude into a citizen's private life.[79] Specifically, the framers did not trust that a government, unchecked in the ability to peer into its citizens' private lives, would wield that power judiciously.[80] On the other, society must balance this privacy interest against the public's interest in justice, which requires the gathering of evidence and enforcement of law.[81]

This theoretical framework forces the judiciary to walk an often-uncomfortable plank. The judiciary must do justice against bad actors, but also suppress evidence obtained in contravention of the Fourth Amendment

---

ing a "paperless billing" function, which also largely relies on the use of e-mail and the Internet. *See* Jim Mullen, *Going paperless – priceless!*, THE EVENING SUN (Jan. 31, 2012), *available at* http://www.evesun.com/news/stories/2012-01-31/14097/Going-paperless-priceless/.

76. The group of hackers known as "Anonymous" have already attacked data systems of MasterCard and PayPal. Kevin Rawlinson, *Secret cyber-warriors: our war on Whitehall*, INDEPENDENT NEWS AND MEDIA (June 9, 2011), *available at* http://usecmagazine.usecnetwork.com/uk/?p=12561. Even government agencies should be aware of data security issues. The United States, for example, was advised to adopt a policy of "covert sabotage" against Iran's nuclear development sites, including the use of computer hacking. Josh Halliday, *Leaked cable reveals nuclear sabotage advice to US*, THE GUARDIAN (Jan. 19, 2011), *available at* 2011 WLNR 1076360.

77. Boyd v. United States, 116 U.S. 616, 630 (1886).

78. *Id.*

79. THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 4 (2009) ("To help ensure that there will be limits on the power of the American government to arbitrarily interfere in the lives of its citizens the first Congress proposed and in 1791 the states ratified the Fourth Amendment to the Constitution.").

80. *Boyd*, 116 U.S. at 641 ("the [F]ramers of the [C]onstitution had their attention drawn, no doubt, to the abuses of this power of searching private houses and seizing private papers.").

81. *See, e.g.*, United States v. Place, 462 U.S. 696, 703 (1983) ("We must balance the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.").

by application of the exclusionary rule.[82] Excluding key evidence can result in allowing an otherwise guilty defendant to escape justice. To avoid this discomfort, several exceptions to the Fourth Amendment's warrant requirement have been carved out by the Court. As this section will discuss, the legal aphorism that "hard cases, make bad law"[83] is exceedingly true as the Court brings the Fourth Amendment into the digital age. This Note takes the position that the Court's wait-and-see approach[84] to technology and the Fourth Amendment illustrates the aphorism,[85] where the application of the exclusionary rule "appeals to the feelings and distorts the judgment"[86] of the Court. The Fourth Amendment can survive the *virtual* reality if the Court adheres to the original intent of the Fourth Amendment when confronting novel, technological challenges of the Fourth Amendment.

More than a century ago, the Supreme Court acknowledged that the concerns underlying the Fourth Amendment extend beyond the "breaking of . . . doors, and the rummaging of . . . drawers" to "*all invasions* on the part of the government . . . *of the sanctity of a man's home and the privacies of life*."[87] Privacy is the primary value protected by the Bill of Rights' restriction of "searches."[88] Over eighty years ago, Justice Brandeis warned that technological surveillance creates perilous dangers to Fourth Amendment rights.[89] This danger remains today. Failure to apply the Fourth Amendment in the digital age will have a chilling effect on society's ability to use technology in the business setting.

To begin the discussion of Fourth Amendment protections against warrantless cell phone searches, this section will travel back in time 400 years and consider the bedrock upon which the framer's created the Amendment,

---

82. As this section will discuss, the exclusionary rule of the Fourth Amendment has been said to allow the criminal "to go free because the constable has blundered," and is thus subject to ardent controversy. *See* People v. Defore, 242 N.Y. 13, 21, 150 N.E. 585, 587 (1926).

83. Crocker v. Whitney, 10 Mass. 316, 322 n.9 (1813) ("[h]ard cases make shipwreck of the law"); N. Sec. Co. v. United States, 193 U.S. 197, 364 (1904) (Holmes, J., dissenting).

84. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746, 768 (2010) (Scalia, J., concurring in part and concurring in the judgment) ("The-times-they-are-a-changin' is a feeble excuse for disregard of duty"). Justice Scalia aptly notes, "[a]pplying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case [the Court] has no choice." *Id.*

85. *N. Sec. Co.*, 193 U.S. at 364 (Holmes, J., dissenting) (a judge's task, when called to interpret the language of a statute, "is merely academic to begin with,-to read English intelligently,-and a consideration of consequences comes into play, if at all, only when the meaning of the words used is open to reasonable doubt").

86. *Id.*

87. Boyd v. United States, 116 U.S. 616, 630 (1886) (emphasis added).

88. *See* Horton v. California, 496 U.S. 128, 133 (1990).

89. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting); *see also* Goldman v. United States, 316 U.S. 129, 138–40 (1942) (Murphy, J., dissenting).

providing a principled framework for courts to rely on in applying its protections to modern technology. Accordingly, this section will briefly consider the English roots of the Fourth Amendment's protections as well as early, seminal United States Fourth Amendment cases. Returning to the present day, this section will then discuss the two sides of the circuit split, illustrated by the Fifth and Eleventh Circuits,[90] the California and Ohio Supreme Court decisions regarding cell phone privacy,[91] and the recent decisions of *Ontario, Cal. v. Quon* and *United States v. Jones*.[92] This analysis will expose an open question on the issue of whether the Fourth Amendment's jurisprudence can logically apply to modern technology. Because this question remains unanswered by the Supreme Court, password-protection policies in employment handbooks are wholly insufficient. Until the Court answers the call of duty and provides a meaningful discussion about law and technology, businesses should be weary of communicating or accessing confidential information on mobile handsets.

A. Historical Development of Fourth Amendment Jurisprudence

1. *Historical Bedrock*

The Fourth Amendment principle that citizens should be protected against unreasonable searches and seizures is not an American creation.[93] In 1604, *Semayne*'s[94] first identified the protection that would become central to the Fourth Amendment.[95] Sir Edward Coke ruled that "the house of everyone is to him as his castle and fortress, as well for his defence against inju-

90. United States v. Finley, 477 F.3d 250 (5th Cir. 2007) (reasonable expectation of privacy in the call records and text messages on the cell phone); United States v. Jones, 149 Fed. App'x 954 (11th Cir. 2005) (no reasonable expectation of privacy in text message pager).

