Journal of Criminal Law and Criminology

Volume 97
Issue 2 *Winter*

Article 4

Winter 2007

Why 2007 is Not Like 1984: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence

Ric Simmons

0091-4169/07/9702-0531
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY
Vol. 97, No. 2

WHY 2007 IS NOT LIKE *1984*: A BROADER PERSPECTIVE ON TECHNOLOGY'S EFFECT ON PRIVACY AND FOURTH AMENDMENT JURISPRUDENCE

RIC SIMMONS*

Technological advances have generally been seen as the enemy of privacy, giving the government advanced tools to monitor our most intimate activities. This Article takes a broader look at the effect of new technologies and privacy, and comes to the opposite conclusion: over the past one hundred and fifty years, new technologies have for the most part enhanced our privacy, and many of the invasive surveillance technologies that the government now uses are simply a response to this enhanced level of privacy—that is, an attempt to return to the former balance between individual privacy and law enforcement needs. The Article first examines the ways in which new technology has enhanced our privacy, and then examines the effect of new technology on government surveillance, dividing surveillance technologies into three categories: those that allow government agents to do what was previously impossible; those that allow government agents to conduct traditional methods of surveillance more efficiently; and those that the government has developed in response to privacy-enhancing technologies. The Article then reviews the current statutory and constitutional law regarding surveillance technology in light of these categories, and critically examines that law—and the balance or imbalance that it creates between the two competing goals of Fourth Amendment jurisprudence.

* Assistant Professor of Law, Moritz College of Law at the Ohio State University. I am grateful for the extensive editing and feedback provided by Professor Angela Lloyd and the research assistance and comments provided by Courtney Cook, J.D. 2007.

I. INTRODUCTION

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in 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.[1]

George Orwell's chilling vision of the future depicted ways in which new technologies could one day be used by a totalitarian state to obliterate all privacy and freedom. Orwell wrote the novel in 1948,[2] when television was still in its infancy, computers filled entire rooms and processed data at a snail's pace, and devices such as thermal imagers and particle detectors existed only in science fiction stories.[3] At the dawn of this technological revolution, Orwell presented us with a clear message: new technologies would allow the state to dramatically increase its power over the individual, enabling totalitarian and fascist states to control every aspect of the lives of their citizens.[4]

It is now evident that Orwell's vision was wrong. Modern technology has turned out to be the totalitarian state's worst enemy. Video cameras are indeed everywhere, but they are embedded into cell phones and wielded by millions of individual citizens—and as a result it is the people who are watching the government, not the other way around.[5] These same cell

---

[1] GEORGE ORWELL, 1984 158 (Bernard Crick ed., Oxford Univ. Press 1984) (1949).

[2] *Id.*

[3] Television use did not become widespread until the postwar era; in 1945, it is estimated that there were only seven thousand working television sets in the entire country. History of Television, http://www.high-techproductions.com/historyoftelevision.htm (last visited Apr. 21, 2007). Also in the postwar era, one of the first "high-speed" electrical computers began operation. It was called the Electrical Number Integrator and Calculator, or ENIAC, and it used 18,000 vacuum tubes and took up 1,800 square feet of floor space. exploremy: brief history of the computer, http://www.softlord.com/comp/ (last visited Apr. 21, 2007) [hereinafter exploremy].

[4] ORWELL, *supra* note 1. This view is also held by many leading scholars and judges. *See, e.g.*, Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting) ("Electronic surveillance . . . makes the police omniscient; and police omniscience is one of the most effective tools of tyranny.").

