Technology and the Fourth Amendment:

Balancing Law Enforcement with Individual Privacy

Eleanor Birrell

Introduction:

The constitution of the United States was constructed to safeguard the rights of American citizens. One of the rights that people could expect, as stated by the Fourth Amendment, was the right "to be secure in their persons, houses, papers, and effects against unreasonable search and seizure."[1] While the Fourth Amendment took a step towards guaranteeing privacy, its protection is limited by the interpretation of the phrase "unreasonable search." Unfortunately, this phrase was never well defined, and its definition has become increasingly blurred by the technological advances of the last century.

With the aid of new technologies, privacy protection has been eroded in favor of law enforcement. This shift has undermined one of the rights that American citizens have depended upon for hundreds of years; the right to privacy against unreasonable searches. So how has this happened? And what, if anything, might be done to restore the fundamental protection once offered by the Fourth Amendment?

Tardy Regulation:

One of the reasons for the imbalance between privacy and law enforcement is the lengthy gap between the availability of a new technology and the passage of regulations (either legal or judicial) governing its use. Without any legal or judicial restrictions, law enforcement agencies are free to take advantage of new technologies for years, potentially violating the privacy of American citizens.

[1] "The Constitution of the United States of America"

One of the more famous examples of such exploitation of new technology is law enforcement's use of wiretapping. The practice of wiretapping began as soon as telephones were introduced in the 1870s. Wiretapping "without authority" was prohibited during World War I as a defense measure, and many states outlawed wiretapping by the 1920s[2]. However, at the same time that private wiretapping was being restricted, the technology was increasingly employed by law enforcement agencies to collect evidence against prohibition violators. When one such defendant appealed this use of federal wiretaps, the Supreme Court ruled that wiretapping was not a "search" in the sense of the Fourth Amendment and therefore did not require a warrant.[3]

The first restriction placed on law enforcement's power to wiretap telephone conversations did not appear until 1934, when Congress passed the Communications Act, more than fifty years after wiretaps had first been employed. However, although this regulation was reinforced when the Supreme Court ruled that the Communications Act applied to law enforcement agencies as well as private citizens,[4] the restriction was widely ignored, and law enforcement agencies continued to employ unwarranted wiretaps for the next thirty years.[5]

In 1967, the Supreme Court ruled in *Katz v. United States* that wiretapping was a search in the sense of the Fourth Amendment and that law enforcement agencies needed to obtain a warrant before they could tap a phone line. After ninety years, a significant restriction was finally placed on law enforcement agencies' ability to wiretap private conversations.

---

[2] "Listening in the Dark"
[3] *Olmstead v. United States (1928)*
[4] *Nardone v. United States (1938)*
[5] "New Technologies and the Constitution" (OTA)

In this case, both Congress and the Federal court system were slow to protect citizens against the privacy-infringement enabled by the new technology. As a result, power was shifted in favor of law enforcement.

Although wiretapping is probably the most famous example of the failure of Fourth Amendment protections to keep up with new technology, it is far from the only such example. Many other technologies have been employed without restriction for years including electronic bugs, pen registers, and thermal scans.

COINTELPRO, an FBI counterintelligence agency that targeted communist party members, civil rights advocates, and anti-war protesters (among others) has become famous for what are now considered blatant violations against the Fourth Amendment rights of American citizens. COINTELPRO, which conducted more than 2000 operations between 1956 and 1971, made use of unwarranted electronic bugs to observe citizens, many of whom were not suspected of any specific crime.[6] Because they did not charge these subjects, this practice of unwarranted electronic surveillance was not brought to public attention. One now notorious example of COINTELPRO's programs was its observation of Martin Luther King, Jr. His house and hotel room were bugged by the FBI on no less than sixteen different occasions.[7] COINTELPRO's activities were not addressed or restricted until after Frank Church made a comprehensive report to the Senate in 1976; this report partially inspired the Electronic Communications Act of 1986.[8] However, this law, which expanded pre-existing protections to include modern technologies, only came after thirty years of privacy violations by the FBI. In the

[6] "COINTELPRO"
[7] Ibid.
[8] "Privacy and Government"

intervening years, electronic bugs had allowed law enforcement to infringe upon personal privacy.