91. People v. Diaz, 51 Cal.4th 84, 244 P.3d 501, 1199 Cal.Rptr.3d 105 (2011) (warrantless cell phone search acceptable), *cert. denied* Diaz v. California, 132 S. Ct. 94 (2011); State v. Smith, 124 Ohio St.3d 163, 2009-Ohio-6426, 920 N.E.2d 949 (Ohio 2009) (cell phone search not permissible without a warrant).

92. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds*, City of Ontario, Cal. v. Quon, 560U.S. 746, 130 S.Ct. 2619 (2010) (declining to rule directly on the issue).

93. *See* Semayne's Case, 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194, 195–96 (K.B. 1603), *available at* http://groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2005/weeks/semayne.html.

94. *Id.*

95. *Id.*

ry and violence as for his repose."[96] Coke proclaimed that subjects of the kingdom had the right to be protected from searches and seizures that were unlawfully conducted, even when the King's agents conducted the search.[97]

The seminal case of *Entick v. Carrington* illustrates the application of such a right.[98] There, royal representatives broke into the private home of John Entick searching for material that was critical of the Crown.[99] They broke into locked boxes and desks, confiscated papers, charts, pamphlets, and other personal effects of Mr. Entick.[100] During the trial, Entick charged that the search and seizure of his property was unlawful.[101] Abhorring the issuance of a general warrant, the court stated:

The great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole. . . . By the laws of England, every invasion of private property, be it ever so minute, is a trespass. No man can set his foot upon my ground without my license[.][102]

A quarter of a century after *Entick*, the drafters of the Constitution declared that the people had a right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]"[103] That right "shall not be violated, and no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[104] In *Boyd v. United States*,[105] the Court identified that *Entick*'s holding stood for the proposition that the physical act of searching a person's home or belongings is not the essence of a Fourth Amendment violation, but instead is "the inva-

96. *Id.*
97. *Id.*
98. Entick v. Carrington, 95 Eng. Rep. 807(K.B. 1765), *available at* http://www.constitution.org/trials/entick/entick_v_carrington.htm (disapproving search of plaintiff's private papers under general warrant, despite arrest).
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. U.S. CONST. amend. IV.
104. U.S. CONST. amend. IV. It is also generally understood that the use of general search warrants by England "was a motivating factor behind the Declaration of Independence." Berger v. New York, 388 U.S. 41 (1967). The Declaration of Independence, in pertinent part, provides: "But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security." THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).
105. 116 U.S. 616 (1886).

sion of [his or her] indefeasible right of personal security, personal liberty[,] and private property."[106]

A remedy for the violation of the Fourth Amendment was not recognized until the Court created the exclusionary rule.[107] The general application of the exclusionary rule requires the suppression of evidence obtained in violation of the Fourth Amendment. The purpose of this rule is to deter the government from obtaining evidence in contravention of the Fourth Amendment.[108] The Court reasoned that if evidence was unlawfully seized but could still be used against a criminal defendant, the Fourth Amendment would be meaningless and "might as well be stricken from the Constitution."[109] With the deterrent principle in place, this Note will observe how these early concepts, created in a world of brick and mortar, eroded with time as "hard cases" created a Fourth Amendment with "more holes in it than a piece of Swiss cheese."[110]

2. *Erosion of the Bedrock*

As a preliminary matter, the text of the Fourth Amendment expressly imposes two requirements on the government: "all searches and seizures must be reasonable (the reasonableness clause)[111]and a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity (the warrant clause)."[112] The reasonableness clause performs two countervailing functions: promoting a person's reasonable expectation of privacy while also serving as a gatekeep-

106. *Id.* at 630.

107. Weeks v. United States, 232 U.S. 383 (1914), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961).

108. *Id.* at 393.

109. *Id.* The creation of the exclusionary rule illustrates the intent of the Fourth Amendment: a proverbial "stick" to compel the government's compliance with the Fourth Amendment. *See* People v. Glorioso, 924 N.E.2d 1153. 1157 (Ill. App. 2d Dist. 2010) *appeal denied,* 932 N.E.2d 1033 (Ill. 2010). It should also be noted that *Mapp* stood for the proposition that the exclusionary rule was a constitutional right under the Fourth Amendment. *See* Jack W. Nowlin, *The Exclusionary Rule*, THE NATIONAL JUDICIAL COLLEGE, http://www.olemiss.edu/depts/ncjrl/pdf/May%202011%20Comp%20Search%20and%20Seizure/D16_Exclusionary_Rule.pdf (last visited Mar. 12, 2012) (citing *Mapp*, 367 U.S. at 651). This is no longer the case. *Id.* The exclusionary rule has been "de-constitutionalized," and now courts attempt to balance the deterrent impact of the exclusionary rule with the cost it takes on law enforcement objectives. Jack Nowlin, *The Exclusionary Rule* . (citing United States v. Leon, 468 U.S. 897, 906 (1984)).

110. United States v. McClain, 444 F.3d 537 (6th Cir. 2006) (Martin, Moore, Cole, and Clay, JJ., dissenting).

111. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011).

112. *Id.* (citing *Payton v. New York*, 445 U.S. 573, 584 (1980)).

er to determine whether the Fourth Amendment applies to the context of a search where no reasonable expectation of privacy exists.[113] If there is a reasonable expectation of privacy in the given context, then the government must either obtain a warrant or try to meet one of the numerous exceptions to the Fourth Amendment.[114]

a. Reasonable Expectation of Privacy

A person's expectation of privacy stands as the measuring stick for how far the government may encroach upon its citizens' private lives in order to further the cause of justice.[115] This is illustrated by *Katz v. United States*, where the Court considered the government's warrantless use of an electronic listening device on a public telephone booth.[116] The government argued that the use of the listening device was not a search under the Fourth Amendment because the telephone booth was a public space. [117] By way of Justice Harlan's concurrence, the Court rejected the notion that a "search" can occur only when there has been a "physical intrusion" into a "constitutionally protected area" because "the Fourth Amendment protects people, not places."[118] Monitoring Katz's conversation "violated the privacy upon which he justifiably relied while using the telephone booth," and accordingly, it constituted a search within the meaning of the Fourth Amendment."[119]

Katz created a two-part test to determine whether a person is entitled to Fourth Amendment protection.[120] First, that person must have an actual, subjective expectation of privacy in the area or object being searched.[121] Second, that expectation must be one that society recognizes as reasonable.[122] The *Katz* standard was questioned in 2001, when a thermal imaging device was used to scan the home of a suspected marijuana farmer.[123]

The scan in *Kyllo v. United States* allowed the government to see heat radiation within the home, which was consistent with high-intensity lamps used in the cultivation of marijuana.[124] With this knowledge, a magistrate

113. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).
114. *Id.*
115. *Id.* at 361.
116. *Id.*
117. *Id.* at 351.
118. *Id.* at 360–62.
119. *Katz*, 389 U.S. at 353.
120. *Id.* at 360–62 (Harlan, J., concurring).
121. *Id.*
122. *Id.*
123. Kyllo v. United States, 533 U.S. 27, 30 (2001).
124. *Id.*

judge issued a search warrant for the home, where marijuana was in fact growing.[125] The Ninth Circuit upheld the search and explained that Mr. Kyllo failed on both prongs of the *Katz* test.[126] First, he did not show a subjective expectation of privacy in the heat radiating from his house because he did not attempt to conceal it.[127] Second, even if such an attempt was made, because the thermal imager only exposed amorphous hot spots on the home's exterior, no objective, reasonable expectation of privacy could exist.[128]

The Court rejected the Ninth Circuit's rationale, however, because the use of a thermal imager was not in general public use.[129] It held that when the government uses a device that is not in general public use to explore details of a private home that would otherwise be hidden, a Fourth Amendment search has occurred and is presumptively unreasonable without a warrant.[130] Although the government argued that the invasiveness of the thermal-imaging search was too minimal to trigger the *Katz* expectation of privacy test, the Court disagreed, reasoning that:

To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that, obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area" constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.[131]

b. Exceptions to the Fourth Amendment

The Supreme Court has long recognized exceptions to the Fourth Amendment that allow police officers to conduct searches without first procuring a warrant.[132] These include searches with consent,[133] in plain

125. *Id.*at 30.
126. *Id.* at 29–30.
127. *Id.* at 31.
128. *Id.*
129. *Kyllo*, 533 U.S. at 32–34.
130. *Id.*
131. *Kyllo*, 533 U.S. at 34 (quoting Silverman v. United States, 365 U.S. 505 (1961)).
132. There are several exceptions to the Fourth Amendment's warrant requirement that are outside the scope of this Note. For an excellent discussion of the many exceptions to the Fourth Amendment's warrant or probable cause requirement, see Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1473 (1985) ("[t]here are over twenty exceptions to the probable cause or the warrant requirement or both").

view,[134] incident to arrest,[135] of automobiles,[136] and under exigent circumstances.[137] While each exception chips away at the bedrock of the Fourth Amendment and accordingly exposes businesses with mobile technology to increased liability, of main concern in the context of this Note are the consent and search-incident-to-arrest exceptions.[138]

Consent is important in this context because it is a controllable human action, and as Part IV discusses, should be addressed by employers while redrafting technology policies. Consenting to a search is a voluntary waiver of Fourth Amendment protections, and is valid even if the person consenting is not aware of the right or intelligent enough to understand the implications of its waiver.[139] Two important considerations determine the validity of a consent search. First, consent must be voluntary in consideration of the to-

---

133. If consent is given by a person reasonably believed by an officer to have authority to give such consent, generally, no warrant is required for a search or seizure. *See* Illinois v. Rodriguez, 497 U.S. 177, 179 (1990).

134. No warrant is required to seize evidence in plain view if the police are legitimately in the location from which the evidence can be viewed. *See* Horton v. Cal., 496 U.S. 128 (1990) (eliminating the requirement that the discovery of evidence in plain view be inadvertent).

135. A search incident to lawful arrest does not require issuance of a warrant. *See* Chimel v. Cal., 395 U.S. 752 (1969). Thus, if someone is lawfully arrested, the police may search the person and area surrounding the arrestee. *Id.* at 756–69.

136. Because vehicles are highly mobile, a warrant is not required to search vehicles if police have probable cause to believe the vehicle contains evidence of a crime, the instrumentalities of crime, contraband, or the fruits of a crime. *See* Carroll v. United States, 267 U.S. 132, 151–56 (1925).

137. "It is well established that 'exigent circumstances,' including the need to prevent the destruction of evidence, permit police officers to conduct an otherwise permissible search without first obtaining a warrant." Kentucky v. King, 563 U.S. ___, ___, 131 S. Ct. 1849, 1853–54 (2011).

138. Several scholarly articles provide excellent and exhaustive analyses of Fourth Amendment jurisprudence relating to searches of mobile devices. *See* Adam M. Gershowitz, *Password Protected? Can A Password Save Your Cell Phone from A Search Incident to Arrest?*, 96 IOWA L. REV. 1125 (2011); Adam M. Gershowitz, *The iPhone Meets the Fourth Amendment*, 56 UCLA L. REV. 27 (2008); Jana L. Knott, *Is There an App for That? Reexamining the Doctrine of Search Incident to Lawful Arrest in the Context of Cell Phones*, 35 OKLA. CITY U. L. REV. 445 (2010); Chelsea Oxton , *The Search Incident to Arrest Exception Plays Catch Up: Why Police May No Longer Search Cell Phones Incident to Arrest Without A Warrant*, 43 CREIGHTON L. REV. 1157 (2010); Ashley B. Snyder, *The Fourth Amendment and Warrantless Cell Phone Searches: When Is Your Cell Phone Protected?*, 46 WAKE FOREST L. REV. 155 (2011); Bryan A. Stillwagon, *Bringing an End to Warrantless Cell Phone Searches*, 42 GA. L. REV. 1165 (2008). This Note will provide a workable overview of the Court's treatment of Fourth Amendment protection of emerging technologies, arguing that such a "Swiss-cheese" framework inhibits the ability of businesses attempting to modernize the workplace to securely access confidential information stored on mobile devices or on data systems in any meaningful way.

139. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 241 (1973).

tality of the circumstances, which is determined by five dispositive factors.[140] The second consideration is whether the scope of the search exceeded the scope of consent given.[141] The test for determining the scope of consent is whether a reasonable person would have understood the conversation between the officer and the suspect.[142]

The search-incident-to-arrest exception creates a unique problem for employers because searches under this exception are not within the purview of an employee's decision making power at the time the search arises. This exception was not recognized until the 1969 decision of *Chimel v. California*,[143] where the Court expressly held that officers may perform searches incident to a lawful arrest in certain narrow situations.[144] One situation involves a threat to the officer's safety by the presence of accessible weapons on or near the suspect.[145] Another involves the officer's need to prevent the destruction of evidence.[146] These warrantless searches, the Court held, must be limited to areas accessible by the arrestee.[147]

The scope of this exception expanded in *United States v. Robinson*, where the Court considered whether police officers could open closed containers located on the arrestee's person.[148] In this instance, the officer conducted a search-incident-to-arrest of an arrestee's person and felt an object in one of the jacket pockets.[149] After he unzipped it, he found a crumpled cigarette package with heroin inside it.[150] Rejecting Robinson's challenge to the search, the Court held that officers conducting a search-incident-to-arrest could open and search all items on an arrestee's person, including closed containers, even if the officer had no suspicion that the contents would contain contraband.[151]

The Court once again broadened the scope in *New York v. Belton*.[152] The Court considered whether an officer's recovery and subsequent search of a jacket from a non-accessible portion of a vehicle was valid under the

140. The five factors are knowledge of the constitutional right to refuse giving consent; the age, intelligence, education, and language ability of the person giving consent; whether the person is cooperating with the police; the arrestee's attitude about the police inevitably finding some contraband; and length and type of questioning used. *See Warrantless Searches and Seizures*, 37 GEO. L.J. ANN. REV. CRIM. PROC. 39, 87 (2008).