[5] As far back as 1991—eons ago in the technological age—an amateur video photographer captured the beating of Rodney King by four Los Angeles police officers, who were eventually convicted for violating King's civil rights. *See* United States v. Koon, 833

phones use satellite transmissions to communicate information to every corner of the globe, defying government censors.[6] Meanwhile, the Internet has exponentially increased the flow of personal, commercial, and political information to and from individuals in ways that are largely beyond state control. The powerful computers that were foreseen do in fact exist today—only instead of being massive mainframes that fill rooms and that are so expensive only huge corporations and state actors can afford them, these computers sit on the desk or in the lap of private individuals, allowing each of us to create, store, manipulate, and process amounts and types of data that were inconceivable forty years ago.[7] All the terrifying technological tools that Big Brother used in Orwell's dystopian vision[8] are instead owned and controlled by individual citizens, both in this country and around the world. New technologies have indeed dramatically altered the balance of power between state control and individual autonomy—but the effect has been just the opposite of what Orwell predicted.

A similar misperception has occurred in the context of the Fourth Amendment and privacy—despite evidence that technology has enhanced privacy for many people, there exists a fear that new technologies are eroding Fourth Amendment protections.. Lay people read about powerful new surveillance technologies used by law enforcement agents and understandably react with trepidation.[9] Over the last century, the government has begun tapping our phones;[10] flying (at lower and lower

F. Supp. 769 (C.D. Cal. 1993). As *Time* magazine noted in its "Person of the Year" issue for 2006: "Do a YouTube search today on the term police brutality, and you get more than 780 videos, from Houston, Hungary, Egypt, and beyond." James Poniewozik, *The Beast with a Billion Eyes*, TIME, Dec. 25, 2006/Jan. 1, 2007, at 63, 63.

[6] *See, e.g.*, Mark O'Keefe, *China Widens Crackdown on Faithful*, OREGONIAN (Portland), Sept. 18, 1999, at A11 (describing how underground Christian leaders in China communicate with each other via cell phone while traveling around the country to evade the authorities).

[7] The ENIAC computer in use in Orwell's day was capable of making three hundred calculations per second. exploremy, *supra* note 3. A modern laptop computer available for around $1,000 can perform over two billion calculations per second. *See* Dell XPS M1210, http://www.dell.com/content/products/productdetails.aspx/xpsnb_m1210?c=us&cs=19&l=en&s=dhs&~section=specs#tabtop (last visited Apr. 21, 2007).

[8] *See supra* note 1 and accompanying text.

[9] Jennifer Lee, *Police Seek to Increase Surveillance*, N.Y. TIMES, May 31, 2005, at B3 (noting that after police announced installation of four hundred surveillance cameras in high-crime, high-traffic areas in New York City, some people feared the cameras would compromise their privacy). One councilman in Loma Linda, California equated the installation of surveillance cameras in public areas with "Cuba or communist Russia." Jacob Ogles, *Privacy Experts Worry About Public Cameras*, INLAND VALLEY DAILY BULL. (Ontario, Cal.), Nov. 20, 2005.

[10] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

altitudes) over our houses and yards;[11] installing video cameras or hidden microphones in our offices, homes, and hotel rooms;[12] intercepting our e-mails;[13] scanning images of our faces in crowds;[14] monitoring our web browsing;[15] seizing and copying from our hard drives;[16] and even looking through the walls of our houses.[17] Legal scholars have also reacted with alarm, decrying the loss of privacy and individual rights brought on by new surveillance technologies.[18]

But the impact of new surveillance technologies is only one chapter of the story of how technology has affected privacy in modern society. Over the past century, millions of individuals—both innocent and culpable—have begun using everyday technology to increase their privacy. Just as George Orwell misunderstood the implications of new technologies by focusing only on their use by government agents, Fourth Amendment scholars all but ignore the ways in which technology has enabled average citizens and criminals to keep their activities hidden from law enforcement.[19] New technology has also strengthened individual privacy in

---

[11] *See* Florida v. Riley, 488 U.S. 445, 451 (1989) (describing government agents flying over the defendant's field at four hundred feet of altitude); California v. Ciraolo, 476 U.S. 207, 215 (1986) (describing government agents flying over the defendant's field at one thousand feet of altitude).

[12] *See, e.g.*, United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984).

[13] *See, e.g.*, United States v. Jones, 364 F. Supp. 2d 1303, 1304-05 (D. Utah 2005).