Another example of the failure of regulations to keep up with evolving technologies is the case of pen registers and trap and trace devices. Pen registers allow law enforcement agents to record the phone numbers of all outgoing calls from a particular phone line; trap and trace devices record all incoming numbers. Both of these technologies were widely available by 1960, however, the Supreme Court did not rule on their use until *Smith v. Maryland (1979).* Although the Court ultimately decided that such devices only required a court order rather than a warrant, the fact that the issue was not addressed for twenty years is a further indication of the failure of the judicial system to respond to new technologies in a timely manner. In this case, Congress was even slower to deal with the issue; no legal restrictions on the use of pen registers or trap and trace devices existed prior to the Electronic Communications Act of 1986. Once again, new technologies had outstripped both legal and judicial regulation, allowing law enforcement agencies to profit from potentially invasive searches for years.

A more recent example of this phenomenon is thermal scanning. Since the late 1980s, police agents have employed thermal scanning as a means of gathering evidence with which to obtain a warrant. Thermal scans are particularly effective in detecting drug growing operations, because marijuana can be grown indoors with the aide of high-intensity lamps. The issue was first addressed in 1994 and 1995, when several Circuit courts ruled on the use of thermal scans; the 7th, 8th, and 11th Circuits all ruled that thermal scans did not represent an illegal search in the sense of the Fourth Amendment. It was not until 2001, ten years after the new technology was first employed by law

enforcement agencies, that the Supreme Court decided that thermal scans are a search under the Fourth Amendment and therefore require a warrant.[9] Once again, a new technology enabled law enforcement agencies to infringe on the fourth amendment rights of American citizens.

There are several reasons for the delay in responding to a new technology. In the case of the judicial system, the only source of final decisions is the Supreme Court (and even these decisions can be reversed by a later decision). In order for the Court to decide on a new technology, the police must first take advantage of the new technology. Then the case must go to trial (instead of ending with a plea bargain). If the evidence is admitted to the trial court and the defendant is acquitted anyway, the case will stay at the trial court level. Otherwise, if the defendant chooses to appeal on the grounds that the new technology constituted an illegal search, then there is a chance of the case rising up through the appeals circuits to the Supreme Court, and then, if the Court chooses to hear the case, the technology will be addressed. Not only does this long process ensure that most cases never reach the Supreme Court, thereby extending the interim period between the introduction of a new technology and a judicial decision, but each individual case takes a long time to move through the system. In the case of *Kyllo v. United States* (in which the Supreme Court ruled on thermal scanning), the police agents used a thermal scanner to look at Kyllo's home in 1992, but the case was not decided by the Supreme Court until 2001. This lengthy judicial process necessarily causes large gaps between the advent of a new technology and the implementation of any judicial restrictions governing its use.

[9] *Kyllo v. United States (2001)*

In the case of the federal legislature, one of the problems is that there are so many new technologies that it can be difficult to predict which ones will be used to encroach on Fourth Amendment rights until after it has happened. Another issue is that although Congress is capable of acting very quickly on occasion (for example, the Patriot Act of 2001 was passed within a month of the September 11 attacks on the World Trade Center), such haste is unusual. Instead of proposing legislation that could be interpreted as impeding justice or protecting criminals, politicians prefer to wait until a technology has clearly infringed upon privacy rights before enacting regulations.

Because of the institutional and political restrictions imposed on the judicial and legislative branches, the federal government is slow to enact regulations on the use of new technologies by law enforcement agencies. Accordingly, the availability of increasing numbers of new technologies has shifted the balance of power towards law enforcement agencies and away from individual privacy.

