2010

Katz in the Era of Mobile Computing: How Society's Changing Expectations of Privacy Impact the Law

Michael B. Fusco
Seton Hall Law

KATZ IN THE ERA OF MOBILE COMPUTING: HOW SOCIETY'S CHANGING EXPECTATIONS OF PRIVACY IMPACT THE LAW

Michael B. Fusco

TABLE OF CONTENTS

I. INTRODUCTION

As technology has rapidly evolved over the past century there has been a great schism created between technical advances and the refinement of the laws in order to protect the rights of citizens. This friction frequently takes years to remedy and often results in scattered case law and a patchwork of statutory provisions that make compliance with the law daunting for aspiring innovators. The time has come for the legal community to address issues related to privacy in the context of mobile devices.

While it is easy to take the idea of privacy for granted, the justification behind the "right to be let alone" has developed generation-by-generation and evolved gradually throughout the history of our nation. What began as a revolutionary era desire to be free from illegal governmental searches and seizures evolved into a moral right cherished by intellectuals. By the end of the 19th century, legal scholars recognized a legal "right to privacy" and classified certain invasions as tortuous acts punishable with damages. With the dawn of electronic communications the common law right to privacy became a constitutionally mandated "expectation" in the context of governmental searches. The 21st century has brought the prospect of universal communication via mobile devices and the current law has reached a cresting point as it relates to new technologies.

This paper seeks to briefly document the development of privacy law and it's relationship to technological developments in an effort to project where the law should go given the looming era of ubiquitous wireless mobile computing. In order to narrow the scope of discussion, the focal point will be the evolution of the *Katz* "expectation of privacy" in governmental searches and seizures under the Fourth Amendment. The resulting analysis will be presented in light of changing *technologies*, *ideologies* and *expectations*.

II. A BRIEF HISTORICAL OVERVIEW OF THE RIGHT OF PRIVACY

It was two young Harvard Law School graduates who warned, "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[1] While this dire prediction seems to fit squarely into the discussion of mobile devices, it was actually a reference to George Eastman's development and popularization of the film roll and "Kodak Camera™" in 1885.[2] The rise of "yellow journalism" created a cause for alarm within legal circles that the scope of generally accepted legal rights should be broadened to include the "the right to be let alone."[3]

A. From a Moral Right to a Legal Right: "The Right to Privacy"

Samuel Warren and Louis Brandeis's 1890 law review article gave birth to the notion of "privacy"-- a concept that there is an injury caused by the invasion of privacy that can be remedied by law. They wrote, "the existing law affords a principle from which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds." Borrowing from the French right of privacy,[4] the authors outlined six limits on the right to privacy.[5] More importantly they suggested legal remedies for the invasion of the right of privacy in the form of either "an action of tort for damages" or the limited possibility of "an

---

[1] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[2] http://www.kodak.com/global/en/corp/historyOfKodak/eastmanTheMan.jhtml.
[3] Thomas C. Cooley, LAW OF TORTS 29 (2d ed. 1888).
[4] LOI RELATIVE À LA PRESSE (May 11, 1868).
[5] Warren and Brandeis's limits on the right to privacy: 1) "does not prohibit any publication of matter which is of public or general interest," 2) "does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel," 3) probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage," 4) "The right to privacy ceases upon the publication of the facts by the individual, or with his consent," 5) "the truth of the matter published does not afford a defence [sic]," and 6) "the absence of "malice" in the publisher does not afford a defence [sic]."

injunction." Within a decade courts had begun to acknowledge the invasion of privacy as a tort cause of action[6] and in 1903 New York became the first state to enact a privacy statute.[7] By 1960, courts had tried over 300 privacy court cases that William Prosser broke down into four distinct "invasion of privacy torts": (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light, and (4) appropriation.[8]

B. From a Legal Right to a Constitutional Right: Brandeis Dissents in Olmstead

Almost exactly a century before Warren and Brandeis penned their article, a group of men gathered on Wall Street to discuss potential limitations on the powers of the Federal government. Drawing from Lockean principles of protecting citizen's economic rights against government,[9] the debate focused upon protection against invasion of "the sanctities of a man's home and the privacies of life."[10] Improving upon the prohibition against baseless search and seizure found in Virginia's *Declaration of Rights*,[11] they resolved that it is the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[12] These men were the first Congress of the United States and their proposal was the Bill of Rights.

By 1928, Brandeis had become an associate justice of the United States Supreme Court and again a small group of men were debating citizen's rights to privacy from governmental searches, only this time it was in light of the latest technological innovation-- the telephone. In a 5-4 decision authored by Chief Justice William Taft -- the former President -- the Supreme Court

---

[6] *Pavesich v. New England Life Insurance Co*., 50 S.E. 68 (Ga. 1905).
[7] N.Y. CIV. RIGHTS ACT § 51 (1903).
[8] William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
[9] Jerome Huyler, *Locke in America: The Moral Philosophy of the Founding Era*, 218-250 (1995).
[10] *Boyd v. United States*, 116 U.S. 616 (1886).
[11] V.A. DECL. OF RIGHTS, ART. 10 (1776).
[12] U.S. CONST. AMEND IV.

held that telephone wires extending outside of one's home "are not within the protection of the Fourth Amendment"[13] and thus telephone conversations were subject to interception by the government. In one of the most famous dissents in Supreme Court history,[14] Justice Brandeis made a compelling argument against the "evil incident to invasion of privacy."[15]

Brandeis's opinion is prophetic in warning against the invasion of individual security afforded by new technologies: "the progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping." He argued that in light of the fact that "subtler and more far-reaching means of invading privacy have become available to the government," the Supreme Court should extend the protection of the Fourth Amendment to telephone conversations as well as "every unjustifiable intrusion by the government upon the privacy of the individual." His reasoning was based upon the idea that drafters of the Constitution sought to promote the pursuit of happiness, therefore "they conferred, as against the government, the right to be let alone-- the most comprehensive of rights and the right most valued by civilized men."

While the holding in *Olmstead* was settled law for nearly 40 years, Brandeis's concerns about the development of technology proved true as the sophistication of electronic surveillance increased in the 1960's. In 1963, the Supreme Court narrowly upheld the use of an informant using a hidden recording device, but the dissent relied heavily upon Brandeis's theory of privacy.[16] Justice Brennan warned against the narrow application of the Fourth Amendment, fearing that it could have a chilling effect on speech: "there is only one way to guard against such

[13] *Olmstead v. United States*, 277 U.S. 438 (1928).
[14] http://www.rbs2.com/privacy.htm.
[15] *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, J. dissenting).
[16] *Lopez v. United States*, 373 U.S. 427 (1963).

a risk, and that is to keep one's mouth shut on all occasions." He further concluded that "the right of privacy would mean little if it were limited to a person's solitary thoughts."

C. From a Constitutional Right to an Expectation: Katz's "Expectation of Privacy"

In 1967, the Supreme Court had come full circle and was now willing to extend Fourth Amendment protection to warrantless wiretaps of telephone conversations held in public telephone booths.[17] Justice Stewart's majority opinion states that "the Fourth Amendment protects people, not places . . . but what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[18] The *Katz* test, articulated in Justice Harlan's concurrence, was a "twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Subsequent Supreme Court majority decisions embraced this test[19] and Congress showed their support with the enactment of the Federal Wiretap Act in 1968.[20]

In abandoning the *Olmstead* decision, the Supreme Court not only expanded the scope of Fourth Amendment protection but also created a sliding scale framework for privacy based upon the expectations of both the citizen and society. *Katz* created a useful method for courts to gradually adjust Fourth Amendment protections as technology evolved and changed expectations as to the right of privacy. In theory, it has become that Fourth Amendment protection only applies where society expects privacy. In practice, mobile devices have rapidly narrowed not only the places people consider private but also the information.

---

[17] *Katz v. United States*, 389 U.S. 347 (1967).
[18] *Id*. at 351.
[19] *See Smith v. Maryland*, 442 U.S. 735 (1979).
[20] THE OMNIBUS CRIME CONTROL AND SAFE STREETS ACT OF 1968, Title III, 18 U.S.C §§ 2510-20 (1968).