[14] *See infra* notes 51-53 and accompanying text.

[15] *See* Orin S. Kerr, *Internet Surveillance, Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 633-34 (2003) [hereinafter Kerr, *Internet Surveillance*].

[16] *See, e.g.*, United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999).

[17] *See* Kyllo v. United States, 533 U.S. 27, 29-30, 40 (2001).

[18] *See, e.g.*, Patricia L. Bellia, *Surveillance, Records & Computers: Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1458 (2004) (arguing that government agents should have to obtain a warrant before seizing e-mail messages stored by a third party).

[19] There are a few exceptions. Some scholars have looked at the ways in which technology has increased privacy, particularly in the context of encryption. *See generally* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?,"* 33 CONN. L. REV. 503, 530-31 (2001) [hereinafter Kerr, *Fourth Amendment in Cyberspace*] (noting that "code itself extends far greater privacy protection than the warrant requirement of the Fourth Amendment ever could"). Professor Kerr also noted in another article that in the narrow context of surveillance "[s]ome new technologies make pre-existing forms of surveillance more intrusive; others have the opposite effect." Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 865 (2004) [hereinafter Kerr, *New Technologies*] (giving examples of thermal insulators, soundproofing, and white-noise generators as examples of technological countermeasures which could be employed by individuals to defeat new surveillance technologies). But Kerr also notes that "[m]ost commentators focus

at least two other ways: by enabling governments to target surveillance more effectively, resulting in more narrowly tailored searches;[20] and by enhancing our ability to monitor the conduct of government agents.

The conventional wisdom among scholars consists of two assertions, one factual and one normative. The factual assertion is that the effect of new technologies has been to alter the balance between individual privacy and the state's power to investigate crimes, thereby decreasing individual privacy and increasing the ability of government agents to learn private information about us.[21] The normative assertion is that this shift is a negative development, and therefore it is necessary to restore the original balance—either by creating more regulations or statutes to limit government power, or perhaps by changing the way the Fourth Amendment is interpreted by the courts in cases involving new technologies.[22] This Article will argue that this factual assertion is incorrect—or, more accurately, that it is incomplete—and therefore too simplistic, because it does not take into account the wide variety of ways in which technology has affected the balance between individual privacy and government investigatory power.

This Article will examine the interplay between technology, law, and privacy, taking a broad view on how technology has affected the critical balance between individual privacy and effective law enforcement.[23] Section II will examine how technology has, for the most part, enhanced the

---

on the [intrusive] half of this equation while ignoring the second half,"—and even Kerr himself is only talking about counter-surveillance technology, not common, everyday technology (such as cell phones, computers, and the Internet) which have increased privacy (and secrecy) for nearly every member of society. Kerr, *Fourth Amendment in Cyberspace*, *supra*, at 865 n.383.

[20] *See infra* notes 128-133 and accompanying text.

[21] *See, e.g.*, Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 382 (2003) (suggesting that while consumers enjoy new technologies, such as cell phones, these products have become the consumer's "ankle bracelet," because the government can now monitor citizens' movements more easily).

[22] *See, e.g.*, Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH L. & POL'Y 135, 153-56 (2003) (arguing that the Fourth Amendment should be interpreted to provide more privacy to e-mail conversations than to phone conversations); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 130 (2002) (arguing that the Supreme Court's approach to Fourth Amendment cases undervalues privacy).

[23] According to Fourth Amendment jurisprudence, courts judge the reasonableness of a search "by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652-53 (1995).

privacy of individuals in their everyday lives, allowing them to communicate more privately, store data more securely, and conduct a much wider range of activities within the privacy of their own homes. Section III then turns to the effect of new technology on government surveillance, and divides surveillance technologies into three categories: those that allow government agents to do what was previously impossible; those that allow government agents to conduct traditional methods of surveillance more efficiently; and, those that the government has developed in order to combat the privacy-enhancing technologies described in Section II. Section IV will review the current statutory and constitutional law regarding surveillance technology, and Section V will then critically examine that law—and the balance or imbalance that it creates between the two competing goals of Fourth Amendment jurisprudence. Finally, Section VI will examine other ways in which technology has impacted everyday privacy.