A Downward Spiral:

The other reason that Fourth Amendment privacy is being undermined lies in the current judicial definition of an "unreasonable search." To this day, Fourth Amendment privacy decisions are guided by the two-pronged test outlined in Justice Harlan's concurrence to *Katz v. United States (1967).* Under this test, the Court first considers whether an individual demonstrated an expectation of privacy and then decides whether this expectation (if it is demonstrated) is reasonable. However, developing technologies have turned this test into a downward spiral.

The first problem with this test (especially in light of the time lapse between the introduction of a new technology and the implementation of regulations governing its

use) is that it fails to allow for the fact that societal expectations change with time. As soon as a privacy-invasive technology becomes pervasive, it is no longer reasonable for an individual to expect the technology not to be employed, therefore there ceases to be any privacy protection against that technology.

The second problem with the *Katz* test is that the Supreme Court has a tendency to rely on precedent when determining whether or not new technologies should be governed by the Fourth Amendment. This sometimes causes privacy invasion when new, more powerful technologies are considered analogous to prior technologies.

New technologies have been compared to old since *Lee v. United States (1952)* declared that a bugged informer was analogous to eavesdropping, and therefore did not require a warrant. In recent years, this legal theory has been expanded to justify Carnivore, aerial photography, and DNA analysis (all without warrants).

Carnivore is a packet sniffer employed by the FBI to intercept email sent by a suspect. It can be configured either to record only the address information, or to record the subject line and email content. The FBI claims that, because Carnivore is only used to intercept address information, it is analogous to pen register and trap and trace devices. This interpretation was supported by Congress in the Patriot Act of 2001, which extended the definition of these devices to include programs like Carnivore.[10] However, many privacy groups have raised concerns that Carnivore is too powerful to be compared to traditional pen registers.[11] One of the objections is that the envelope information on an email (particularly email addresses) is not analogous to the envelope information for a telephone conversation (the phone number). While most telephone numbers say little

[10] Internet Surveillance Law After the USA Patriot Act
[11] Carnivore and the Fourth Amendment (EFF)

about the person with whom a conversation is being held, email addresses can say a lot more about the person; many email addresses include a person's name, and many people use email addresses that contain the name of their school or employer. In this case, one might expect the precedent established in *United States Telecommunications Association v. FCC (2000)* – that the Fourth Amendment protects digits that convey context – to become relevant. However, current law makes no such provision, so email addresses that convey "context" (name or affiliation) remain unprotected.

The analogy between Carnivore and pen registers has a second flaw: The structure of the internet necessitates that the distinction between transactional and substantive data, which is clear when dealing with telephone conversations, becomes blurred by the internet. As such, Carnivore necessarily picks up both envelope information and content in any search, although it can be configured to only record transactional information. Privacy groups have claimed that Carnivore therefore constitutes a search in the sense of the Fourth Amendment even if it is configured to only deliver envelope information.[12] This raises the question of whether an automated search can still be invasive, a question that has not been considered by the Supreme Court.

Moreover, the analogy between pen registers and Carnivore calls into question the logic employed in the original pen register case, *Smith v. Maryland.* In that decision, the Supreme Court justified the use of pen registers without a warrant on the grounds that citizens do not have a reasonable expectation of privacy (having asked a third party, the telephone company, to connect them to the phone number they dialed). However, individuals have a much higher expectation of privacy within their home,[13] and many do

[12] Ibid.
[13] *Kyllo v. United States(2001)*

not consider sending an email to be handing that information to a third party. Is that expectation of privacy reasonable? Perhaps not, but it is another question that deserves to be more fully considered rather than ignored by the U.S. Congress. Despite the unanswered legal questions, the analogy between pen registers and Carnivore clearly seems to expand the definition of a reasonable search by including the additional powers of Carnivore in that category.