141. *Id.* at 95.

142. *Id.* at n.250 (citing Florida v. Jimeno, 500 U.S. 248, 251 (1991)).

143. Chimel v. Cal., 395 U.S. 752, 768 (1969).

144. *Id.* at 755.

145. *Id.* at 763–6.

146. *Id.* at 764.

147. *Id.*

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

149. *Id.* at 222–23.

150. *Id.* at 223.

151. *Id.* at 236.

152. *Belton*, 453 U.S. 454 (1981).

search-incident-to-arrest exception.[153] The Court reasoned that officers need "a straightforward rule, easily applied, and predictably enforced."[154] The Court expanded the container doctrine to apply to any object capable of holding another object.[155]

Realizing that this exception far exceeded the *Chimel* justifications, the Court narrowed the search-incident-to-arrest exception in *Arizona v. Gant*,[156] a case involving the search of an arrestee's vehicle after he was cuffed and detained in the back of a police cruiser.[157] The Arizona Supreme Court struck down the search because the *Chimel* rationales, police safety and preservation of evidence, did not justify the search.[158] The Supreme Court affirmed because "[t]he safety and evidentiary justifications underlying *Chimel*[] . . . determine *Belton*'s scope."[159] Police may not perform a search incident to arrest of an automobile once the arrestee "has been secured and cannot access the interior of the vehicle" unless it is "reasonable to believe that evidence of the offenseof arrest might be found in the vehicle."[160]

The search-incident-to-arrest exception is particularly important in the context of searches involving modern technology because many devices like cell phones are mobile and can fit in pockets or other readily accessible areas. The first cases involving the search-incident-to-arrest exception and modern technology appeared in the mid-1990s and involved beeper-pagers.[161] For example, in *United States v. Chan*,[162] the police turned on a pager and copied telephone numbers that linked Chan to other drug dealers.[163] The court upheld the search of the pager because it considered a pager to be an electronic container, the search of which was authorized under the container doctrine of the search-incident-to-arrest exception.[164] Whether the arrestee could retrieve a weapon or destroy evidence on the beeper was irrelevant for the court, and it found no need to differentiate between searching an electronic beeper and searching a piece of luggage, box, or cigarette

153. *Id.* at 455–47.
154. *Id.* at 459.
155. *Id.* at 460–61.
156. *Gant*, 556 U.S. 332 (2009).
157. State v. Gant, 216 Ariz. 1, 162 P.3d 640 (Ariz. 2007) *aff'd,* 556 U.S. 332, 129 S. Ct. 1710 (2009).
158. *Id.* at 643 (noting that all the arrestees were handcuffed and secured in patrol cars, there were no unsecured civilians in the vicinity, four officers were on the scene, and there was no reason to believe that anyone on the scene could have gained access to Gant's car).
159. *Gant*, 556 U.S. 332, 332 (2009).
160. *Id.* at 335 (citing Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring in judgment)).
161. *See* United States v. Chan, 830 F.Supp. 531 (N.D. Cal. 1993).
162. *Id.*
163. *Id.* at 533.
164. *Id.*

carton.[165] Despite Justice Brandeis's cautionary dissent so many years ago,[166] "[t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question."[167]

3. *Leading Circuit Court Decisions*

In *United States v. Finley*,[168] the Fifth Circuit upheld a district court's denial of a motion to suppress call records and text messages retrieved from Finley's cell phone.[169] Finley was arrested after a passenger in his van sold methamphetamine to a police informant.[170] The police recovered a cell phone from his pocket and examined the call record and text message folders to confirm Finley's narcotic-trafficking activities.[171] Upholding the search, the Fifth Circuit analogized Finley's cell phone to a closed container like that of *Belton*.[172]

Recently, in *United States v. Curtis*,[173] the Fifth Circuit held that an officer's warrantless search of data stored on a cell phone did not violate the arrestee's Fourth Amendment rights, reaffirming the *Finley* decision despite the Supreme Court's limiting of the search-incident-to-arrest doctrine in *Arizona v. Gant*.[174] In *Curtis*, the arrestee was using the mobile device at the time he was apprehended, and applying the container doctrine, the court upheld the search.[175] *Curtis* illustrates two things. First, it shows how confused Fourth Amendment jurisprudence has become as the search-incident-to-arrest doctrine developed. Second, it illustrates an example where the Supreme Court has sacrificed an opportunity to end the confusion.

---

165. *Id.*at 533–35.

166. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

167. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) *rev'd and remanded sub nom.*, City of Ontario, Cal. v. Quon, ___ U.S. ___, 130 S. Ct. 2619 (2010); *c.f.* United States v. Finley, 477 F.3d 250 (5th Cir. 2007) (reasonable expectation of privacy in the call records and text messages on the cell phone); United States v. Jones, 149 Fed. App'x 954 (11th Cir. 2005) (no reasonable expectation of privacy in text message pager).

168. *Finley*, 477 F.3d 250 (5th Cir. 2007).

169. *Id.*

170. *Id.* at 254.

171. *Id.* at 254–55.

172. *Id.* at 259–63.

173. 635 F.3d 704 (5th Cir. 2011) *cert. denied,* 132 S. Ct. 191 (2011).

174. *See id.* at 707–10; Arizona v. Gant, 556 U.S. 332 (2009).

175. Curtis, 635 F.3d at 708–13; see United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) (objective expectation of privacy in contents of cell phone because "mere possession" of phone and "wealth of private information" contained therein—including emails, text messages, call histories, address books, and subscriber numbers—make privacy expectation reasonable).

