Technology Revolution and the Fourth Amendment

Final Project for i235 - Cyberlaw

Michael Lissner • 22 May 2009

"Judges should firmly advance arguments that seek to preserve original values of liberty in a new context."

-- Lawrence Lessig[1]

1 Lawrence Lessig, *Code and other laws of cyberspace*, 1999, 222.

Introduction

In 1980, if you had about $80,000, you could purchase a mainframe from IBM that would hold 2.5 gigabytes of data.[2] Today, for about $100, you can purchase a drive that can hold one terabyte.[3] Adjusting for inflation,[4] and disregarding such things as speed and reliability, this is 28,000 times more storage space per dollar per year. It is safe to say that our society is in the midst of what the Center for Democracy and Technology has called the "storage revolution."[5] Not long ago, storing vast quantities of data required vast amounts of resources, but in the aftermath of this revolution, truly incredible amounts of data can be both stored and retrieved cheaply and easily.

This change in the convenience and quantity of storage has completely upended the ways we think about information. No longer must we decide what to keep, and what to throw away; we can now keep all of the data that we would have previously had to make careful decisions about. We can copy it from one device to another, back it up to yet another, and still easily carry all of our information in a purse or briefcase.

---

2 "Computer History Museum - Timeline of Computer History - Storage," *Computer History Museum*, http://www.computerhistory.org/timeline/?category=stor.

3 "1TB hard drive - Google Product Search," http://www.google.com/products?hl=en&hs=b1q&q=1TB%20hard%20drive&um=1&ie=UTF-8&sa=N&tab=wf.

4 $1 in 1980 has the same buying power as $2.59 in 2009. "Inflation Calculator: Bureau of Labor Statistics," *CPI Inflation Calculator*, http://www.bls.gov/data/inflation_calculator.htm.

5 *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology* (Center for Democracy & Technology, February 2006), 6.

In addition, where the storage revolution has not changed the way we think about information, new technologies have changed the ways we think about privacy. We now have satellites and airplanes that can look into our yards,[6] cameras that can see temperature from almost any distance, deception detection devices that can attempt to see our thoughts through our eye sockets,[7] and massive warrantless wiretapping of our conversations with foreigners.[8] Simultaneously, exceptions to the once-firm fourth amendment abound, with the current tally at about nine exceptions,[9] and some judges rallying for still more.[10]

As these changes have occurred, they have stretched and bent the ways that we think about the fourth amendment's promise to prevent unreasonable searches and seizures. Whereas historically, the fourth amendment was designed to keep the government out of our homes, and to provide Americans with a private space that could not be invaded, in the aftermath of these revolutions, such privacy guarantees are becoming more and more rare. What's

---

6 *California v. Ciraolo*, 476 U.S. 207 (U.S. Supreme Court 1986); *Florida v. Riley*, 488 U.S. 445 (Supreme Court of Florida 1989).

7 R. G. Boire, "Searching the brain: the Fourth Amendment implications of brain-based deception detection devices," *The American Journal of Bioethics* 5, no. 2 (2005): 62.

8 Eric Lichtblau, "Senate Approves Bill to Broaden Wiretap Powers," *The New York Times*, July 10, 2008, sec. Washington, http://www.nytimes.com/2008/07/10/washington/10fisa.html.

9 The current list includes: plain view, open fields, border search, grand juries, good faith on a warrant, exigent circumstance, motor vehicle, incident to lawful arrest, and communication with foreign nationals abroad.

10 Richard Posner, "Rethinking the Fourth Amendment," *Sup. Ct. Rev.* (1981): 49.

more, when searches do occur lawfully, the once bright line about where a search begins and where it ends is being challenged by new ways of storing data, and the merging of computing services between different aspects of our lives. Previously, it may have been possible to create a warrant with a particular scope, as is required by the fourth amendment,[11] but with the expansion of digital storage, such carefully scoped warrants are no longer possible.