D. Then and now: Technology from 1967 to 2010

Just two years before *Katz*, a computer science professor named Gordon Moore stated "the complexity for minimum component costs has increased at a rate of roughly a factor of two per year."[21] As his projection proved true, the scientific community began to describe the constant progress of computing power as "Moore's Law." The first electronic computer, created in 1945, filled an entire room and had a clock speed of 100,000 pulses per second (0.1 mHz).[22] In 1971, Intel introduced it's first microprocessor, the 4004™, which had a clock speed of 740 kHz (.74 mHz) and was roughly the size of a fingernail.[23] Just last year, Apple introduced the iPhone 3GS™, a smart phone with a processor clock speed of 600 mHz.[24] Just as Moore had predicted, these advancements mean that an iPhone user has a pocket-sized device that is 800 times more powerful than the fastest processor being developed at the time *Katz* was decided.

Almost more important than the advancement of silicon wafer microchips is the rapid development of wireless technologies in the first decade of the 21st century. Much of the analysis in *Olmstead* and later *Katz* focused on the fact that telephone wires can originate in one's home yet travel through public forums at the other end of the conversation. Wireless cell phones have become a staple of modern society, with over 89% of Americans identifying themselves as cell phone users.[25] Since communication on a mobile device by definition can originate anywhere the user get's reception, there is no longer an expectation that personal telephone conversations would be conducted within one's home.

---

[21] Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, ELECTRONICS MAGAZINE (Apr. 19, 1965).
[22] http://isc.temple.edu/sdrury/survey/detail/ENIAC.html.
[23] http://www.intel.com/museum/archives/4004facts.htm.
[24] http://www.appleinsider.com/articles/09/06/10/a_closer_look_at_iphone_3g_s_cortex_a8_arm_and_powervr_chips.html.
[25] http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf.

In December 2000, Microsoft CEO Bill Gates wrote an essay proclaiming the arrival of the "Internet Age."[26] Gates predicted "by enabling instantaneous and seamless communication and commerce around the globe, *from almost any device imaginable*, this technology will be one of the key cultural and economic forces of the early 21st century."[27] Gate's prediction has already proven true as today over 79% of adults in America are internet users and 55% connect to the internet wirelessly.[28] The ability to send and receive data electronically using a mobile device has meant that users not only have access to their own personal data (such as mobile online banking) but also are more likely to upload new personal information to the internet from their cell phones (such as posting a photo or status update on Facebook).

Katz made clear that the Fourth Amendment does not protect spaces, but rather people.[29] In the "internet age" people are defined not by sensory observations but rather their personal data. Today, the average American would have little problem with their picture being taken by a photojournalist (as was the complaint of Warren and Brandeis) but would most likely object to the electronic transmission of their medical history to a third party without their consent. Congress has created laws that reflect these modern societal norms in establishing photographer's rights[30] and enacting the Health Insurance Portability & Accountability Act (HIPAA).[31]

---

[26] http://www.microsoft.com/presspass/exec/billg/writing/shapingtheinternet.mspx.
[27] *Id.* (emphasis added).
[28] http://www.pewinternet.org/Reports/2010/Internet-broadband-and-cell-phone-statistics.aspx.
[29] *Katz*, 389 U.S. at 351.
[30] http://www.krages.com/ThePhotographersRight.pdf.
[31] *See* THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ("HIPAA"), codified at 42 USC § 201 et seq.

E. The State of the Art: App Phones

The current state of the art for mobile devices is what *The New York Times* columnist David Pogue has termed "app phones."[32] A generation beyond the "smart phone" ("a cellphone with e-mail") "this new category — somewhere between cellphones and laptops, or even beyond them — deserves a name of its own." The app phone feature list -- pioneered by the introduction of the iPhone -- typically includes: multiple wireless technologies (wifi, 3G, Bluetooth), a full web-browser, a video camera, proximity sensors ("light, tilt, location, proximity") and even a Global Positioning System ("GPS"-- a location technology that uses satellite data). In addition to advanced hardware, app phones feature operating systems that allow users to store vast amounts of personal information in the form of calendars, contacts, photo albums, financial calculators and even medical information.

Apple has sold over 50 million iPhones[33] and has a library of over 185,000 downloadable iPhone "apps,"[34] which are essentially small single-purpose applications. These apps are capable of using the iPhone's hardware to input data, collect personal information and transmit it to potentially anyone connected to the internet. Mobile users commonly use apps to trade stocks, make purchases, locate restaurants and can even be used to read an MRI.[35] Dumping cell phone data used to be simply getting numbers, but with the iPhone, now it's everything about your life and often every bit of data you own.

The fact is that cell phones cannot only be used in the facilitation of a crime (calling the getaway driver) but can actually be the crime scene itself. The government has an active interest

[32] http://www.nytimes.com/2009/11/05/technology/personaltech/05pogue.html.
[33] http://events.apple.com.edgesuite.net/1004fk8d5gt/event.
[34] http://www.macrumors.com/2010/04/08/apples-iphone-os-4-0-media-event-sneak-peek-into-the-future.
[35] http://itunes.apple.com/us/app/osirix/id296246375

in monitoring app phone activity if the device is being used for illegal gambling, fraudulent financial transactions or child pornography. However, access to this data may not be constitutional, as many would consider this data to be private and protected under the Fourth Amendment.

The apps often store their data not only locally on the mobile device, but also transmit certain data to remote servers wirelessly in order to provide increased functionality. With many users unaware of how their personal data is stored or transmitted using an app phone, it becomes difficult to gauge what their "actual (subjective) expectation of privacy" might be under the first prong of the *Katz* test. If a mobile wireless user were to be subject to a governmental search of their app phone data, it is unclear to what extent "society is prepared to recognize as 'reasonable'" under the second prong of *Katz*. A thorough review of case law will help reveal how courts have dealt with past technological developments and this should provide some answers as to the direction the law should take in the future.

III. REVIEW OF CASE LAW

In the four decades since *Katz* was decided, technology has evolved at a faster pace than any other time in human history.[36] In the context of criminal investigations, courts have been reactive in addressing new technological developments, creating a remedial patchwork of case law with each new innovation. For purposes of analysis, the major cases will be broken down chronologically by innovation: (a) the telephone, (b) electronic surveillance, (c) the personal computer, (d) the internet and (e) the mobile phone. Note that even with these major evolutions in technology, the basic "expectation of privacy" test outlined in *Katz* remains the Constitutional guidepost for determining Fourth Amendment rights.

[36] *See* Ray Kurzweil, *The Law of Accelerating Returns* (Mar. 7, 2001) (available KurzweilAI.net).

A. The Telephone: The Katz Progeny

Decided in the final years of the Warren Court, the *Katz* ruling gave rise to the public perception that telephone conversations were constitutionally protected under the Fourth Amendment. Chief Justice Warren himself was such a firm believer in personal privacy that as a District Attorney in California he is said to have refused to wire tap the cell of a prisoner suspected of murdering his father, Methias Warren.[37] By 1969, the Supreme Court was under the leadership of Warren Burger and was charged with the task of deciding how to apply the *Katz* doctrine.

In 1971, the Supreme Court held in *United States v. White* that recordings of conversations obtained by undercover informants through the use of electronic listening devices were admissible in a criminal trial.[38] Much of the rationale for this holding was based on the idea that an agent could already constitutionally transcribe,[39] record,[40] or electronically transmit[41] a conversation without violating a suspect's Fourth Amendment rights. The majority reasoned that "if the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the state's case."[42] Some saw the ruling in *White* as a degradation of the rights instilled by *Katz*. In an apocalyptic dissent, Justice Douglas' warned that unsupervised electronic surveillance would lead to a police state, stating

---

[37] Yale Kamisar, *How Earl Warren's Twenty-Two Years in Law Enforcement Affected His Work as Chief Justice*, 3 OHIO ST. J. CRIM. L 11, n. 6 (2005).
[38] *United States v. White*, 401 U.S. 745 (1971).
[39] See *Hoffa v. United States*, 385 U.S. 293, 300-303 (1966).
[40] See *Lopez v. United States*, 373 U.S. 427 (1963).
[41] See *On Lee v. United States*, 343 U.S. 747 (1952).