II. TECHNOLOGY AND PRIVACY

In order to understand the true impact of technology on privacy—and, more specifically, in order to accurately gauge the effect of new surveillance technology on the balance between individual privacy and government investigatory power—the first step is to evaluate how technology has changed the amount of privacy in society for everyday citizens. As in any context in which we are examining the effects of technology on society, the changes tend to be subtle and incremental in the short term, but dramatic and momentous in the long run. In the field of medicine, for example, each new drug or surgical technique might have a small influence on the way a certain disease is treated—but the cumulative effect of all of these advances has increased life expectancy in this country from around forty-seven to seventy-eight over the past one hundred years.[24]

Likewise, the effect of new technologies on our privacy in everyday life is easy to overlook, since we quickly adapt to the small gains that are made and fail to notice how fundamentally our lives are changing. By taking a broader perspective, however, we can see how new technology has dramatically increased the amount of privacy each of us now enjoys in our lives.

---

[24] In 1900, life expectancy at birth was only forty-seven years. NAT'L CTR. FOR HEALTH STATISTICS, HEALTH, UNITED STATES, 2006 167 tbl.27 (2005), *available at* http://www.cdc.gov/nchs/data/hus/hus05.pdf#027. Life expectancy in the year 2004 was nearly seventy-eight years. *See* ARIALDI M. MINIÑO ET AL., CTRS. FOR DISEASE CONTROL, DEATHS PRELIMINARY DATA (2004), *available at* http://www.cdc.gov/nchs/products/pubs/pubd/hestats/prelimdeaths04/preliminarydeaths04.htm.

To better visualize this broad perspective, let us engage in a time-travel thought experiment. Assume that Sally and Harry, two residents of early nineteenth century America, wish to have a private communication with each other. As it turns out, their options are limited. Sally could invite Harry to her home—though of course anyone could see Harry entering and leaving Sally's home, so the fact that they were conversing would be public knowledge. Sally could write Harry a letter, but again the name of the person with whom she was communicating would be open to the world. More troubling would be the fact that—assuming there was no legal impediment—any government agent wishing to know the content of her communication could intercept and read the mail before it got to its destination.

Now assume that Sally and Harry live in 1950. The technological advance of the telephone[25] has greatly increased their chances of having a private conversation. Casual observers of their affairs will have no idea that the two of them are talking, much less what they are talking about. But although the telephone is an improvement, it is not foolproof. They can only use the telephone at certain locations—their home, their office, perhaps a quasi-public phone booth. Furthermore, the local telephone operator might be listening in on their phone conversation.[26] Almost all residential lines are party lines, which each have to share with up to ten other households—and any member of any of those households could be eavesdropping on their conversation without their knowledge.[27] And once again (assuming no legal restrictions exist), government agents could subpoena phone records to determine whom Sally is calling, or set up a device to tap Sally's phone.[28] It should be noted, however, that these actions by the government require substantially more effort and technical expertise than simply looking at Sally's outgoing and incoming mail.[29]

---

[25] *See infra* notes 32-33 and accompanying text.

[26] California v. Greenwood, 486 U.S. 35, 54 (1988) (Brennan, J., dissenting) (suggesting that an operator can listen in on telephone conversations).

[27] *See* Privateline.com Telephone History: Party Line Service, http://www.privateline.com/TelephoneHistory5/partyline.htm (last visited Apr. 21, 2007).

[28] *See, e.g.*, Olmstead v. United States, 277 U.S. 438 (1928) (discussing the use of wiretaps as early as 1928); N.Y. Times Co. v. Gonzalez, 459 F.3d 160 (2d Cir. 2006) (discussing the constitutionality of subpoenaing a reporter's phone records from a third party).