In this paper, I will attempt to address the ways that these technological advances and changes have affected our constitutional rights. I will do so in three sections. In the first, I will discuss the ways that new technologies, habits and legal interpretations are challenging traditional fourth amendment protections. In the second, I will discuss one of the nine fourth amendment exceptions mentioned above, and will outline the problems that the broad exception has encountered as a result of digital technology. Finally, in the third section, I will conclude with a discussion of some policy changes that could be used to address the problems identified throughout.

11 *The Constitution of the United States, Amendment 4* states that warrants must, "particularly describ[e] the place to be searched, and the persons or things to be seized."

The Weights on the Fourth Amendment's Shoulders

As technology marches on, there are a number of new issues that are making interpretation of the fourth amendment more and more challenging. One such area is with regards to technology that gives greater sensory capability to government officials. An iconic example of this issue is the 2001 Supreme Court case, Kyllo v. United States.[12] In this case, the FBI believed that Kyllo was using heat lamps to grow marijuana in his garage, and used infrared imaging to determine that the exterior of his garage walls were unnaturally warm. Using this information, they were granted a warrant to search the house, ultimately resulting inn Kyllo's arrest. Although they were granted a warrant, and never entered Kyllo's house, when the Supreme Court heard the case, it decided that the evidence was inadmissible because the technology used invaded Kyllo's sense of privacy.

The reasoning in this case is unique, and has been cited widely as a turning point in fourth amendment interpretation. Prior to this case, with the exception of a couple of wiretapping cases, the Supreme Court had not ruled on many cases where the invasion of the property had been done by technological means. In this case however, the government used an infrared imaging device to determine the outside temperature of Kyllo's walls. The

12 *Kyllo v. United States*, 533 U.S. 27 (U.S. Supreme Court 2001).

government made two arguments to legitimize its use of the device. First, it argued that the devices merely enhanced their ability to obtain information that they could have obtained in other ways, such as by noting the lesser quantity of snow near or on the garage. Second, it argued that there had been no invasion of Kyllo's privacy, since the information obtained by the imaging device was at the surface of the outside walls of the house, not inside them.

Justice Scalia however, in writing the opinion of the court, saw the issues differently. He believed that, "any information regarding the home's interior 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."[13]

This decision created waves in fourth amendment interpretation because it created a new exception to its application. Some scholars have called this the "popularity exception,"[14] since, according to the quote above, once a technology is in general public use, it can then be legitimately used for government searches and seizures.

This is problematic for a number of reasons, not least of which is the new power given to marketers, governments and companies with new products.

13 Ibid., vol. 533, sec. (b), quotation in original, original citation omitted.
14 Boire, "Searching the brain," 63.

The argument now goes that if a company that has a product that can be used in searches and seizures can popularize their product, they can thus create a new fourth amendment exception. What may be worse is that if a government should decide to popularize a product or technology, they too can go around the law. In addition, these scenarios are not limited to only American companies or governments – regardless of origin, according to the quote above, if a technology becomes popular, it can be used as a fourth amendment exception. It should go without saying that this is an unprecedented and dangerous power for any organization to have, public or private.

On a larger scale, the outcome of Kyllo is also problematic because of the way that technological innovation will thus slowly erode constitutional guarantees. Although Scalia likely intended this finding to future-proof the Court's stance on new technology, until this finding is overturned or a new precedent is created, each innovation that becomes generally popular will result in further erosion of the fourth amendment.