Another analogy employed by recent courts is that between trash and abandoned DNA. In *California v. Greenwood (1988),* the Court ruled that the defendants had no expectation of privacy in the trash bags they had left on the roadside. Under this precedent, judicial logic has held that anything that is "abandoned" can be searched without a warrant. Police have recently claimed that this logic covers abandoned DNA; if you leave your DNA sample behind, you cannot expect it to remain private. This argument has sparked protests from privacy advocates who argue that DNA is fundamentally different from trash. While it is possible to burn trash instead of "abandoning" it on the curb, it is impossible to avoid leaving behind DNA evidence. Allowing police to analyze this abandoned DNA without a search warrant allows them to obtain large amounts of personal information about a suspect without the reasonable expectation of guilt necessary for obtaining a warrant, and thereby bypasses traditional investigation procedures. Moreover, DNA contains much more personal information that a trash bag, making the analogy even less plausible. However, although the Supreme Court has not ruled on the case of abandoned DNA, State courts have consistently ruled that abandoned DNA is analogous to abandoned trash and therefore not subject to the

protection of the Fourth Amendment.[14] This analogy has greatly expanded the amount of personal information that the police can gather without a warrant, thereby further infringing upon personal privacy with the aid of new technology and the *Katz* test.

A third example of applying the precedent of "analogous" situations to new technology has been used to justify the use of aerial photography. In *Dow Chemical Co. v. United States (1986),* the Supreme Court ruled that the police did not need a warrant to take aerial photographs of the Dow Chemical Co. complex because the helicopter was in public airspace and the zoom lens only augmented human vision; these arguments, according to the Court, implied that the police had not infringed on any reasonable expectation of privacy. Under this interpretation, taking aerial photographs with a zoom lens is analogous to standing outside the complex and looking in, and is therefore not a search in the context of the Fourth Amendment.

In each of these situations, a new technology is considered analogous to an older, less powerful technology and is therefore subject to the same level of regulation. This policy is unsettling. As new technologies grow increasingly powerful, this "decision by analogy" seems to imply that a "reasonable expectation of privacy" will diminish. Before Carnivore, the affiliations of a suspect's correspondents were protected unless a warrant for a wiretap was obtained, but now a court order will suffice. That information no longer has a reasonable expectation of privacy. Before DNA testing, people could expect their genetic and health information to be private, but the advent of a new technology, combined with the analogy to abandoned trash, has made it unreasonable for an individual to expect their genetic information to remain private. Before helicopters and cameras, constructing a fence around your property and posting "keep out" signs was

[14] *State v. Wickline (Neb. 1989)* and *State v. Buckman (Neb. 2000)*

sufficient to expect the contents of your back yard (or chemical complex) to remain private, but the new technologies have made that expectation unreasonable.

The policy of comparing new technologies to older, less powerful technologies further emphasizes the problem with current constitutional privacy protection: it allows privacy to be eroded by advances in technology.

Beyond *Katz*:

Through both tardy regulations and the use of the *Katz* test, technological advances have been eroding the privacy protections once guaranteed by the Fourth Amendment. So how can we stop this downward spiral and restore a balance between the interests of individual citizens and those of law enforcement agencies?

The example of thermal scanning technology offers a solution to the second half of this problem. The early cases considering thermal scanning likened the new technology to abandoned trash.[15] The rationale was that thermal radiation was allowed to leak out of a private residence into public space, where it could be observed by anyone who happened to be standing there with a thermal scanner. In this sense, the heat waves, like the trash in *Greenwood*, had been abandoned out in public. The fact that the defendants had taken no steps to prevent their heat waves escaping was used to show that they clearly did not expect their heat waves to remain private, and therefore they could not object when those waves were observed by police officers. However, the Supreme Court chose to abandon this logic (and the *Katz* test that motivated it) and instead created a special domain apart from the *Katz* test: the private home. Justice Scalia, writing for

[15] *United States v. Pinson – 8th circuit (1994), United States v. Ford – 11th circuit (1995), United States v. Myers – 7th circuit (1995)*

the majority, declared that "In the case of the search of the interior of homes… there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that exists and is acknowledged to be reasonable. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[16] By distinguishing the private home from a more general location and asserting the existence of a minimal reasonable expectation of privacy, the *Kyllo* decision managed to break out of the privacy-erasing circular logic of the *Katz* test.