[29] For example, one problem police sometimes encounter when intercepting a phone call is converting the communication to a digital signal, which requires the use of sophisticated software. *See* Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics,"* 7 HARV. J.L. & TECH. 239, 241 n.9 (1994). There is obviously no need for such technology when intercepting and reading mail.

Finally, assume that Sally and Harry live in the modern world. Now they can communicate with each other from almost any spot in the country using cell phones, with no chance of a human operator casually eavesdropping on their conversation. They can also send e-mails or instant messages to each other from their computers. And if they are very worried about privacy, they can easily take measures to make their conversation even more secure. A cell phone can be bought and used for a day and then discarded, making the calls much more difficult to trace.[30] E-mail can be sent and received to and from anonymous accounts, or the two individuals could purchase an inexpensive encryption program which would shield their e-mail communications from even the most sophisticated government code breakers.[31]

Of course, the government has been able to find ways to intercept electronic communications—but this in itself does not mean that the new technology has led to a decrease in privacy. A modern-day Sally and Harry still have all the old ways of communicating with each other—they can still visit each other's houses, send each other mail, or call each other on land-based phone lines. In other words, technology has given them *more* ways

---

[30] In response to this practice, federal and state governments have passed laws making it easier for law enforcement to track and wiretap telephone calls from such "disposable" phones. *See generally* Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971, 980-82 (2003) (discussing the proliferation of new state and federal laws which allow for "roving wiretaps"). In the past, wiretap warrants applied only to a specific phone line. *Id.* at 980. Thus, use of disposable cell phones could render such warrants useless because a criminal could have moved on to another phone before law enforcement obtained a warrant to wiretap the previous phone. However, in 1986, so-called "roving" wiretaps were authorized for domestic surveillance under the Electronic Communications Privacy Act. *Id.* at 981; *see also* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986); 18 U.S.C. § 2518 (2000). A roving wiretap warrant permits surveillance of "any communications device a target of an investigation is likely to use, without specifying the telephone or other facilities in the orders or applications." Kennedy & Swire, *supra*, at 980-81. Essentially, a roving wiretap wiretaps the person, rather than the phone. The PATRIOT Act extended such roving wiretap authority to foreign intelligence investigations and now allows such a wiretap order to apply nationwide, rather than simply in the district in which the authorizing judge sits. *Id.* at 981-82; *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, §§ 206, 216(a), 115 Stat. 272, 282, 288 (2001). Although these statutes assist law enforcement in tracking and wiretapping disposable phones, they are not perfect. Law enforcement would still need to discover what disposable phone a terrorist is using or would be likely to use before a roving wiretap would be of any use.

[31] *See* Charles Barry Smith, *Current U.S. Encryption Regulations: A Federal Law Enforcement Perspective*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 11, 15-16 (2000) (describing encryption technology and criminals' and terrorists' use of such technology to evade law enforcement).

to communicate; more options to choose from in deciding which method of communicating is the most secure.

In addition, the economic effects of new technologies must be considered, since in discussing the effect of technology on privacy, we should not look at the amount of privacy a person has in theory, but the amount they have (or used to have) in practice. In 1800, a face-to-face visit was extremely difficult to set up because most people lived in rural areas that were great distances apart, and so travel between residences took considerably longer than it does today. Those who lived in urban areas could more easily travel to see each other—but nineteenth century cities were difficult places to find privacy, as most individuals lived in apartments or tenements which were shared with many other family members. As has been true throughout history, the very rich—enjoying private residences and easy access to transportation—could engage in private conversations without a problem, but for the vast majority of citizens, private communications were difficult to come by.

The telephone was invented in 1876,[32] but in the early twentieth century, it was still a rare device, used only by those wealthy enough to afford them.[33] By the 1950s, the telephone was more commonplace, but almost no home had more than one phone line, and many residences still had none.[34] Today, nearly 70% of Americans have their own personal telephone which they carry with them everywhere[35]—cellular phones are so inexpensive that they are prevalent among every economic class[36]—and

---

[32] Catherine J. Lanctot, *Attorney-Client Relationships in Cyberspace: The Peril and the Promise*, 49 DUKE L.J. 147, 162 n.34 (1999) (citing U.S. Patent No. 174,465 (issued Mar. 7, 1876)).