[42] *United States v. White*, 401 U.S. 745, 752 (1971) (citing *Lopez v. United States*, 373 U.S. 427 (1963)).

that "what the ancients knew as 'eavesdropping,' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb."[43]

In *Smith v. Maryland* the Supreme Court sought to determine whether the government could constitutionally utilize data obtained from a "pen register" in monitoring a suspect's home phone activity.[44] A "pen register" is a mechanical device installed at the central telephone facility that is used to record numbers dialed on a telephone.[45] Applying *Katz*, the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[46] Likening call activity to bank deposit records, the majority found that the suspect "assumed the risk that the company would reveal to police the numbers he dialed"[47] and therefore use of such call logs by the government did not amount to a "search" under the Fourth Amendment.

Following *Smith* there was once again public outcry regarding the degradation of *Katz*,[48] so much so that Congress passed legislation in 1986 limiting the use of such devices in law enforcement.[49] Some state courts even outright rejected the holding in *Smith*. For example, the New Jersey Supreme Court found a reasonable expectation of privacy in telephone records under the state constitution.[50] While the content of one's private conversations remained protected under *Katz*, it was now possible for the government to constitutionally obtain transactional data about a suspect's telephone activity.

---

[43] *United States v. White*, 401 U.S. 745, 756 (1971) (Douglas, J. dissenting).
[44] *Smith v. Maryland*, 442 U.S. 735 (1979).
[45] *Id.* at 736, fn. 1.
[46] *Id.* at 743.
[47] *Id.*
[48] *See* Lawrence Tribe, AMERICAN CONSTITUTIONAL LAW 1391 (2d ed. 1988).
[49] *See* 18 U.S.C. §§ 3121-3126 (2005).
[50] *See State v. Hunt*, 450 A.2d 952 (N.J. 1982).

B. Electronic Surveillance: Searching Beyond the Naked Eye

Between 1967 and 1971, a "national surveillance state"[51] had begun to emerge through the development of the "regulatory search doctrine." A regulatory search is "governed by the Fourth Amendment but does not require probable cause as defined traditionally by the Supreme Courts."[52] In 1967, the Supreme Court held in *Camara* that a warrant procedure is required under the Fourth Amendment for administrative entry and inspection of private commercial premises.[53] Yet by 1971, the Supreme Court had decided that caseworker home visits were not violations of Fourth Amendment rights, as welfare benefits were not required by law.[54] The Supreme Court took a similar stance when it came to whether or not telephone carriers were obligated to aid the government in conducting criminal investigations.[55] In *New York Telephone*, the Supreme Court held that federal courts had authority over telecommunications providers to "compel, upon request, any assistance necessary to accomplish an electronic interception."[56]

In 1972, the Supreme Court handed down the "*Keith*" case, holding that the Fourth Amendment required judicial approval before the government could conduct electronic surveillance for domestic criminal investigations.[57] The majority proclaimed that the Warrant Clause of the Fourth Amendment "is not dead language"[58] nor "an inconvenience to be somehow 'weighed' against the claims of police efficiency," rather it is "an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but

---

[51] Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008).
[52] *United States v. Seslar*, 996 F.2d 1058, 1061 (1993).
[53] *Camara v. Municipal Court of San Francisco*, 387 U.S. 523 (1967).
[54] *Wyman v. James*, 400 U.S. 309 (1971).
[55] *See United States v. New York Telephone*, 434 U.S. 159 (1977).
[56] *Id.* at 176-177.
[57] *United States v. U.S. District Court*, 407 U.S. 297 (1972).
[58] *Id.* at 315.

mistakenly overzealous executive officers' who are a part of any system of law enforcement."[59] The Supreme Court seemed very much at ease with the government's use of electronic surveillance-- so long as the judiciary was able to act as a check on executive power.

For nearly two decades, courts have looked approvingly upon video surveillance in domestic criminal investigations.[60] In *Taketa*, the Ninth Circuit wrote that "videotaping of suspects in public places, such as banks, does not violate the [F]ourth [A]mendment; the police may record what they normally may view with the naked eye."[61] However, courts have reasoned that "even if one cannot expect total privacy while alone . . . [a] diminished privacy interest does not eliminate society's expectation to be protected from the severe intrusion of having the government monitor private activities through hidden video cameras."[62] In *Trujillo*, the Ninth Circuit ruled that there was a reasonable expectation of privacy in a police locker room and therefore a video surveillance camera that "recorded [the officers] in various states of undress" violated the Fourth Amendment.[63]

Today, video surveillance cameras operated by government agencies are so ubiquitous, that citizens often complain when they are not present or functional.[64] However, the development of new surveillance technologies has created cameras that can see well beyond what a human "may view with the naked eye."[65] It is well established that there is no reasonable expectation of privacy in "open fields," even when one attempts to keep them shielded from public view.[66] In *Dow Chemical*, the Supreme Court held that "the taking of aerial photographs of an industrial

---

[59] *Id.* at 315-316 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)).
[60] *United States v. Koyomejian*, 946 F.2d 1450 (9th Cir. Cal. 1991).
[61] *United States v. Taketa*, 923 F.2d 665, 667 (9th Cir. Nev. 1991).
[62] *United States v. Nerber*, 222 F.3d 597, 604 (9th Cir. Wash. 2000).
[63] *Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1104 (C.D. Cal. 2006).
[64] http://www.nytimes.com/2010/03/30/nyregion/30subway.html.
[65] *United States v. Taketa*, 923 F.2d 665, 667 (9th Cir. Nev. 1991).
[66] *Oliver v. United States*, 466 U.S. 170 (1984).

plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[67] The opinion states that "the mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[68] Much of the majority's reasoning is based on the fact that the camera used was a standard aerial photography camera that was generally available to the public. The majority conceded that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[69]

In *Dow Chemical*, Justice Burger prophetically imagined "an electronic device to penetrate walls or windows so as to hear and record confidential discussions of chemical formulae or other trade secrets" and warned that such a device "would raise very different and far more serious questions."[70] By 2001, police had begun to use thermal imaging cameras to detect infrared radiation given off by the presence of special high-intensity lamps used for the growth of marijuana in suspect's homes. In *Kyllo*, the Supreme Court held that use of such a device "to explore details of the home that would previously have been unknowable without physical intrusion" amounted to a "search" under the Fourth Amendment and is presumptively unreasonable without a warrant.[71] The majority rested their opinion upon the fact that the government was using a device that was not in general public use. Taken in combination, *Dow Chemical* and *Kyllo* can be read together to suggest "government use of new technologies should always be subject to the warrant requirement unless they are in general public use."[72]

---

[67] *Dow Chemical Co. v. United States*, 476 U.S. 227, 239 (1986).
[68] *Id.*
[69] *Id.* at 237.
[70] *Id.* at 239.
[71] *Kyllo v. United States*, 533 U.S. 27, 40 (2001).
[72] Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1329 (2002).

The Supreme Court has expressed concern about surveillance techniques that invade citizen's lawful activities, such as thermal imaging cameras,[73] but seems less concerned with techniques that reveal only unlawful activities.[74] For example, the Supreme Court held in *Place* that "a 'canine sniff' by a well-trained narcotics detection dog" was *sui generis* in the fact that "it does not expose noncontraband items that otherwise would remain hidden from public view."[75] In 1998, the FBI began using "packet sniffer" technology called "Carnivore" that was able to search internet traffic for certain keywords pertaining to investigations.[76] The system was "in principle capable of searching through that data in order to find particular names, or key phrases such as 'nuclear bomb.'"[77] There was much public outcry over the use of Carnivore and the privacy concerns it raised were "eerily reminiscent of George Orwell's book '*1984*.'"[78] Despite the fact that the system -- in theory -- only revealed unlawful activities, it was abandoned in early 2005 in favor of commercially available software programs.[79]

However, the FBI has subsequently developed "Magic Lantern" software that can record a computer user's keystrokes remotely. Previously the Supreme Court ruled that in order to install a "keystroke capture" device on a suspect's computer, agents had to show probable cause that a suspect was involved in a crime and that there was evidence of criminal activity contained on a specific computer.[80] However, Magic Lantern does not require physical access to a suspect's computer and can be installed remotely without ones consent, much like a computer

---

[73] *See Kyllo v. United States*, 533 U.S. 27 (2001).
[74] *Illinois v. Caballes*, 543 U.S. 405 (2005).
[75] *United States v. Place*, 462 U.S. 696, 707 (1983).
[76] Neil King Jr. and Ted Bridiss, *FBI System Covertly Searches E-mail*, THE WALL STREET JOURNAL (Jul. 11, 2000).
[77] E. Judson Jennings, *CARNIVORE: Little Red Riding Hood or Big Bad Wolf? An Analysis of the FBI Internet Surveillance Project*, 6 VA. J.L. & TECH. 10 (2001).
[78] http://computer.howstuffworks.com/carnivore.htm.
[79] *Id.*
[80] *See United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001).