The other side of the circuit split is illustrated by *United States v. Park*,[176] where the court granted Park's motion to suppress the warrantless search of his cell phone.[177] There, police officers observed Park enter and exit a building suspected to be an indoor marijuana farm.[178] After they executed a search warrant for the building, they confirmed their suspicions and arrested Park.[179] After booking him, the officers searched his cell phone and recorded some names and phone numbers.[180]

At trial, the district court granted Park's motion to suppress the evidence obtained from the cell phone, reasoning that cell phones "have the capacity for storing immense amounts of private information" and thus likened the devices to laptop computers, in which arrestees have significant privacy interests—rather than a lower privacy interest like one in an address book or pager.[181] Because the search of the cell phone's contents was not conducted out of concern for the officer's safety or to preserve evidence, the court found that it did not fall under the search-incident-to-arrest exception and that the officers should have obtained a warrant to conduct the search.[182]

In *State v. Smith*,[183] the Ohio Supreme Court rejected *Finley*'s approach and held that the warrantless search of data stored on an arrestee's cell phone, seized incident to a lawful arrest, is prohibited by the Fourth Amendment when the search is unnecessary for the safety of law enforcement officers and there are no exigent circumstances.[184] There, Antwaun Smith was arrested on drug-related charges after responding to a call from a police informant.[185] Recovering his cell phone, the officers searched its call records and stored contact information to confirm the prior exchange between him and the informant.[186] Like *Park*, the court held that because officer safety or evidence preservation was not an issue, the search was beyond the scope of the search-incident-arrest doctrine.[187]

But the Supreme Court of California did not find *Park* so convincing when it decided *People v. Diaz*.[188] Analogizing a cell phone to cigarette carton, the Silicon Valley High Court held that a warrantless search of the text

176. United States v. Park, CR 05-375SI, 2007 WL 1521573 (N.D. Cal. 2007).
177. *Id.* at *1.
178. *Id.* at *2.
179. *Id.*
180. *Id.* at *3.
181. *Park*, 2007 WL 1521573, at *8.
182. *Id.* at *8–12.
183. State v. Smith, 124 Ohio St.3d 163 (Ohio 2009) (cell phone search not permissible without a warrant).
184. *Id.* at 170–71.
185. *Id.* at 163.
186. *Id.* at 63–64.
187. *Smith*, 124 Ohio St.3d at 167.
188. *People v. Diaz*, 51 Cal. 4th 84 (2011) *cert. denied*, 132 S. Ct. 94 (U.S. 2011).

message folder on an arrestees' cell phone was valid even though the search was not contemporaneous occur with the arrest.[189] Akin to *Robinson* and *Edwards*, the court construed the cell phone as being an item of personal property on a defendant's person at the time of arrest, and thus, held that the warrantless search was valid.[190]

Somewhere on the spectrum between the Fifth and Eleventh Circuit positions rests Judge Posner's very recent Seventh Circuit opinion of *United States v. Flores-Lopez*.[191] There, in considering whether a warrantless search of an arrestee's phone solely for the purpose of ascertaining the phone's number was valid, Judge Posner begins the analysis by identifying several issues regarding modern cell phones.[192] First, he acknowledged the vast capabilities of the modern cell phone and admitted that they are computers.[193]

A modern cell phone is in one aspect a diary writ large. Even when used primarily for business it is quite likely to contain, or provide ready access to, a vast body of personal data. The potential invasion of privacy in a search of a cell phone is greater than in a search of a "container" in a conventional sense even when the conventional container is a purse that contains an address book (itself a container) and photos.[194]

Despite a very thorough understanding of the capabilities of modern cell phones, like being able to monitor a home security system with the iCam App, the Seventh Circuit still flatly accepted the government's argument that a cell phone falls under the *Robinson* container doctrine.[195]

On the same token, the court observed that the *Chimel* rationale for a warrantless search limited the container doctrine to searches due to officer safety or the preservation of evidence.[196] Hypothesizing possible justifications

---

189. *Id.* at 89, 101. This holding roused an outcry from many Californians and, after the Supreme Court of the United States denied certiorari, the California legislature passed SB 914, a bill limiting searches incident to arrest in California. *See* Ken Kozlowski**,** *Fourth Amendment in the Electronic Age-Part II*, 17 NO. 1 INTERNET L. RESEARCHER 1 (Jan. 2012) ("California passed SB 914 (http:// www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0901-0950/sb_914_bill_20110902_ enrolled.pdf) on September 1, 2011."); *see also In the States*, TELECOMMUNICATIONS REPORTS (Nov. 1, 2011), *available at* 2011 WLNR 21568425. Governor Jerry Brown vetoed the bill, however, stating that courts are better suited to resolve the complex and case specific issues relating to constitutional search-and-seizures protections. *California Governor Jerry Brown (D) vetoed a bill . . .* , COMMUNICATIONS DAILY (Oct. 12, 2011), *available at* 2011 WLNR 21177941.

190. *Id.* at 99.

191. *Flores-Lopez*, 670F.3d 803, 2012 WL 652504 (7th Cir. 2012).

192. *Id.* at 804.

193. *Id.* at 804 ("a modern cell phone *is* a computer").

194. *Id.* at 805.

195. *Id.* at 805–06.

196. *Id.* at 806. Alternatively, it recognized that *Gant* relaxed the standard for the search-incident-to-arrest exception when a vehicle is involved, allowing officers to search the passenger compartment even if they have no reason to believe they will find any evidence. *Id.*

for police safety, the court found that some stun guns are sold to resemble cell phones and that an officer may search a phone to ensure their safety was not at risk.[197] Moreover, on the issue of destruction of evidence, it observed that some apps exist that allow the user to remotely or locally wipe information from a phone.[198] This line of reasoning was also somewhat negated because the risk of the destruction of evidence could be eliminated by placing the phones in "Faraday bags" or by using the UFED.[199]

Casting *Chimel* aside, the court wrote that the cost of requiring police officers to carry Faraday bags and UFEDs is not a feasible undertaking.[200] Even when the risk to a police officer or for the destruction of evidence is negligible, the search is allowed as long as it is "no more invasive than . . . the search of a conventional container."[201] What Posner suggests is a sliding-scale test determined by the type of information the search reveals. Because the police only searched for a phone number, the court found that the search was not intrusive.[202]

The implications of this opinion are numerous. First, commentators forecast that this opinion will help justify the Supreme Court's intervention.[203] Certainly, it adds a new approach to the circuit split with a moderate middle-ground. Second, it provides a backdrop to the fundamental problem in the analysis of the Fourth Amendment in the digital age. A cell phone is not a container in the traditional sense. The analogy of a crumpled cigarette box to an iPhone 4 fails when the court admits a cell phone is essentially a computer. When courts apply outdated principles to new technology, they alter technology's natural course through society.[204] The outcome creates a chilling effect on the use of technology for society as a whole, and specifically for businesses attempting to stay current with and reap the benefits of

---

This was of no consequence because the arrestee did not use a car. *Flores-Lopez*, 670F.3d 803, 806(7th Cir. 2012).