[33] In the early part of the twentieth century, only 1.5 million Americans had telephones. *Id.* Even by the beginning of World War II, fewer than half of Americans had telephones. *Id.* Cost may have been part of the cause of the rarity of telephones. *See* Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667, 714-15, n.289 (2006). Telephone companies attempted to increase the pervasiveness of telephones in the early twentieth century by cutting the service cost in half so more Americans could afford them. *Id.*

[34] As late as 1985, there was only one residential phone line for every three citizens, and fewer than one residential phone line per household. U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES tbls.2, 57 & 1131 (2007), http://www.census.gov/compendia/statab/. Census records show that there were 79 million residential phone lines for a population of about 85 million households and 238 million people. *Id.*

[35] As of 2005, 207 million Americans owned cell phones. *Id.* at tbl.1132. This represented 70% of the total population of the United States that year (296 million), and 75% of the total population of the United States over five years old (276 million). *Id.* at tbl.21.

[36] In fact, many cell phones themselves are free when the individual purchases a service plan. *See, e.g.*, Amazon.com: Cingular, http://www.amazon.com/s/103-3259454-8491016?ie=UTF8&index=wireless-phones&field-vendorcode=Cingular (last visited Apr. 21, 2007).

those that do not have a cell phone almost certainly have access to a traditional telephone. In short, advancing technology has not only given us devices which dramatically increase our privacy, but has also made these devices affordable to almost everyone.

The same analysis can be applied to most other categories of privacy. Take data storage: a nineteenth century diary writer would have very limited options as to how to secretly record and store his writings. In modern times, the diary could be written on a laptop computer, accessible only to someone with the password—or stored on a hard drive the size of a pen and hidden almost anywhere. More broadly, the rise of the personal computer and the Internet has allowed individuals to stay in the privacy of their own home to conduct many activities which formerly had to be done in public. An individual today can browse and shop online for any item she might want, from clothing to cooking utensils to pornography;[37] she can access and download almost any kind of picture, political treatise, song, or book;[38] she can even "develop" her own digital pictures, insert them into a pamphlet she is writing, and print multiple copies of the pamphlet for distribution later.[39] Only twenty years ago, almost any of these tasks would require the average person to leave her home and personally visit any number of other businesses; it was impossible to browse through and purchase a book without leaving your home, while developing your own pictures and printing your own pamphlet at home was possible only with expensive and unwieldy equipment.

In short, one of the primary effects of technology on society over the past two hundred years has been to *increase* the amount of privacy in our everyday lives. Individuals—including criminals—can now conduct many more activities secretly, particularly activities which involve communicating, storing, or processing information. This increased secrecy has posed a problem for law enforcement officials, who have responded by developing and using special technology to conduct their surveillance.

III. ADVANCES IN SURVEILLANCE TECHNOLOGY

With this understanding of the overall effect of technological advancements on privacy as a backdrop, we will now turn to the more traditional concept of the relationship between technology and privacy: the threat to privacy posed by modern surveillance technology. This Article

---

[37] *See, e.g.*, Amazon.com, http://www.amazon.com/ (last visited Apr. 21, 2007).

[38] *See, e.g.*, Apple—iTunes, http://www.apple.com/itunes/store/ (last visited Apr. 21, 2007).

[39] *See, e.g.*, Apple.mac, http://www.apple.com/dotmac/ (last visited Apr. 21, 2007) (describing the software iLife).

will divide modern surveillance technology into three categories: (1) devices that allow government to see things it could never see before; (2) technology that allows governments to conduct more traditional surveillance more efficiently; and (3) "responsive" surveillance technology, which the government has been forced to use in order to keep up with new privacy-enhancing technologies.