virus.[81] For example, a suspect could unknowingly install the software by clicking on a "Click here to win!" pop-up ad.[82] This technical difference means that the government can install a keystroke logger on a suspect's computer without physically trespassing into their home,[83] creating a legal distinction within the context of the Fourth Amendment. The Ninth Circuit has recently ruled that the government's use of a key-logging surveillance device is "constitutionally indistinguishable from the use of a pen register that the Supreme Court approved in [*Maryland v.*] *Smith*."[84]

C. The Personal Computer: The Search and Seizure of Data

In 1967, the Supreme Court held in *Warren v. Hayden* that a search warrant could be issued to seize evidence of a crime.[85] Ever since the advent of the personal computing, digital storage of data has allowed authorities to reconstruct facts surrounding any number of alleged crimes through evidence obtained through computer forensics. While courts have recognized evidence obtained through governmental searches and seizures of computer data,[86] strict standards have emerged as to the validity of search warrants related to such information.[87]

The Supreme Court has repeatedly emphasized the particularity requirement of the Warrant Clause, stating "by limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be *carefully tailored* to its justifications, and will not take on the character of the wide-ranging

---

[81] Amitai Etzioni, *Implications of Select New Technologies for Individual Rights and Public Safety*, 15 HARV. J.L. & TECH 257, 277 (2002).
[82] *Id.*
[83] http://news.cnet.com/8301-10784_3-9741357-7.html.
[84] *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. Cal. 2008).
[85] *Warden v. Hayden*, 387 U.S. 294 (1967).
[86] See *United States v. Gawrysiak*, 972 F. Supp. 853 (D.N.J. 1997).
[87] *See Department of Justice Computer Search Guidelines*, at 36 (January 2001).

exploratory searches the Framers intended to prohibit."[88] The Supreme Court has rejected blanket warrants as being too broad, finding "the requirement that the warrant itself particularly describe the material to be seized is not only to circumscribe the discretion of the executing officers but also to inform the person subject to the search and seizure what the officers are entitled to take."[89]

However, in the context of computer search warrants, the Ninth Circuit has allowed generic warrants "when a more precise description is not possible."[90] It is often the case that investigators will not know what exact data they are searching for, merely the fact that evidence of a crime may be stored digitally on a suspect's computer. The Ninth Circuit has also allowed the search of a suspected child pornographer's computer without specifying any "specific acts, time frames or persons" involved.[91] Once computer equipment is seized, it is implied that "extraction of unlawful images from within the computer and diskettes was therefore contemplated by the warrant."[92] Following the Ninth Circuit's precedent, the First Circuit has also upheld a warrant that allowed for the "seizure of computer equipment," without any further particularity.[93]

Police often prefer vague search warrants, so as not to hamper the admissibility of incriminating evidence found on a computer once it has been searched. For example, in *Carey* the Tenth Circuit held that when searching a suspect's computer under a warrant for information about illegal drugs, images discovered containing child pornography were not within the scope

---

[88] *Maryland v. Garrison*, 480 U.S. 79, 84 (U.S. 1987) (Emphasis added).
[89] *In re Application of Lafayette Academy, Inc*., 610 F.2d 1, 5 (1st Cir. R.I. 1979).
[90] *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. Wash. 1997) (quoting *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982)).
[91] *United States v. Hay*, 231 F.3d 630, 637 (9th Cir. Wash. 2000).
[92] *United States v. Upham*, 168 F.3d 532, 536 (1st Cir. Me. 1999).
[93] *Id.*

of the warrant and were therefore inadmissible.[94] *Carey* states that when dealing with "intermingled documents," law enforcement "must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant."[95] However, the Ninth Circuit has allowed the searching of intermingled computer files where the difficulty of sorting the data on-site is specifically outlined in an affidavit.[96] Nevertheless, the Tenth Circuit has found that when a police warrant specifies a specific number of illegal images, and more are found on a suspect's computer, the additional images may be admissible.[97] In *Campos*, the court allowed an additional six images of child pornography to be admitted at trial even though the search warrant was based off of two specific images that had been transmitted from the suspects computer.[98]

Absent a search warrant, there are still methods for government officials to search suspect's computers under exceptions to the Warrant Clause. The well-established "plain view doctrine" allows police to search a suspect's property without a warrant when there is probable cause based on an officer's visual observations.[99] This principle is often invoked by U.S. Customs, which has the authority to examine a laptop when a citizen enters the county from a foreign nation.[100] Some state courts have held that viewable images on a suspect's computer fall under the "plain view" exception. In *Schroeder,* a Wisconsin Appellate Court held that the

[94] *United States v. Carey*, 172 F.3d 1268, 1276 (10th Cir. Kan. 1999).
[95] *Id.* at 1275.
[96] *United States v. Comprehensive Drug Testing, Inc*., 513 F.3d 1085 (9th Cir. 2008).
[97] *United States v. Campos*, 221 F.3d 1143, 1146 (10th Cir. Okla. 2000).
[98] *Id.*
[99] *Arizona v. Hicks*, 480 U.S. 321 (1987).
[100] *United States v. Arnold*, 2008 U.S. App. Lexis 8590 (9th Cir. 2008).

doctrine was applicable to an officer seeing images of child pornography displayed on the monitor of a suspect's computer.[101]

The "consent doctrine"[102] also applies in the context of computer searches under the Fourth Amendment.[103] The Eight Circuit has even allowed a co-tenant to consent to the search of one's computer without a warrant.[104] However, possessors of illegal content often take the time to password protect their computers in order to limit access to incriminating files. The Fourth Circuit has held that password protecting a user's files on a shared computer serves as an affirmative intention to exclude others from access and therefore other users could not consent to access.[105] Courts have grappled with the issue of passwords in depth, concluding "because intimate information is commonly stored on computers, it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy."[106]

In addition to passwords, users will often seek to encrypt files using software that only allows access to those with the proper cipher key. One legal scholar has concluded, "while encrypting a file cannot itself trigger Fourth Amendment protection, it does not eliminate the Fourth Amendment protections that otherwise govern law enforcement access to the file."[107]

In 2007, the Tenth Circuit outlined a broad framework for determining whether or not a computer was locked using the "totality of the circumstances" approach[108] to search and seizure

---

[101] *State v. Schroeder*, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000).
[102] *United States v. Matlock*, 415 U.S. 164 (1974).
[103] *See United States v. Brooks*, 427 F.3d 1246, 1249-53 (10th Cir. 2005).
[104] *United States v. Hudspeth*, 518 F.3d 954, 961 (8th Cir. Mo. 2008).
[105] *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. Va. 2001).
[106] *United States v. Andrus*, 483 F.3d 711, 718 (10th Cir. Kan. 2007).
[107] Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?*, 33 CONN. L. REV. 503, 531 (2001).
[108] *United States v. Kimoana*, 383 F.3d 1215 (10th Cir. Utah 2004).

consent.[109] State Courts have also recently begun to establish local standards for computer searches.[110]

The issue of shared computers often arises in the context of the workplace, where users are often given specific logins in order to access, store and share files. In the past decade, a majority of jurisdictions have held that there is no reasonable expectation of privacy in files downloaded to a workplace computer.[111] For example, the Ninth Circuit has held that there is no reasonable expectation of privacy in workplace computers and thus there is no standing to invoke Fourth Amendment protection.[112] The *Ziegler* Court reasoned, "social norms suggest that employees are not entitled to privacy in the use of workplace computers, which belong to their employers and pose significant dangers in terms of diminished productivity and even employer liability."[113] Similarly, the Tenth Circuit in *Barrows* has ruled that where a government employee brings a personal computer to work and connects to the network there is no reasonable expectation of privacy.[114] The *Barrows* opinion states that "those who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably expect their personal materials to remain private."[115] However, the Ninth Circuit has recently retreated from its earlier position in *Ziegler*, holding in an en banc rehearing that "even where a private employee retains an expectation that his private office will not be the subject of an

[109] *United States v. Andrus*, 483 F.3d 711 (10th Cir. Kan. 2007).
[110] *See In re Forgione*, 49 Conn. Supp. 613, 635 (Conn. Super. Ct. 2006).
[111] *See United States v. Simons*, 206 F.3d 392, 398 (4th Cir. Va. 2000).
[112] *United States v. Ziegler*, 456 F.3d 1138 (9th Cir. Mont. 2006).
[113] *Id.* at 1145-1146.
[114] *United States v. Barrows*, 481 F.3d 1246 (10th Cir. Okla. 2007).
[115] *Id.* at 1249.

unreasonable government search, such interest may be subject to the possibility of an employer's consent to a search of the premises which it owns." [116]

D. The Internet: Personal Data Goes Viral

A century before the first e-mail was ever sent[117] the Supreme Court created the guiding principle that today applies to government seizures of messages while in transit.[118] In 1878, *Ex Parte Jackson* held that mailed documents are private under the Fourth Amendment and therefore the government must obtain a warrant prior to seizing mailed items.[119] However, unlike traditional mail, electronic messages are often retained on third-party servers long after being "delivered." This difference creates legal issues for when the government can access potentially incriminating messages depending on what stage a message is being sought during an investigation.