Turning again to the infrared imaging from Kyllo makes a poignant example. In 2005 when the Supreme Court heard the case, such imaging was not popular, but since that time sites that allow the sharing of photographs have proven that infrared imaging is perhaps not as uncommon as it may

seem,[15] with the result being that in the next few years such photography could become a legitimate way to search without a warrant. Couple this to the fact that weather satellites of increasing resolution commonly use infrared imaging, and a more daunting picture begins to emerge. This scenario is not only true for infrared imaging, but also for any other technology that can be used to obtain information about the private information of a home. Without tilting at windmills too much, another example that may need to be resolved in the near future could be the use of X-ray imaging, which is already used quite commonly, and can be used in a manner similar to a camera.[16]

These are of course but two ways that current case law and advances in technology are together eroding our fourth amendment rights. Other ways occur as a result of not only technological advancement, but as a result also of changes in habit. An example of such a change that is currently bubbling to the surface of American awareness is the increasing tendency to store private information with third party service providers on the Internet. Despite the fact that there are a number of prominent cases that have determined that by and

15 See "Flickr: "infrared"," http://www.flickr.com/photos/tags/infrared/, indicating that at present there are over 100,000 pictures tagged as infrared.

16 Two examples of its use in large-scale outdoor scenarios come to mind. The first, is its present use to scan cars at the Mexican border. (Jeanne Meserve, "High-tech portals to aid border screenings - CNN.com," *CNN.com*, October 16, 2008, sec. Technology, http://www.cnn.com/2008/TECH/10/16/border.portal/index.html?eref=rss_tech.) The second is the inspiring work of artist Nick Veasay who does x-ray photography of everything from flowers to jetliners (Nick Veasay, "NICK VEASEY | X-RAY PHOTOGRAPHER | X-RAY PHOTOS / PHOTOGRAPHY / FILM / ABSTRACT / ART," *Nick Veasay X-Ray*, http://www.nickveasey.com/.)

large we are not entitled to fourth amendment protection when our data is shared with third parties,[17] the convenience of doing so is moving more data in that direction. As this occurs, more information is inevitably going to be available to government search and seizure.

The two cases that are most often cited when discussing the sharing of private data with third parties are Smith v. Maryland[18] and U.S. v. Miller,[19] both of which hinge on the somewhat circular Katz doctrine, which says that the fourth amendment only provides protection to information when there is a "reasonable expectation of privacy."[20] (Put another way, this doctrine dictates that information is private when people think it's private.) To interpret this, we turn to the example provided by Smith v. Maryland, in which the Supreme Court found that because Smith had been sharing the phone numbers he dialed with the phone company, and that because those numbers appeared on his bill, it should have been clear to him that those numbers were being tracked and logged. As a result, it should have therefore been clear to him that since the phone company had those numbers, the information may not have been kept private, and he should not have a reasonable expectation of privacy with regards to those numbers. In the second example, United States v. Miller

17 *United States v. Miller*, 307 U.S. 174 (U.S. Supreme Court 1939); *Smith v. Maryland*, 442 U.S. 735 (U.S. Supreme Court 1979).

18 *Smith v. Maryland*, vol. 442, .

19 *United States v. Miller*, vol. 307, .

20 Harlan, *Katz v. United States (Concurring Opinion)*, 389 U.S. 347 (U.S. Supreme Court 1967).

applied a similar logic to expand this doctrine to records held by banks, and even went so far as to state, "a person has *no* legitimate expectation of privacy in information he voluntarily turns over to third parties."[21]

This case history notwithstanding, the Supreme Court has not yet heard any case on how this doctrine applies to cyberspace. As the Internet currently operates, much of the data that is used by third party Internet service providers (ISPs) is never seen by human eyes, creating a feeling of privacy and security that might lead people to believe they have fourth amendment rights. Unfortunately though, by applying the four prong test laid out in Katz, a different picture begins to emerge. According to the test, an individual has objective expectation of privacy only if:

(1) the information was not disclosed to others to a significant extent;
(2) the third party organization did not have a legitimate business interest in the data;
(3) the third party organization was not the intended recipient of the information; and
(4) the third party did not have a legitimate business reason to memorialize or store the information.