A. THE ORWELLIAN NIGHTMARE: TECHNOLOGY AS THE ENEMY OF PRIVACY

The conventional wisdom is undeniably correct in one aspect: surveillance technology has vastly improved over the past century, giving the government valuable tools to investigate potential criminals, but also creating new challenges for the legislatures and the courts as they struggle to determine how (if at all) the new technologies should be regulated. Perhaps the most frightening type of surveillance technology involves devices which allow the government to see, hear, or gather information that would otherwise be impossible for it to detect. Specifically, electronic eavesdropping devices and hidden cameras can now be installed in homes or offices to see and hear what people are doing in their most private places.[40] If agents are not able to get inside a home or office, parabolic microphones are available that can listen to conversations through a window from a significant distance.[41] Meanwhile, outside the home, hand-held detectors can "see" through clothing and provide an outline of every item the subject is carrying.[42] Nearly every cell phone in use today is

---

[40] *See* Charles B. Craver, *Privacy Issues Affecting Employers, Employees, and Labor Organizations*, 66 LA. L. REV. 1057, 1068-70 (2006) (discussing employees' potential statutory protection from employers' use of hidden cameras in private places, such as lavatories or locker rooms, and hidden microphones that pick up conversations between co-workers); Daniel R. Dinger, *Should Parents Be Allowed to Record a Child's Telephone Conversations When They Believe the Child Is in Danger?: An Examination of the Federal Wiretap Statute and the Doctrine of Vicarious Consent in the Context of a Criminal Prosecution*, 28 SEATTLE U. L. REV. 955, 968-89 (2005) (discussing the legality of parental electronic recording of children's telephone calls in the home); *see also* Shana K. Rahavy, *The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home*, 2 J. HIGH TECH. L. 87, 95-98 (2003).

[41] *See* United States v. Karo, 468 U.S. 705, 712 (1984) (describing a parabolic microphone as "capable of picking up conversations in nearby homes"); United States v. Infelise, No. 90 CR 87, 1991 U.S. Dist. LEXIS 17174, at *17 n.1 (N.D. Ill. Oct. 18, 1991) ("A parabolic microphone is a portable device that allows the listener to eavesdrop on all conversations that come within the range of the microphone."); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1265 (2004) ("[P]arabolic microphones can record conversations at long distances.").

[42] *See* David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 7-13 (1996) (describing the development of

required to contain a GPS-based locator device, so that emergency responders can locate a 911 caller—but the location information may also be available to government agents for other purposes.[43] Ion scanners can be waved over any surface to detect the presence of drugs or explosives;[44] airplanes fly over our fenced-in fields, allowing law enforcement agents to view our backyards;[45] and satellites in space can take pictures of these backyards with a stunning level of detail.[46] Finally, law enforcement agents are compiling vast and growing DNA databases, which allow them not only to determine if a certain individual was present at a certain crime scene, but also to identify sensitive and personal health information about the individuals who are catalogued in the database.[47]

The effect of this category of surveillance technology on our personal privacy is unambiguously negative. Not only can government agents see and hear things that were formerly impossible to see and hear, but most of the time when they do so, we are unaware of the surveillance. Unlike a traditional search of our home or our person, during which we can see the agents rifling through our belongings or feel them patting down our clothing, we have no idea when hidden video cameras or microphones are recording our actions or conversations. This combination of increased intrusiveness and the potentially hidden nature of the surveillance has fueled much of the concern over the effect of technology on privacy, and has in some cases led to tight legal restrictions on the use of some of these surveillance methods.[48]

---

portable detectors which can "see" through clothing from a distance to detect guns); *see also* Steven G. Brandl, *Back to the Future: The Implications of September 11, 2001 on Law Enforcement Practice and Policy*, 1 OHIO ST. J. CRIM. L. 133, 149 (2003) (noting the use of low level x-rays that facilitate detection of weapons, explosives, drugs, and contraband under clothing).

[43] *See* Thomas Lee, *supra* note 21, 381-87.