Early in the days of the internet it was established that there is a reasonable expectation of privacy for e-mail served on a "centralized and privately-owned computer bank." [120] In *Maxwell*, the U.S. Court of Appeals for the Armed Forces held that an AOL user's e-mails were protected from warrantless search under the Fourth Amendment.[121] Even with a proper warrant, government agents have "the constitutional obligation of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated or the purpose for which electronic surveillance has been authorized."[122] Some Courts have even

[116] *United States v. Ziegler*, 474 F.3d 1184, 1191 (9th Cir. Mont. 2007).
[117] http://ask.yahoo.com/20010824.html.
[118] *Ex Parte Jackson*, 96 U. S. 727 (1878).
[119] *Id*. at 735.
[120] *United States v. Maxwell*, 45 M.J. 406, 411 (C.A.A.F. 1996).
[121] *Id*. at 419.
[122] James G. Carr, THE LAW OF ELECTRONIC SURVEILLANCE, § 5.7(a) at 5-28 (1994).

found that there is such a strong expectation of privacy in workplace e-mails that private interceptions of e-mail can give rise to common law claims of intrusion of privacy.[123]

There is also a longstanding legal distinction between the content of a message versus the information found on the outside of the envelope. Any investigator that is legally allowed to search e-mail header information can learn a lot about a suspect without ever infringing upon the person's Fourth Amendment rights in the content of the message.[124] Legal scholar Orin Kerr points out that "each of the lines in the mail header has specific meaning, and when read together, tells a story about the message, how it was processed, and how and when the network directed it from its origin to its destination."[125] So while the contents of an e-mail may be protected, the "who, what, where, when and how" may be revealed without a search warrant.

Courts have also found that the more transient a message is, the less the content of the message will be protected. Instant messages, text messages and chat room discussions have been analyzed differently than traditional e-mails and are more comparable to short messages found on the back of a post card. Therefore, at least some jurisdictions have held that individuals do not have a reasonable expectation of privacy for statements made in an internet chat room.[126] Much of the reasoning in such cases is that when third-parties are given access to information, there is a lessened expectation that the communication will be kept private. The Eleventh Circuit has just recently applied this same principle to e-mails, holding that there is no reasonable expectation of privacy in an e-mail once a copy has been delivered to a third-party.[127] However, the Ninth

---

[123] *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).
[124] Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611 (2003).
[125] *Id*. at 613.
[126] *United States v. Charbonneau*, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997)
[127] *Rehberg v. Paulk*, 2010 U.S. App. LEXIS 5198 (11th Cir. Ga. Mar. 11, 2010).

Circuit has found a reasonable expectation of privacy in text messages because in the Court's opinion there is "no meaningful distinction between text messages and letters."[128]

There is a strong governmental interest in intercepting certain e-mails when it comes to criminal investigations, but there has been sizable amounts of litigation on what is meant by the term "intercept."[129] In 1986, congressed enacted Title II of the Electronic Communications Privacy Act ("ECPA")[130] as a method of extending restrictions on telephone wiretaps to include electronic messages send via computer. The ECPA created three classes for electronic messages: (1) real time, (2) transient and (3) long term (more than 180 days). Therefore the Courts were able to carve out differing expectations of privacy depending on how a message was classified.

The Ninth Circuit has noted that the "ECPA was deliberately structured to afford electronic communications in storage less protection than other forms of communication."[131] It is a violation of the ECPA to intercept a "real time" message while it is in transit.[132] Similarly, an e-mail in temporary storage en route to it's final destination may not be intercepted under the ECPA.[133] There is also a narrow definition of what constitutes an "electronic communication," and the at least one Court has held that information stored in an airline's online reservation system was not subject to the ECPA.[134]

The tiered structure of classifying e-mails based on their state is useful to courts, but makes it very difficult for a government agent to answer the simple question "do the police need

---

[128] *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 905 (9th Cir. 2008).
[129] *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 462 (5th Cir. 1994).
[130] THE ELECTRONIC COMMUNICATIONS PRIVACY ACT ("ECPA"), Title II, 18 U.S.C. 2701, et. seq. (1986).
[131] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877 (9th Cir. Cal. 2002)
[132] *See Fraser v. Nationwide Mut. Ins. Co.,* 352 F.3d 107 (3rd Cir. Pa. 2003).
[133] *United States v. Councilman*, 418 F.3d 67, 70 (1st Cir. Mass. 2005)
[134] *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 304 (E.D.N.Y. 2005).

a warrant to obtain e-mail?"[135] The way e-mail actually works it is not anything like a traditional letter send through the mail, of which there is presumably just a single copy. A typical e-mail from person A to person B is stored in at least four places: (1) the sender's computer, (2) the sender's e-mail host, (3) the recipient's e-mail host and (4) the recipients computer.[136] So unlike a traditional letter, there are at least three additional copies of every message sent which are outside of the sender's constructive possession. Each copy may reside in a different jurisdiction and potentially be subject to varying laws based upon locality. This distinction makes the laws regulating e-mail hosts and Internet Service Providers ("ISPs") critical in determining what information the government may access without a search warrant.

A decade before there were any ISP's, the Supreme Court held that the government could seize evidence from third-party news organizations without violating Fourth Amendment rights.[137] Congress quickly responded to the Supreme Court's decision by passing the Privacy Protection Act ("PPA") in 1980, which limited the ability of law enforcement to use warrants in searching or seizing certain materials possessed for the purpose of public dissemination.[138] However, as one Federal judge has pointed out, "cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis."[139]

The government may require that an ISP provide stored communications and transactional records under two circumstances, if: "(1) it obtains a warrant [], or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing

---

[135] Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 365-67 (2003).
[136] *Id*. at 366.
[137] *See Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).
[138] *See* PRIVACY PROTECTION ACT ("PPA"), 42 U.S.C. § 2000aa (1980).
[139] *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999).

disclosure of the information in question."[140] Absent either of these two circumstances, the user must have a reasonable expectation of privacy in the data being sought under a traditional *Katz* analysis. To have an interest in privacy, there must be some exclusion of others to the data.[141] According to the *Hambrick* court, this is possible when two conditions have been met: "(1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure."[142] Disclosure of certain information, such as a user's public profile information, does not constitute a violation of one's Fourth Amendment's rights. In *McVeigh*, a soldier's AOL profile revealed that his sexual preferences violated the military's "Don't Ask, Don't Tell" policy, but as the profile was publically available it was not protected under the Fourth Amendment.[143]

Nevertheless, there are certain instances where an ISP warrant is not required.[144] In *Guest v. Leis*, the Sixth Circuit found that a sender "would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter."[145] Some state courts have taken different approaches as well, such as the New Jersey Supreme Court who held that a subscriber has a privacy interest in his ISP information under New Jersey's state constitution.[146]

---

[140] *Id*. (citing 18 U.S.C. § 2703(a)-(c)(1)(B)).
[141] *Id.*
[142] *Id.*
[143] *McVeigh v. Cohen*, 983 F. Supp. 215 (D.D.C. 1998)
[144] *See Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. Ohio 2001).
[145] *Id*. (citing *United States v. King*, 55 F.3d 1193, 1196 (6th Cir. 1995)).
[146] *State v. Reid*, 194 N.J. 386 (N.J. 2008)

E. The Mobile Phone: Wirelessness Leads to Lawlessness

On October 17, 1973, a Motorola researcher filed a patent for a "radio telephone system," giving birth to the first hand-held mobile phone.[147] From that point forward, telephone conversations ceased being tied to a physical infrastructure of wires and conversations became "wireless." What was once a technology limited to the privacy of ones home became available in public spaces. Just five years earlier the Supreme Court had created the "plain view doctrine," which holds that there is no reasonable expectation in privacy if it possible for something to be heard or seen from a public vantage point.[148] Taking the telephone outside of the literal language of the Fourth Amendment meant courts had to re-evaluate how the law should apply to mobile devices.