197. *Id.* .

198. *Flores-Lopez*, 670 F.3d at 806–07.

199. *Id.* at 809 (citing *ACLU Seeks Records about State Police Searches of Cellphones*, AMERICAN CIVIL LIBERTIES UNION OF MICHIGAN, www.aclumich.org/issues/privacy–and–technology/2011–04/154 (last accessed Apr. 13, 2011)).

200. *Id.*

201. *Flores-Lopez*, 670 F.3d at 809.

202. *Id.* at 809–10.

203. Orin Kerr, *Judge Posner on Searching a Cell Phone Incident to Arrest*, THE VOLOKH CONSPIRACY (Feb. 29, 2012, 5:06 pm), *available at* http://www.volokh.com/2012/02/29/judge-posner-on-searching-a-cell-phone-incident-to-arrest/.

204. While this is discussed more fully below in Part III.B.5 of this Note, the Court itself takes the position that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." City of Ontario, Cal. v. Quon, 560 U.S. 746, 759 (2010).

technology.[205] While the courts should not ignore the doctrine of *stare decisis*, they likewise should not use failed logic in establishing precedent. Instead, the courts should recognize the failed analogies, embrace the spirit and purpose of the Fourth Amendment, and fashion a rule that balances the interests in personal privacy with the interest in justice. The Supreme Court admonished the lack of straightforward, predictably enforced rules in *Belton* to justify the increased scope of the search-incident-to-arrest exception.[206] Instead of allowing the lower courts to guess at the right answer with consistent inconsistency, it must illuminate a clear, workable standard. When called to action, however, the Court refused in "disregard of duty."[207] This Note urges the Court to answer the call of duty and enforce the warrant requirement of the Fourth Amendment to avoid any chilling effect on society's use of mobile phone technology.

4. *Failures and Opportunities*

The Court had an opportunity to answer the call of duty in *City of Ontario, California v. Quon*. The case did not involve a criminal matter, but instead dealt with a public employer's search of an employer-provided pager.[208] Quon, a police sergeant, exceeded the text-message plan's limitations and sustained overage charges for the department.[209] When confronted about the nature of the charges, he admitted that many messages were personal and agreed to pay the extra charges.[210] Though he paid the overages, his supervisors still decided to audit the message contents to determine whether officers were using the pagers for work-related reasons—requiring an increase in text message allotment—or whether they were using them for personal reasons.[211] They learned that in one month alone, Sergeant Quon sent

---

205. A current example of this push-and-pull between technology and its regulation is the debate regarding Internet regulation. *See, e.g.*, Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011); *see* John Billings, *Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011)*, 20 COMM. LAW 295 (2011); *see also* David Post, *Stopping the Stop Online Piracy Act*, THE VOLOKH CONSPIRACY (Dec. 5, 2011), *available at* http://www.volokh.com/2011/12/04/stopping-the-stop-online-piracy-act/ .

206. New York v. Belton, 453 U.S. 454, 459 (1981).

207. City of Ontario, Cal. v. Quon, 560 U.S. 746, 768 (2010) (Scalia, J., dissenting).

208. *Id.* at 751–52.

209. *Id.* at 752.

210. *Id.* at 752–53.

211. *Id.* at 751–52. Quon signed a statement acknowledging the City's Computer Usage, Internet, and E-Mail Policy that "reserve[d] the [Department's] right to monitor and log all network activity including e-mail and Internet use, with or without notice," which was later expanded to treat text messages as e-mail. *Id.*

or received 456 messages during work hours, 399 of which were personal.[212] When Quon learned that the department read the contents of his text messages, he filed an action under the Stored Communications Act and Fourth Amendment against the text-message service provider and the department.[213]

At trial, he argued that the search violated his Fourth Amendment rights because he had a reasonable expectation of privacy in the contents of his text messages.[214] The trial court found that he did have a reasonable expectation of privacy in the text messages the search did not violate the Fourth Amendment.[215] The Ninth Circuit reversed, holding that the search was unreasonable as matter of law, presenting the Supreme Court with a prime opportunity to decide whether society places a reasonable expectation of privacy in the contents of a text message.[216]

Surrendering the opportunity, the Court stated that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[217] Instead of deciding whether there is a reasonable expectation of privacy in the contents of a text message, the Court assumed *arguendo* that even if it existed, the search itself was reasonable under the circumstances.[218] The Court sent a clear message that it did not want *Quon* to become the reference case that would give employees an expectation of privacy in text-message content sent on employer-provided devices.[219]

Justice Scalia lambasted in his concurrence that such a narrow holding was the Court's "disregard of duty."[220] The Court chose to blow the horn of retreat instead of answering the call of duty to set a workable standard. This narrow holding leaves businesses stranded in the battle to safeguard data in the digital age because too many questions are left unanswered. It is unclear whether *Quon* applies to private employers or if it is only limited to searches of government employee cell phones. Likewise, where an employee owns a device but the employer partially pays the service charges, *Quon* cannot answer whether the search would be allowable. Most importantly, it also does not answer whether there is a reasonable expectation of privacy in the stored data of a cell phone. Without answering this crucial question, busi-

212. *Id.* at 753.
213. *Quon*, 560 U.S. at 753 (citing 42 U.S.C. § 1983; 18 U.S.C. § 2701).
214. *Id.* at 754.
215. *Id.*
216. *Id.* at 753–54.
217. *Id.* at 759.
218. *Id.* at 759–60.
219. The "[r]apid changes in the dynamics of communications" make it difficult to predict "how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable." *Quon*, 560 U.S. 759–60.
220. *Id.* at 768 (Scalia, J., concurring in part and concurring in judgment).

nesses are ill-equipped to write adequate technology policies to prevent data breaches caused by police surveillance. *Quon* for businesses is tantamount to Scylla and Charybdis for Odysseus.[221]

With this failure aside, the Court had another great opportunity to elaborate on the Fourth Amendment's application to new technologies. In *United States v. Jones*, the police installed a credit-card sized GPS chip behind the license place of Antoine Jones, a suspected drug dealer.[222] Using the GPS chip, they tracked him for twenty-eight days without a valid search warrant.[223] Ultimately, he was arrested and sentenced to life in prison for conspiracy to distribute cocaine.[224] The U.S. Court of Appeals for the District of Columbia reversed the conviction and found that the GPS tracking was a search within the meaning of the Fourth Amendment and was therefore unconstitutional.[225]