In analyzing each of these points, it appears that most data stored on the Internet does not receive fourth amendment protection. The first point of this test aims to determine the number of people that know the fact, and to thereby determine if it is considered private information. In many cases, the Internet

21 *Smith v. Maryland*, 442:743, emphasis added.

facilitates broadcasting information in ways that were not previously possible to most people, and in such cases, courts have already hinted that the fourth amendment does not generally apply.[22] However, in the case that the ISP is not being used for communication of a message to more than a few people, this first prong of the test might be completed without a loss of constitutional rights. In those instances where that is the case, we must then turn our attention to the next three prongs.

With regards to the second point, fourth amendment protections appear vastly weaker, as nearly all information that is shared with a third party ISPs is likely to be of a business interest to them, but in the case where an ISP freely admits that the information is not of business interest to them, expectations of privacy may still in theory objectively exist.

In contrast to the first two prongs, the third does give some hope to users of third party Internet services, since in most cases, the ISP is not the intended recipient of the information. As is explained by Matthew Hodge,[23] it is unlikely that many users create online accounts in order to share their personal information with the site administrators. He does point out though

22 For example, in United States v. Maxwell (45 M.J. 406 (C.A.A.F. 1996)), it was hinted that the fourth amendment might not apply in chat rooms, or even to emails sent to more than a few people.

23 M. J. Hodge, "Fourth Amendment and Privacy Issues on the New Internet: Facebook. com and Myspace. com, The," *S. Ill. ULJ* 31 (2006): 116.

that in some cases this is not true, such as when information is shared with an online banking provider.

For the final prong of the test, again a bleak picture is painted, for in most cases, ISPs do have a legitimate business interest in storing (memorializing) private information provided by the user. As is indicated by the 30 day rule for stored email that is in the Electronic Communications Privacy Act (ECPA),[24] users previously stored information such as email on their own personal computers, and used ISPs simply as temporary storage and communications providers, however such practices are becoming less common, and more and more communication and information is being stored, as a legitimate business practice, by ISPs.

Taken together, the four prongs of the Katz test do not paint a rosy picture for users of online services, since only one of the above exceptions must be true in order for fourth amendment rights to privacy to be forfeited. If information is intended for the ISP, stored by the ISP, sent to others, or if the ISP claims a business interest in the information, fourth amendment rights to privacy will be waived. Simultaneously, for information that is not stored on the Internet, new technologies and the "popularity exception" are allowing new ways for searches to occur. This combination of fourth amendment

24 *Electronic Communications Privacy Act*, *United States Code*, 1986.

exceptions leaves few options the average American, but there is yet one more place where fourth amendment protections are under even more pressure: The American border.

The "Constitution Free Zone"[25]

Another area of the law that is being tried by this time of technological advancement are the generally accepted exceptions to the Fourth Amendment. A prominent example of this is the border search exception, which allows federal agents to search our person and possessions if we at an international border – without probable cause or a warrant. Under this exception, such searches "may occur when entry is made by land from the neighboring countries of Mexico or Canada, at the place where a ship docks in the U.S. after having been to a foreign port, and at any airport in the country where international flights first land."[26] Additionally, so-called "extended border searches" may be made within an extended distance from such borders under certain circumstances.

Generally speaking, this exception creates a broad exception to fourth amendment that allows border patrol officers to complete highly invasive

25 "American Civil Liberties Union : Fact Sheet on U.S. "Constitution Free Zone"," *Fact Sheet on U.S. "Constutition Free Zone"*, http://www.aclu.org/privacy/37293res20081022.html.