One of the major issues pertaining to mobile phones is that phone companies are able to determine where a user is located using triangulation of a user's wireless signal.[149] This technology provides mobile users with location-based services ("LBS"), including such popular uses as vehicle navigation,[150] locating nearby businesses[151] and even monitoring the location of children.[152] Critics of LBS warn that since cell phone users are almost nearly near their phones, the technology is essentially amounts to human tracking.[153] In 2003, two GPS researchers went as far as to warn that "society must contemplate a new form of slavery, characterized by location control."[154]

---

[147] U.S. PATENT NO. 3,906,166 (filed Oct. 17, 1973).
[148] *Harris v. United States*, 390 U.S. 234 (1968).
[149] http://events.apple.com.edgesuite.net/1004fk8d5gt/event.
[150] http://www.tomtom.com/products/product.php?ID=940.
[151] http://www.yelp.com/yelpmobile.
[152] https://familymap.wireless.att.com/finder-att-family/welcome.htm.
[153] J.E. Dobson and P.F. Fisher, *Geoslavery*, IEEE TECHNOLOGY AND SOCIETY MAGAZINE, 47-52 (2003).
[154] *Id.* at 48.

While there has been little legislation on the issue of LBS in mobile devices, there is well-established case law on the government's use of GPS to track suspects. In *Karo*, the Supreme Court held that "the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[155] The majority found it to be "obvious" that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."[156]

While private residences are clearly protected, the Fourth Amendment is more narrowly construed in the context of automobiles. In *Knotts*, the Supreme Court found that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and therefore the government could track a vehicle without a warrant so long as it was on a public highway.[157] This holding was based upon the earlier *Cardwell* decision, which reasoned that "one has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects."[158]

Both *Karo* and *Knotts* are often interpreted in the context of GPS, yet they were actually decided more than decade before the technology was available for civilian use.[159] Those cases involved older beeper technology, which involved wireless signal triangulation instead of satellite tracking as is found in many modern app phones. While the Supreme Court has yet to

---

[155] *United States v. Karo*, 468 U.S. 705, 714 (1984).
[156] *Id.*
[157] *United States v. Knotts*, 460 U.S. 276, 281 (1983).
[158] *Cardwell v. Lewis*, 417 U.S. 583, 590 (1974).
[159] *See U.S. Global Positioning System Policy Press Release* (available at http://clinton4.nara.gov/textonly/WH/EOP/OSTP/html/gps-factsheet.html (March 29, 1996)).

rule on GPS specifically, at least one state has ruled that police need a warrant in order to attach a GPS responder to a car. [160] However, the *Jackson* case was decided under the Washington State Constitution[161] and did not fully address the subjective expectation of privacy under the Fourth Amendment.[162]

At least one District Court has found that the government is allowed access to cell phone location information under the same consent reasoning discussed above in *Smith v. Maryland*.[163] Judge Gorenstein of the Southern District of New York concluded that "Congress expected physical location information -- including cell site information -- would be obtainable by the Government by using some mechanism in combination with the Pen Register Statute."[164] There have been at least three other District Court cases on government access to cell site data,[165] none of which flatly prohibited government access to such data under the Fourth Amendment.

IV. DISCUSSION

Warren and Brandeis wrote of their article, "it is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is." This paper has the

---

[160] *State v. Jackson*, 76 P.3d 217, 224 (Wash. 2003).
[161] WASH. CONST. ART. I § 7.
[162] *Jackson*, 76 P.3d at 222.
[163] *In re United States for Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435, 443 (S.D.N.Y. 2005).
[164] *Id*. at 443.
[165] *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005) ("Texas Decision"); *In re United States for an Order Authorizing the Use of a Pen Register*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) ("EDNY Decision); and *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information*, 402 F.Supp.2d 597 (D. Md. Nov. 29, 2005) ("Maryland Decision").

same goal, merely time shifted to the present era of the "mobile internet tsunami"[166] in which we currently live. This discussion will seek to identify changes between the time *Katz* was decided and now, specifically related to *expectations*, *technologies* and *ideologies*.

A. Changing Expectations

> *"There was of course no way of knowing whether you were being watched at any given moment… It was even conceivable that they watched everybody all the time. But at any rate they could plug into your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinized."* [167]
>
> *- George Orwell, "1984"*

The *Katz* test has created a sliding scale approach to interpretation of the law such that as society's expectations change, therefore the law should as well. The issue is complicated by the fact that the test relies upon both the individual's subjective expectations as well as objectively what society is prepared to recognize as reasonable. Without completely dismissing the first prong of *Katz*, it is safe to assume that when it comes to the admissibility of incriminating evidence obtained during a government investigation, most defendant's would argue *post facto* that they individually expected the evidence to remain private. Therefore, the crux of the issue for the purposes of this analysis is identifying the objective expectations of society with regard to the privacy of one's personal information.

In 1987, the Supreme Court laid down a number of factors to consider in measuring the expectations of society: "although there is no 'talisman' that determines whether society will find a person's expectation of privacy reasonable, a court may consider (1) the nature of the search, (2) where the search takes place, (3) the person's use of the place, (4) our societal understanding that certain places deserve more protections than others, and (5) the severity of the search."[168]

---

[166] http://www.thestreet.com/story/10570940/cramers-mad-money-recap-my-mobile-internet-index-final.html.
[167] http://www.theorwellprize.co.uk/the-award/orwellatoxford2009.aspx.
[168] *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987).

While the *Ortega* factors are still good law, the factors are greatly complicated by the scope and complexity of the internet. Government searches can now take place across borders, without the suspect's knowledge and even on anonymous or seemingly random suspects.

While courts have generally seemed to permit searches conducted on specific persons with narrowly worded warrants, the issue of warrantless "road stop" stings still persists. The problem is not so much the lack of clear statutory directives on the issue, but more the issue of a government agent in the field not knowing whether their actions are constitutional under the Fourth Amendment. To give examples of this phenomenon, three hypothetical situations will be identified and discussed.

First, there is the inadvertent possessor of child pornography. Unfortunately, much of the case law on internet searches and seizures involves child pornography or the exploitation of children. The millennial generation has dove head-first into social networking and in some social circles it is considered "normal" for people to meet over the internet prior to meeting in person. It would not be hard to imagine A meeting B online on Match.com and due to B lying about their age they actually a 16-year-old minor. After sending flirty text messages back and forth, B sends A a naked picture, which A views on their iPhone (known colloquially as "sexting,"[169] a portmanteau of "sex" and "texting.") This problem could escalate into a crime even if A was completely under the belief that B was of age.

Under the *Ortega* factors it is unclear what society's expectation would be as to A's right to privacy. Assuming the government became aware of A's possession of the illegal images from B's parents, the government would have a difficult time determining the best way to prosecute A for possession of child pornography. They would likely have tracer information from the e-mail,

[169] http://www.cbsnews.com/stories/2009/01/15/national/main4723161.shtml.

but this might only reveal an Internet Protocol ("IP") address and server information, not A's actual identity. However, if the government wanted to access data stored on A's iPhone (specifically within the Match.com app), society could easily consider such information private. The expectation of privacy would probably be less for the information made already public on A's Match.com profile, so the government could likely use that information to track down A. It is also likely that since text messages are tied to individual user's telephone numbers, the government could subpoena the cell phone provider to hand over A's contact and usage information. There might also be implications for Match.com under the Children's Online Privacy Protection Act ("COPPA").[170]

This hypothetical seems bizarre, but is apparently a common problem and some teenagers have even faced child pornography charges under similar circumstances. Last year, a number of young couples at Greensberg Salem High School in Greensburg, PA were caught "sexting" when a principal confiscated one of the student's cell phones.[171] The students, ranging in ages from 14 to 17, were charged with manufacturing, disseminating and possessing child pornography[172] and could face up to 10 years in prison and have to register as sex offenders for their actions. While society expects the government to protect children and be strict with sexual predators, it seems that the law has not taken in to account the development of technology and the changes in societal expectations.