On review, the Supreme Court considered whether the GPS tracking of Jones on public roads was akin to constant visual surveillance or whether such tracking was a search under the Fourth Amendment.[226] If the Court held that the GPS tracking was analogous to constant police surveillance, then no warrant would be required because there is no reasonable expectation of privacy on public roads.[227] On the other hand, if the Court found that the surveillance constituted a search, where a reasonable expectation of privacy exists,[228] then such tracking would be unconstitutional without a warrant.[229]

The Court chose a third option, declaring that the GPS tracking of Jones was a search, but only because "[t]he government physically occupied private property for the purpose of obtaining information [and] . . . such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[230] Because the police

---

221. This is a reference to Odysseus' dilemma of passing between Scylla and Charybdis. *See* QBE Ins. Corp. v. Jorda Enter., Inc., 277 F.R.D. 676, 686 n.5 (S.D. Fla. 2012). "Scylla was a supernatural creature, with twelve feet and six heads on long, snaky necks. Charybdis, who lurked under a fig tree on the opposite shore, drank down and belched forth the waters three times a day and was fatal to shipping." *Id.* (citing *Scylla and Charybdis*, BRITANNICA.COM, *available at* http://www.britannica.com/EBchecked/topic/530331/Scylla-and-Charybdis (last visited Feb. 26, 2012).

222. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) *cert. denied*, 131 S. Ct. 671 (2010) *and cert. granted*, 131 S. Ct. 3064 (2011) *and aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945, 946 (2012).

223. *Id.* at 946, 962.

224. *Id.* at 946.

225. *Id.*

226. United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring).

227. *Id.* at 964 (citing U.S. v. Knotts, 460 U.S., 276, 281–82 (1983)).

228. *Id.* at 964.

229. *Id.*

230. *Id.* at 949.

physically invaded the exterior of Jones's vehicle and installed the GPS device, the Court unanimously held that Jones' Fourth Amendment rights were violated.[231]

Although not specifically germane to the topic of warrantless cell phone searches, *Jones* presented an opportunity for the Court to consider how to treat new technologies under the Fourth Amendment. While the Court reached the correct result, it once again refused to confront modern technological challenges to the Fourth Amendment and relied on the physical invasion of Jones's vehicle to justify its ruling. This justification simply ignores reality and Justices Alito and Sotomayor's separate concurrences identified this problem.[232] Justice Alito's concurrence observed that the shortcoming in the majority opinion was that, by focusing on the physical intrusion requirement, the Court failed to address whether such surveillance would be permissible if conducted remotely.[233] Justice Alito posited the following:

For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property.[234]

Justice Sotomayor, in particular, sought to bring the ruling into contemporary focus by observing:

[T]he Government will be capable of duplicating the monitoring undertaken in this case by enlisting . . . GPS-enabled smartphones . . . . In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance.[235]

The physical-search rationale not only conflicts with *Katz*, where no actual physical intrusion was required to constitute a search under the Fourth Amendment, but also fails to capture the *virtual* reality. These are not problems of a brick and mortarworld. Thus, the solutions should not be so limited. The Court should embrace the original intent of the Fourth Amendment and fashion a modern rule that comports with reality.

Consider the GPS-enabled smartphone likely resting at your hip, in your pocket, or inside your purse. It is an open question whether the police

---

231. *Jones*, 132 S. Ct. at 953.

232. *Id.*at 954 (Sotomayor, J., concurring), 957–58 (Alito, J., concurring).

233. *Id.* at 958 (Alito, J., concurring).

234. *Id.* at 962 (Alito, J., concurring).

235. *Id.* at 955 (Sotomayor, J., concurring). Interestingly, Justice Sotomayor also questioned the legitimacy of the Fourth Amendment's third-party doctrine, stating, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *Id.* at 957 (Sotomayor, J., concurring).

could remotely track your every movement, without a warrant, using your phone's GPS chip. While *Jones* is another narrow victory for the Fourth Amendment, the Court cannot sustain its practice of pressing the "ignore" button when called to duty. The Court cannot continue its application of laws developed in a brick and mortar world to issues created by a virtual world.

IV. EMPLOYER HANDBOOK DATA SECURITY POLICIES

While the Court flounders on the issue of whether there is a reasonable expectation of privacy in the contents of mobile devices, and as the government continues its use of cell phone surveillance and forensic technology for crime intervention, businesses cannot take any measure that would provide absolute data security. It is clear that more stringent, conservative data security policies must be enacted, but only complete abstinence from mobile technology would be able to beach the UFED. Still, there are some policy enactments that can reduce a fair degree of risk. This Part will first consider the typical cell phone security policies used by businesses today, and then suggest additions or amendments to current data security policies that should be employed in light of the lack of Constitutional protections of mobile cell phone data.

Many professions have ethical obligations to ensure confidentiality of client information. Attorneys, for example, have a duty to use methods of communication that afford clients a reasonable expectation of privacy.[236] The American Bar Association's Model Rules of Professional Conduct state that attorneys have an ethical duty to "hold inviolate" confidential information pertaining to clients.[237] Some commentators suggest that attorneys should discuss with clients the intent to communicate in electronic format, and confirm with them their preferred method of communication.[238]

Additionally, attorneys should "determine who has access to a client's e-mail messages before corresponding by e-mail."[239] To ensure that destination addresses are correct, one should also send test e-mails, absent confidential information, and request that clients confirm the receipt of such emails.[240] Attorneys, as well as other professionals, should also provide a "confidentiality notice" in emails that states that the contents of such communications are confidential.[241] Typical policies require that e-mails and

236. MODEL RULES OF PROF'L CONDUCT R. 1.6.

237. MODEL RULES OF PROF'L CONDUCT R. 1.6.

238. Howard S. Richman & Elise R. Sanguinetti, *Protect Client Confidentiality in E-Mail*, 44 TRIAL 59 (October 2008), *available at* 2008 WL 4830593.