26 Stephen Vina, *Protecting our Perimeter: "Border Searches" under the Fourth Amendment* (Congressional Research Service, May 17, 2005), 6.

searches with very little judicial oversight. In some cases, for example, they can even use x-ray, complete body canal searches, or even detain individuals for prolonged periods of time.[27]

In upholding this longstanding exception, the Supreme Court has said that "searches made at the border...are reasonable simply by virtue of the fact that they occur at the border,"[28] and has upheld that such searches fall into two types of searches and seizures: routine and non-routine. Routine searches include those searches that many Americans may experience when traveling through customs after visiting a foreign country, but can be escalated to such actions as the cutting of a spare tire, x-ray of a person's possessions, use of a sniffing dog, and the removal of outer garments such as shoes or jackets. Non-routine searches escalate still further from this point, and can include all of the things above, but can also include such things as the dismantling of an automobile, bodily x-ray examinations, and the destruction of inanimate goods.[29]

This exception creates two major problems as it applies to technology, with the first problem similar to those mentioned above. As a result of new technology's increasingly powerful abilities to sense and search, border

27 Ibid., 11.
28 United States v. Ramsey 431 U.S. 606.
29 Vina, *Protecting our Perimeter: "Border Searches" under the Fourth Amendment*, 10-11.

searches can at once be increasingly automated, efficient and invasive. Examples of this problem abound, such as GE's "walk-through portal"[30] that can sniff narcotics or explosives right off your body or clothes, and the "whole-body imaging" tools that are now appearing at airports.[31]

The second, and perhaps larger problem that this exception raises is how such searches are applied to the digital goods such as laptops and mobile phones that travelers often carry with them. Recently, a case was brought forward in the 9th Circuit in which a border search of a man's laptop found what was believed to be child pornography.[32] In the case, the defendant attempted to analogize a laptop to a home and to the human mind, but these claims were dismissed as without merit, with the court ultimately finding that the search of his laptop was admissible. In the opinion of the court they were "satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border."

Like the findings in Kyllo, above, this conclusion has created waves in the popular press and amongst policy organizations. Privacy advocates,[33]

30 "GE Security Products - EntryScan EntryScan Series," http://www.gesecurity.com/portal/site/GESecurity/menuitem.f76d98ccce4cabed5efa421766030730?selectedID=5518&seriesyn=true&seriesID=.

31 Jessica Ravitz, "Airport security bares all, or does it?," *CNN.com*, May 18, 2009, sec. Travel.

32 *United States v. Arnold*, 2008 9th Cir. (9th Cir.).

33 "Schneier on Security: Crossing Borders with Laptops and PDAs," http://www.schneier.com/blog/archives/2008/05/crossing_border.html.

travelers' organizations,[34] and technology policy groups[35] have all come out against this decision, and have argued for a more reasonable approach to searches at the border. Some of these organizations have even gone so far as to make recommendations to travelers, advising them as to how to travel through an international border without running the risk of having their digital information searched.[36]

This finding creates a number of problems, including a complete lack of purpose in such a search. In the words of the Congressional Research Service, the goal of border searches is for a "sovereign nation to protect itself from terrorist activities, illegal immigrants, and contraband,"[37] but there is no evidence that the prevention of information from entering at a border accomplishes any of these tasks. Furthermore, although it is possible that the NSA is working in collaboration with Internet Service Providers to tap and listen into Internet traffic that is passing into and out of the country,[38] there is nothing, short of disconnecting the Internet, that can be done to stop the flow of information into or out of the country. By using simple encryption

34 See generally: "Laptop and Electronic Device Seizures | ACTE," http://www.acte.org/content/laptop_seizures/seizures.

35 "US v. Arnold | Electronic Frontier Foundation," http://www.eff.org/cases/us-v-arnold.

36 Jennifer Granick, "Protecting Yourself From Suspicionless Searches While Traveling | Electronic Frontier Foundation," May 1, 2008, http://www.eff.org/deeplinks/2008/05/protecting-yourself-suspicionless-searches-while-t; "Schneier on Security: Crossing Borders with Laptops and PDAs."

37 Vina, *Protecting our Perimeter: "Border Searches" under the Fourth Amendment*, 1.

38 U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, January 16, 2006.

techniques, contraband information can be protected from government eavesdropping, and can easily enter the country via the Internet. In response to the criticisms raised about this policy, Homeland Security Secretary Michael Chertoff has been quoted saying, "the most dangerous contraband is often contained in laptop computers or other electronic devices,"[39] however in the aftermath of the publicity around this subject, it is likely that such contraband will be very uncommon on laptops traveling to and from the country, and that the net affect of this fourth amendment violation will be negligible.