Second, there is the "*Jack Bauer*"[173] scenario of the suspected terrorist with an app phone. In this hypothetical situation, the government has intelligence reports, which indicate that

---

[170] *See* THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT OF 1998 ("COPPA") (1998).
[171] http://www.msnbc.msn.com/id/28679588.
[172] 18 Pa.C.S. § 6312 (2009).
[173] Protagonist in Fox Series "24" known for foiling terrorists' plots just minutes before their execution.

the terrorist is about to attack and they have been using their iPhone to plan the attack. Access to the terrorist's iPhone data could reveal the terrorist's current location, their communications with other terror cell members and surveillance done of the target. Let's also assume that the government has the resources to access the data remotely from both AT&T's servers and Google's user information.

There are very few American's who would object to the government using all of its resources available to find the terrorist in order to prevent the attack. However, most citizens would take issue with the government monitoring their own iPhone activity as it relates to location, messages and searches. This *NIMBY*[174] dichotomy means that there is great public outcry over systems like CARNIVORE, but at the same time the public has a valid expectation that the government will monitor terrorist activity if they have the ability to do so.

In a post-9/11 world, Americans have seemed to be willing to give up certain rights of privacy for the greater safety of American interests that terrorists have sought to attack. Introduced on October 23, 2001, the USA PATRIOT Act is a controversial piece of legislation that permits the government certain privileges in searching telephone, e-mail, medical, financial and other records.[175] Most significantly, the "sneak and peak" section "allows agents executing search warrants to delay telling the targets that their property has been searched or even seized."[176] Without going into a discussion of the validity of anti-terrorism tools, the Act has undoubtedly created new methods for the government to circumvent citizen's Fourth

---

[174] Acronym for "*Not In My Back Yard*".

[175] *See* THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT OF 2001 ("USA PATRIOT Act") (2001).

[176] Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 74 (2006).

Amendment protections. Even though "9/11 changed everything," it is still unclear a decade later what the long-term implications will be on societal expectations of privacy.

Third, let's assume there is a Ponzi schemer who's guilt can be proven by evidence stored on their app phone. In this "*Bernie Madoff*"[177] scenario, federal prosecutors have unveiled a widespread financial fraud scheme and need access to the data stored on the ring-leader's iPhone, such as their calendar, e-mails, and internal memos amongst other data. Let's further assume that the app phone is in the government's possession but it is encrypted so they cannot access the data without using decryption tools, which would be illegal if used by a member of the general public.

Again, in this situation it is not unthinkable to believe that such a wealth of information could be stored on a single iPhone. In the real-life *Madoff* case it was widely reported that he used a single, antiquated IBM AS/400 computer from the 1980's to produce false records with the help of manipulated financial software.[178] Computer models like the one he used were rated as high as 66 MHz,[179] or roughly 11% of the processing power of the latest iPhone -- so it is not hard to imagine such a scheme being conducted entirely on a modern app phone.

Society not only expects the government to keep track of such financial activities, the Securities and Exchange Commission is charged with monitoring such investors.[180] In 1999, Congress passed the Gramm-Leach-Bliley Act[181] ("GLBA"), which had major privacy requirements for financial institutions in the "collection, disclosure and protection of consumers'

[177] Bernard Madoff was the mastermind behind the largest Ponzi scheme in history and was sentenced to 150 years in prison in 2009.
[178] http://money.cnn.com/2009/04/24/news/newsmakers/madoff.fortune.
[179] http://www-03.ibm.com/ibm/history/exhibits/rochester/rochester_4010.html.
[180] http://www.sec.gov/about/whatwedo.shtml.
[181] *See* THE FINANCIAL SERVICES MODERNIZATION ACT OF 1999 ("GLBA") (1999).

nonpublic personal information."[182] Again, there becomes the question of protecting the public versus respecting the privacy of individual citizens. Society would likely expect the government to search for "red flags,"[183] yet at the same time abstain from monitoring individual account activity without probable cause and a search warrant.

These previous three hypothetical's are a combination of recent headlines with notable legislative actions during the past decade. They are meant to illustrate that there are serious conflicts between what society expects of their government-- not only in terms of protection but also individual privacy. These current issues have not only been appropriate bellwethers for measuring the current expectations of society, they also might represent degradations in what society expects to be private because of technological advances.

B. Changing Technology

"Doing a privacy change for 350 million users is not the kind of thing that a lot of companies would do. But we viewed that as a really important thing, to always keep a beginner's mind and what would we do if we were starting the company now and we decided that these would be the social norms now and we just went for it."[184]

- Mark Zuckerberg, Facebook CEO

Many of the Supreme Court cases discussed above warn that while their holdings may be applicable to the current technologies, the law will have to adapt as new developments are made. There is none more prophetic than the *Dow Chemical* case,[185] which involved the EPA taking aerial photographs of a chemical plant. The majority felt that because the aerial photographs were taken using a widely available consumer technology, that Fourth Amendment rights had not been violated. As quoted above, the majority wrote that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as

[182] http://www.nextlabs.com/html/?q=gramm-leach-bliley-act-glba.
[183] http://www.ftc.gov/redflagsrule.
[184] http://www.theinternetpatrol.com/privacy-we-dont-need-no-stinkin-privacy-says-facebook-ceo-mark-zuckerberg.
[185] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).

satellite technology, might be constitutionally proscribed absent a warrant."[186] In 2010, such highly sophisticated surveillance equipment is generally available to the public, specifically any iPhone user via the Google Maps™ app.[187] Users can enter nearly any address in the United States and get a satellite image of that location that is accurate enough to make out buildings, cars and even pedestrians.

In Justice Burger's own words, such a technology "might be constitutionally proscribed absent a warrant" simply because it is beyond what the human eye could observe without magnification. Justice Burger even notes that the Government's own attorney's conceded that satellite images might raise constitutional problems. While Google Maps is not so detailed as to reveal "identifiable human faces or secret documents" as feared in *Dow Chemical*, it could easily reveal a marijuana farm[188] or even an illegally dumped boat.[189] Recently, a Florida police officer used Google Earth™ to track down the owner of a boat that had been dumped into an undeveloped subdivision near Pensacola.[190]

Satellite imagery is clearly a technology that until recently was not available to the average consumer. Today, it is essentially available for free to anyone that is connected to the internet. In theory, this could mean that since society expects public access to such information it is not unreasonable for the government to use such tools to prosecute suspects without a warrant. However, the Supreme Court has yet to decide any cases related to web-based satellite maps.

There is also a more recent Google technology called "Street View™" that allows users to view 360° images of millions of locations throughout the United States. Available on the

---

[186] *Id.* at 237.
[187] http://www.apple.com/iphone/iphone-3gs/maps-compass.html.
[188] http://www.switched.com/2009/01/30/google-earth-leads-to-marijuana-bust.
[189] http://www.switched.com/2010/03/31/google-earth-used-to-solve-case-of-illegally-dumped-boat.
[190] *Id.*

iPhone, "people can virtually explore and navigate neighbourhoods through panoramic street-level images."[191] Because these images are all taken on public streets using standard cameras, some advocates might argue that the government's use of the service to prosecute criminals would be constitutional under the "Plain View Doctrine." According to Google, the Street View function "contains imagery that is no different from what you might see driving or walking down the street."[192] Yet just as a pedestrian might witness a crime, so do Google's camera's in capturing the panoramas. One website[193] has already documented twenty different types of crimes[194] that have been caught on film by Google's Street View cameras.

While citizens have become increasingly comfortable with public surveillance cameras, Google's cameras are more akin to undercover agents than typical traffic cameras. There is at least one case where individuals sued Google over images captured by their Street View cameras.[195] A federal judge recently dismissed the suit against Google filed by a Pittsburgh couple who had sued under the legal theories of invasion of privacy, negligence, unjust enrichment and trespass.[196] While the case did not involve a governmental search under the Fourth Amendment, it does raise almost the same exact issues first raised by Warren and Brandeis in their article 120 years earlier.