239. *Id.*

240. *Id.*

241. *Id.*

other communications are password-protected, and that software suites protect networks that store confidential data.[242] Finally, commentators guide attorneys to create a destruction procedure for electronic confidential information.[243]

These cautions equally extend to HIPAA liability in the medical setting, and employment and labor attorneys advising hospital administrators should encourage handbook policies to include the same protection methods prescribed for attorneys.[244] Commentators on HIPAA liability and mobile devices observe that the lack of password controls, encryption of data, as well as the threat of human error should make medical employers "extremely cautious" about allowing offsite use of access to personal health information through mobile technology, like smartphones, laptops, home-based personal computers, tablet PC's, and other devices.[245] To avoid the infiltration of data systems storing personal health information, commentators state that policies and procedures addressing remote access should be included in trainings that make employers aware of potential threats to data integrity.[246] Authorities suggest that providers include password management procedures for changing and safeguarding passwords, policies that prohibit leaving devices in unattended cars or public thoroughfares, and policies prohibiting the transmission of confidential information over open networks, which includes e-mail and the Internet.[247]

These protection measures are ubiquitous for businesses that allow mobile access to confidential information. Unfortunately, just as technology becomes outdated, so do the handbook policies attempting to control its use. Certainly, current password-protection policies fail to protect against the threat of UFEDs. More importantly, businesses must proactively safeguard data to protect against new and emerging threats.

Returning to the hypothetical client in Part I, if a healthcare provider or attorney is asked to give a police officer her mobile device, or if she is stopped and a police officer searches the phone as an incident to a lawful arrest, even the most confusing passwords would not prevent the dissemination of confidential communications. Against common hackers, policies like that of the lawyer or doctor outlined above would probably be sufficient,

---

242. *Id.*

243. *Id.* Additionally, Professor Andrea M. Matwyshyn provides an excellent overview of the evils related to information vulnerability, which she notes places businesses at risk of criminal prosecutions and civil lawsuits for data breaches. Andrea M. Matwyshyn, *Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*, 84 CHI.-KENT L. REV. 713, 714–15 (2010).

244. *Experts Say Smart Phones at Equal or Greater Risk for Security Breaches; Users Fail to Safeguard Data*, 10 No. 2 GUIDE MED. PRIVACY & HIPAA NEWSL. 5 (March 2011).

245. *Id.*

246. *Id.*

247. *Id.*

where hackers cannot easily gain physical access to a cell phone's hard drive. The government, however, equipped with a UFED, can access troves of confidential data without a warrant.

This Note argues that businesses must employ conservative data security policies. The most conservative policy would simply prohibit employee access to confidential information using mobile handsets or communicate confidential information through mobile e-mail or text messages. In the wake of the shipwrecked Fourth Amendment jurisprudence of the digital age, such a policy may be appealing. Theoretically, only with a complete proscription of mobile access to confidential information can businesses effectively limit liability from breached information systems.

Such a policy is far from practical. Businesses could hardly survive in the Digital Age without mobile communication by their employees. Instead, and in addition to several of the security measures outlined above, employers need to first recognize that data insecurity is largely caused by human error.[248] Accordingly, employers must work with IT professionals to build safe networks and create handbook policies that recognize dangers and proactively guard against this.

The first step a business should take is to educate its workforce about the danger of data breaches by identifying weaknesses and correcting problematic behaviors. For example, the hypothetical doctor consented to the officer's search. While there is an open question of whether there is a reasonable expectation of privacy in the contents of a mobile phone, the doctor by no means should have consented to the search. Instead, the doctor should have objected to the search and, if the officer pressed on, should have contacted her attorney.

Data security education should also be periodical. Employee handbooks are certainly useful tools but are often used in a reactionary manner when contemplating an adverse employment action against an employee. Instead, businesses should periodically retrain employees regarding proper data security. For example, the Department of Defense requires all employees to obtain free, web-based certifications relating to the protection of data security.[249] The certifications are obtained annually.[250] Similar training policies for businesses will impact the rate of human error.

Employers should equally be prepared for any data breach and create procedures to address the problem. The first step should be to instruct the employee to contact their supervisor and inform them of the nature of the

248. *See* Colleen L. Rest, *Electronic Mail and Confidential Client-Attorney Communications: Risk Management*, 48 CASE W. RES. L. REV. 309, 316 (1998) ("human error is another basis for security risk").

249. *Personally Identifiable Information Training*, DONCIO.MIL, *available at* http://www.doncio.navy.mil/Products.aspx?ID=808 (last accessed Feb. 25, 2012).

250. *Id.*

breach. The IT Department should install a remote wiping software on all phones that can clear any stored data on a mobile handset. An example of such a program is Norton Mobile, a service that allows a lost or stolen phone to be remotely wiped.[251]

Finally, employers should discuss the possibility of PGP-encryption for mobile phones, tablets, laptops, and other mobile technology capable of such encryption with an IT professional.[252] If the business has an IT Support department, employee orientation should include a short presentation regarding the need and ability of PGP encryption of various smartphones. The operating system of the phone, depending on whether it is a true smartphone or whether it is a simple cell phone, will likely determine if PGP encryption is possible.

The state of the Fourth Amendment is unfortunate. Businesses are well-equipped to defend against would-be hackers from the private sector, but lack meaningful protection of the laws against government intrusions. Without adequate legal protections, businesses should educate employees about how to limit the controllable risks of data infiltration in a holistic fashion. The Court's reasoning that the judiciary risks error when considering new technology before it has settled into place results in the bastardization of the founder's intent behind the Fourth Amendment. Instead of ignoring the traditional notions of the *privacies of life*, the Court should rigorously uphold the Constitution.

V. CONCLUSION

With the diverging views amongst the courts, the lack of guidance from the Supreme Court, and the pervasiveness of governmental surveillance of cellular data, businesses should cautiously allow employees to use cell phones in the work place when communicating or accessing confidential information. New technologies which enable the radical expansion of police surveillance operations require correspondingly robust legal forces to balance the government's power. The Court should follow the intent of the Framers in limiting the ability of the government from slipping into authoritarian rule and zealously uphold the Fourth Amendment's plain and simple

---

251. *Using the SMS Anti-Theft Features of Norton Mobile Security*, NORTON.COM, http://community.norton.com/t5/Norton-Mobile-and-Tablet-KB/Using-the-SMS-Anti-Theft-features-of-Norton-Mobile-Security/td-p/583144 (last accessed Feb. 25, 2012).

252. *Overview of PGP*, PRETTY GOOD PRIVACY, http://www.pgpi.org/doc/overview/ (last accessed Feb. 25, 2012). "PGP," short for *pretty good privacy*, is a public key encryption program that is relatively old, but may prevent against physical extraction of mobile data. *See e.g.*, Genao v. United States, 2009 WL 1033384, at *4 (S.D.N.Y. 2009) ("when representatives of the Government tried this password on files that were encrypted by PGP ("Pretty Good Privacy"), they could not open the files").

language. Establishing a clear rule that requires law enforcement agencies to obtain warrants to perform cell phone searches would provide needed guidance to law enforcement agencies, quell litigation, protect fundamental liberties, and allow businesses to keep pace with technology without the unnecessary exposure to litigation.

*Abtin Mehdizadegan**