But this is not where the problems with this policy end. Additionally, this policy creates a frustrating problem for anybody that might have confidential information on their digital device, which privacy advocates argue includes just about everybody, including anybody that works in a field that has trade secrets, anybody that works with confidential records (such as health workers and lawyers), and anybody who uses their computer for online banking, or has passwords stored in their browser. In the end, it is safe to say that nearly every computer that is used in nearly any way has private information on it, and any person that is traveling with such a computer has a

39 Ellen Nakashima, "Travelers' Laptops May Be Detained At Border," *The Washington Post*, August 1, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080103030.html.

stake in keeping that information private. Again though, officials miss this point, stating that such searches "do not infringe on Americans' privacy."[40]

Assuming that we have perfect trust in our security workers at our nation's borders, and that we had absolutely nothing we wanted to keep secret from all people, this would not be a problem in any way. Unfortunately though, in response to the complaints about this issue, in addition to the quotes above, the Department of Homeland Security has stated that, "officials may share copies of the laptop's contents with other agencies and private entities for language translation, data decryption or other reasons."[41] Thus not only must international travelers trust the federal security workers, they must also trust undisclosed "private entities" and "other agencies" that may be used for a couple of specific tasks, but also for unknown "other reasons."

In response to this case, and the Department of Homeland Security's botched response to it, The Travelers Privacy Protection Act of 2008 was proposed by Senator Russ Fiengold. This legislation was designed to give privacy protections back to travelers, and to create new fourth amendment protections, but due to the changing of congress at the end of 2008, it did not get passed, and has not, as of now, been reintroduced. At present, it has been

40 Ibid.
41 Ibid.

referred to the Congressional Committee on Homeland Security and Governmental Affairs, where it appears to have all but died.[42]

Conclusions

In the above discussion, I have identified a number of areas where the mettle of traditional fourth amendment policy is being tested. In combination with new legal interpretations, new surveillance and searching techniques, and changes in storage and habits, information that was once private is now within the reach of warrantless government searches.

There are a number of solutions to these problems, each of which will make a significant difference in the privacy that Americans are granted. None of these solutions however will be easy. The first and perhaps least controversial step to take is for Congress to pass, and for the President to sign The Traveler's Privacy Protection Act. This is an example of legislation that has already been written, already proposed to the House and Senate, and which would help all Americans when they travel. Further, since the case that initiated this debate was only recently decided, it is important to strike while the knife is still hot, before warrantless searches of digital media become commonplace at our international borders.

42 This status was determined through original research by the author.

This, in turn, brings us to the next step that must be taken: The "popularity exception" created by Kyllo must be repealed, amended, or otherwise remanded from the record. This is a policy that will enable the slow erosion of a centuries-old privacy protection. Such erosion should not be allowed, much less initiated by the Supreme Court.

Third, a new policy must be written to protect information that we share with third party Internet providers. This is essential to enable the continued growth of the Internet, and to enable Americans to confidently use new services as they are developed, without having to worry that such use will diminish their constitutional guarantees. This step is third to those above because it will likely be the most controversial as well as the most challenging to implement. Numerous questions will need to be answered before such a piece of legislation could be enacted, but it is vital that these questions be raised.

The fourth and final step that must be taken is a call to arms for the American people. Quotes like those above from Secretary Michael Chertoff show a blatant disregard for privacy which must be remedied by those people it most affects. Travelers to foreign countries should take additional steps to secure their computers against governmental inspection,[43] and should rally

43 See *supra* at 36 for starting points.

their congressional representatives to pass the Traveler's Privacy Protection Act so that future warrantless invasions of privacy cannot be daily completed at our international borders.