This offers one possible solution to the current problem of defending privacy against increasingly powerful search technologies. The *Kyllo* decision, by upholding the *Katz* test in general while simultaneously creating a zone of special protection within the private home, opened the possibility of establishing a "minimum expectation of privacy" not only within the home, but also in a more general context. Describing this minimum level of privacy explicitly would be a challenging task; privacy is a very abstract concept, so defining a minimum level of privacy (especially one that would be impervious to new, unpredicted technologies) would be hard. However, the Supreme Court has proven to be capable of adapting general rules to individual situations, so perhaps the declaration that there exists a minimum level of privacy which all people can expect, regardless of technological developments, would suffice to guide Fourth Amendment interpretations along a new, more protective path.

It would, alternatively, be possible to leave the definition of the minimum level of privacy to the legislative branch. However, this seems less likely to be successful in the long term. Congress has repeatedly shown that it is reluctant to address privacy concerns

[16] *Kyllo v. United States (2001)*

until prompted by a particular event. Moreover, legislature is more easily changed as control of Congress shifts, whereas the Supreme Court, as it made clear in 1992,[17] is bound (except in extreme cases) to abide by its own precedents.

However, the establishment of a minimum standard of privacy would not, on its own, be sufficient to protect privacy against the encroachment of new technologies; it still leaves the issue of the time lag between the introduction and the regulation of new technologies. Court precedents have consistently decreased the penalties for conducting illegal searches. In *United States v. Karo (1984),* the Supreme Court decided that evidence gathered with an illegal search can be suppressed only if there were no legal way to gather that evidence. In *Doe v. Chao (2004),* it decided that monetary compensation for privacy invasions could only be claimed upon proof of damages. Together, these two decisions effectively undermined any incentive for law enforcement agencies to avoid potentially invasive technologies. Instead, these rulings encourage these agencies to take advantage of all new technologies until or unless their use is regulated, either by the Supreme Court or by Congress. As previous technologies have demonstrated, this policy allows law enforcement to employ privacy invasive technologies for ten to thirty years before any restrictions are imposed.

Therefore, in order to establish a reasonable level of privacy protection, it would also be necessary to establish an appropriate disincentive. One way to do this would be to reverse one or both of *Karo* and *Doe v. Chao.* However, the Supreme Court would be unwilling to reverse its precedents without any constitutional motivation. Instead, the disincentive can take the form of a law codifying the decisions of the Supreme Court and inflicting an appropriate (monetary) punishment that would be imposed on any law

[17] *Planned Parenthood v. Casey (1992)*

enforcement agency found to have employed privacy-invasive technologies. Such a punishment would create an economic incentive for law enforcement agencies to avoid investing in new technologies that might later be ruled privacy-invasive.

Although this might initially seem like an unfair burden to impose up law enforcement agencies, it is actually quite reasonable. Instead of requiring agencies to have new technologies pre-approved by, say, a congressional committee, it would allow these organizations to make their own decisions; the legal restriction imposing punishment when convicted of privacy invasion by the Supreme Court would simply ensure that law enforcement agencies take the time to consider the possible privacy implications of new technologies (in light of current legislation and judicial precedents) before they employ them.

The combination of a minimal level of privacy (independent of technological advancements) with an incentive for law enforcement to avoid employing new technologies that would invade citizens' Fourth Amendment privacy should be capable of limiting new search technologies and restoring a balance between the interests of law enforcement agencies and those of private citizens.