---

[191] http://www.google.com/press/annc/20091007_streetview.html.
[192] http://maps.google.com/help/maps/streetview/privacy.html.
[193] http://www.criminaljusticeschools.com/blog/20-crimes-caught-on-google-street-view.
[194] The twenty crimes are: (1) reckless driving, (2) burglary/theft, (3) vandalism/destruction of property, (4) public intoxication, (5) assault/battery, (6) indecent exposure, (7) brandishing a deadly weapon, (8) illegal parking, (9) prostitution, (10) joyriding, (11) underage smoking, (12) speeding, (13) drug dealing, (14) jaywalking, (15) lewd behavior, (16) failure to obey a street sign, (17) arson, (18) public urination, (19) stalking, and (20) other unspecified offenses.
[195] *See Boring v. Google*, 598 F. Supp. 2d 695 (W.D. Pa. 2009).
[196] http://www.pcworld.com/article/159740/judge_dismisses_google_street_view_case.html.

C. Changing Ideologies

"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place." [197]

- Eric Schmidt, Google CEO

Society's fears of governmental intrusion are not nearly as strong today as they have been in other times in American history. The greatest threat of the 21st century appears to be not that of government intrusion, but rather the power vested in corporations who control user's data. Google owns three of the top ten visited websites in the United States,[198] which combined account for over 9% of the page views world-wide over the past three months.[199] This unbelievable market share has led many to fear Google due to the amount of information the company possesses[200] about each of its 776 million users.[201] Google is not shy about the fact that it uses data it gathers about its users to create profiles that are used for highly profitable behavioral advertising.[202]

While the government obviously has nearly limitless intelligence resources for gathering data about citizens, it is more likely that individuals will voluntarily provide personal information to corporations who then become the gatekeepers of such privileged information. While there are certainly regulations on privacy and consequences for security breaches, Corporate America has been largely left to police itself with privacy policies,[203] compliance programs[204] and multi-national "safe harbor" treaties.[205] While the government has an obligation

---

[197] http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html.
[198] #1 Google.com, #4 Youtube.com & #6 Blogger.com.
[199] http://www.alexa.com/topsites/countries/US.
[200] See Greg Conti, *Googling Security: How Much Does Google Know About You?* (Oct. 20, 2008).
[201] http://news.cnet.com/8301-1023_3-10149534-93.html.
[202] Jacqueline Klosek, *Every Click You Take, They'll Be Watching You: Top Online Behavioral Advertising Privacy Journal*, PRIVACY & DATA SECURITY LAW JOURNAL (May 2009).
[203] For an example of a corporate privacy policy, *see* http://www.levitra.com/privacy.html.
[204] http://www.truste.com/why_TRUSTe_privacy_services/privacy_best_practices.html.
[205] http://www.export.gov/safeharbor/eu/eg_main_018365.asp.

to regulate privacy, there has generally been a *laissez faire* attitude with regard to enforcement. Absent a few noteworthy exceptions, the government has brought only a limited number of enforcement actions[206] against corporations for failure to uphold their own privacy policies.

As it is increasingly corporations who control information, not the government, it might be said that they have the greatest influence on societal expectations of privacy. The concern then becomes what happens when the government begins to cooperate with corporations to yield data for searches of citizens. While Google is not a traditional ISP under the ECPA, it could be assumed that they would show some willingness to cooperate with subpoenas and warrant requests without the knowledge of their users.

Recall that in *New York Telephone*, the Supreme Court held that federal courts had authority over telecommunications providers to "compel, upon request, any assistance necessary to accomplish an electronic interception." This might lead some to conclude that the government could also compel assistance from technology providers such as Google. Notably, Google has recently teamed up with the Electronic Frontier Foundation ("EFF") to help "block a government attempt to access the contents of a Yahoo! e-mail account without a search warrant based on probable cause."[207]

In an *amicus* brief on the issue, Google states that "as an electronic communications service to the public, Google receives legal process from various state and federal agencies, seeking customer information, including content of Gmail."[208] Google's stance has been to provide assistance when a search warrant is provided, but now appears to contest requests that

---

[206] *In the Matter of Geocities*, FTC File No. 9823015, Agreement Containing Consent Order (1999).
[207] http://www.bespacific.com/mt/archives/024025.html.
[208] *In Re Application of the United States of America for an Order Pursuant to 18 U.S.C. § 2703(d)*, *Amici Curiae* Brief (filed Apr. 13, 2010) (available http://www.eff.org/files/filenode/inreusaorder18/AmiciBriefYahooE-mails.pdf).

are made without a proper search warrant under the Fourth Amendment. The brief specifically argues that "the mere fact that a service provider has the ability to access e-mail messages does not defeat the user's expectation of privacy in their contents."[209]

The ideological change that Google's stance represents is that the balance of power has shifted from that of the government being the sole possessor of the latest military surveillance technologies to corporations being the leader in the collection of personal information which the government would like to access. The next logical step is that the struggle will wind up in the Supreme Court and if Congress objects to the ruling they will respond with appropriate legislation that more accurately reflects societal expectations of privacy (as was the case with the infamous "pen register").

Some scholars have argued that this is the appropriate way for our government to handle such issues, as Congress is better suited for creating laws that reflect changing technologies than the judiciary. Orin Kerr believes that "courts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies . . . [w]hen technology is in flux, the Fourth Amendment protections should remain relatively modest until the technology stabilizes."[210]

There is also the issue of generational ideologies and how to define societal expectations of privacy. The average age of justices of the United States Supreme Court is roughly 68 years old,[211] while the median age of an American citizen is only 36 years old.[212] Famously, recently

---

[209] *Id*. at 4-5.
[210] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004).
[211] C.J. Roberts (55), J. Stevens (89), J. Scalia (74), J. Kennedy (73), J. Thomas (61), J. Ginsburg (77), J. Breyer (71), J. Alito (56), J. Sotomayor (55).

retired Justice Souter wrote the majority opinion in *Grokster*,[213] a case involving peer-to-peer file sharing networks, yet did not know how to operate a computer and wrote all of his opinions longhand using a fountain pen.[214] Even Chief Justice John Roberts -- one of the youngest current members of the Supreme Court -- recently asked during oral arguments the difference was "between email and a pager."[215] Not questioning the brilliance of the Justices or their ability to grasp complex technical issues, it raises some questions about how society is able to define it's own expectations of privacy.

More generally there are generational gaps involving the expectation of privacy, especially as it relates to technology. Since the Congress and Federal Judiciary is generally comprised of an older generation, it may not be that the laws accurately reflect the emergences of new technologies. Typically, new technologies are usually adopted by younger generations prior to more widespread adoption. For example, there are over 50 million iPhone users and more than half of them are under the age of 30.[216] This "mobile generation" has differing expectations of what should be kept private from government searches, however the law does not yet reflect these expectations.

V. CONCLUSION

While *Katz* has served as a wonderful guidepost for the Supreme Court to weigh the law against technological advances over the past four decades, it has come time for a realignment of privacy principles that reflect advancements in technology proactively instead of reactively. America entered the "internet age" nearly a decade ago and wireless mobile computing has

---

[212] http://factfinder.census.gov/servlet/ACSSAFFFacts.
[213] *See Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).
[214] http://www.npr.org/templates/story/story.php?storyId=103694193.
[215] http://blogs.wsj.com/law/2010/04/19/our-tech-savvy-supreme-court.
[216] http://rubiconconsulting.com/downloads/whitepapers/Rubicon-iPhone_User_Survey.pdf.

become a ubiquitous part of our cultural fabric. Congress must work to establish new guidelines for creating self-limitations on the power of the government to conduct law enforcement investigations using the tools that are widely available to consumers on the internet or via app phones.

While the text of the Bill of Rights remains unchanged, societal expectations of what should be kept private from government searches have morphed dramatically over the past few years. While it is true that "the Fourth Amendment protects people, not places,"[217] there are fewer and fewer places that people consider private in light of mobile computing. The government should recognize this anomaly and create increased zones of privacy for users of wireless mobile devices as they become more commonplace amongst society.

It is fitting to end this discussion with the words of Warren and Brandeis, who similarly concluded: "the common law has always recognized a man's house as his castle, impregnable, often, even to his own officers engaged in the execution of its command. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?"[218] Hopefully, the Supreme Court will continue to recognize the Fourth Amendment's core commitment to protection of citizens from unwarranted government searches and usher in a new era of digital democracy.

[217] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[218] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).