Conclusion:

Over the last eighty years, technological development has expanded the scope and power of police searches and shifted power away from the private citizen into the hands of law enforcement agents. The long response time between the introduction of new technologies and their regulation, either by Congress or by the Supreme Court, has combined with cyclic interpretations of the *Katz* test to undermine the privacy protection afforded by the Fourth Amendment. However, this trend away from personal privacy is

not inevitable; by establishing the existence of a minimum level of privacy and reinforcing Court decisions with legislative punishments, it would be possible to restore the privacy protection intended by the Fourth Amendment and simultaneously act to ensure that that protection will continue in the face of the unforeseen technological advances of a future age.

Bibliography:

Bernstein, Merrick D. " 'Intimate Details': A Troubling New Fourth Amendment Standard for Government Surveillance Technology." *Duke Law Journal,* Vol. 46. No. 3 (Dec. 1996) p. 575-610

"Criminal Procedure. Search and Seizure. Tenth Circuit Finds that thermal Imaging Scan of a Home Constitutes a Search. United States v. Cusumano, 67 F.3d 1497 (1oth Cir. 1995)" *Harvard Law Review*, Vol. 109. No. 6 (Apr. 1996), p. 1445-1450.

Documents of American Constitutional and Legal History Ed. Melvin Urofsky and Paul Finkelman. Oxford University Press. 2002.

Fillingham, David. "Listening in the Dark – Wiretapping and Privacy in American" http://www-swiss.ai.mit.edu/6095/student-papers/fall97-papers/fillingham-wiretapping.html

"The Fourth Amendment and Carnivore." Statement of the Electronic Frontier Foundation. U.S. house of Representatives. July 28, 2000. http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html

Joh, Elizabeth. "Reclaiming 'Abandoned' DNA: The Fourth Amendment and Genetic Privacy. UC Davis Legal Studies Research Paper Series. April 2005.

Kerr, Orin S. "Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't." *Northwestern University Law Review*. Vol. 97, No. 2. 2003.

Kyllo v. United States 533 U.S. 27. http://supreme.justia.com/us/533/27/case.html

Nardone v. United States 308 U.S. 338 (1939) http://supreme.justia.com/us/308/338/case.html

"New Technologies and the Constitution." U.S. Congress, Office of Technology Assessment OTA-CIT-366. Washington D.C: U.S. Government Printing Office, May 1988.

Olmstead v. United States 277 U.S. 438 (1928) http://www.law.cornell.edu/supct/html/historics/USSC_CR_0277_0438_ZS.html

"Privacy and Government: The Electronic Communications Act" http://www.privacilla.org/government/ecpa.html

Seamon, Richard H. "Kyllo v. United States and the Partial Ascendance of Justice Scalia's Fourth Amendment." *Washington University Law Quarterly*. February, 2002.

Simmons, Ric. "Technology-Enhanced Surveillance by Law Enforcement." *Annual survey of American Law*. 2004.

Sklansky, David A. "Back to the Future: Kyllo, Katz, and Common Law" *Mississippi Law Journal*. Forthcoming.

Solove, Daniel J. "Reconstructing Electronic Surveillance Law" *The George Washington Law Review*. Vol. 72 p. 1701.

Steinberg, David E. "Sense Enhanced Searches and the Irrelevance of the Fourth Amendment." UC San Diego Legal Studies Research Paper Series.

Thompson, Carolyn. "Police DNA Collection Sparks Questions." Associated Press. March 17, 2007. http://apnews.myway.com/article/20070318/D8NU9GB80.html

Webber, Dawn. "Fourth Amendment, Of Warrants, Electronic Surveillance, Expectations of Privacy, and Tainted Fruits." *The Journal of Criminal Law and Criminology*. Vol. 75, No. 3. (Autumn, 1984), p 630-652.

Wolf, Paul. "COINTELPRO." http://www.icdc.com/~paulwolf/cointelpro/cointel.htm