[44] *See* Heather K. McShain, *Not Quite Bradbury's* Fahrenheit 451*: The Uncertain Future of Sense-Enhancing Technology in the Aftermath of* United States v. Kyllo, 105 W. VA. L. REV. 1, 44 nn.229-30 (2002).

[45] *See, e.g.*, California v. Ciraolo, 476 U.S. 207 (1986).

[46] Ross Kerber, *Privacy: When Is a Satellite Photo an Unreasonable Search?*, WALL ST. J., Jan. 27, 1998, at B1 (describing some of the detail of satellite photos); *see also* Mark Morford, *I Can See Your House From Here; Google's Close-Up Satellite Photo Maps are Way Creepy, But in a Very Cool Way*, S.F. GATE, Apr. 8, 2005, http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2005/04/08/notes040805.DTL (describing the detailed satellite photo technology now available to ordinary citizens through www.google.com).

[47] *See generally* Seth F. Kreimer, *Truth Machines and Consequences: The Light and Dark Sides of "Accuracy" in Criminal Justice*, 60 N.Y.U. ANN. SURV. AM. L. 655 (2005).

[48] *See infra* notes 64-69 and accompanying text.

B. TECHNOLOGY WHICH IMPROVES THE EFFICIENCY OF SURVEILLANCE

Surveillance technologies in the first category invade our private space to gather information which government agents would otherwise be unable to gain access to without conducting an intrusive search of our homes or our bodies. In contrast, the second category of privacy-infringing surveillance technology are devices which merely allow law enforcement officers to process already public information more quickly and efficiently—for example, cameras in public spaces that allow one officer to monitor many different locations at once,[49] or location tracking technology that allows law enforcement to determine the location of anyone in a public area.[50] In practice, the distinction is sometimes a subtle one—indeed, the same technology (such as ion scanners, airplane flyovers, and location tracking devices) can be used to gather information from private or public spaces. Furthermore, individuals being watched by cameras or traced by secret homing devices may feel that their privacy is being infringed upon regardless of whether they are in a public or a private place. But as we will see later, the distinction is a critical one for the legal system.

A good example of this hyper-efficient public surveillance is facial recognition technology. This technology involves installing numerous cameras at a public event or in airports and taking thousands of pictures of all the individuals who pass by.[51] The pictures are then passed through a computer which compares the facial features of each individual to pictures of known fugitives, using standard biometric measurements (such as size of mouth, distance between the eyes, and angle of nose).[52] In theory, this technology would allow law enforcement to scan through thousands of faces in a crowd and alert officers on the ground to the presence of any known fugitives that might be present.[53] As long as the surveillance is only conducted in public places, however, it really is doing no more than what police officers could have done on their own without the technology—scanning faces in crowds and comparing them to pictures of known suspects. The use of the technology simply makes the surveillance more

---

[49] *See supra* note 9 and accompanying text.

[50] *See infra* note 70 and accompanying text.

[51] *See* American Civil Liberties Union: Q&A on Face-Recognition, http://aclu.org/privacy/spying/14875res20030902.html (last visited Apr. 21, 2007).

[52] *Id.*

[53] *See id.* However, in practice, the technology has not been particularly effective so far. *See id.* For example, in the 2001 Super Bowl at Tampa Bay, of the tens of thousands of individuals scanned, only nineteen were flagged, and some of them were false positives. *Id.* Numerous studies have shown that the technology fails to identify target individuals if the camera angle has changed, or if the target has grown or shaved facial hair. *Id.*

efficient, allowing this type of surveillance to occur with a smaller outlay of human resources.

Other examples of this category of surveillance include more efficient ways of gathering public information—mining public data from the Internet, for example, or placing a homing beacon on someone's car to track its movements on the public highway.[54] Without using this technology, a law enforcement officer could gather the same information by traveling to all the appropriate government offices and copying down a suspect's tax records, property records, and so on. Likewise, a team of law enforcement officers could follow the suspect's car twenty-four hours a day to keep track of his movements. But conducting this type of surveillance the old-fashioned way would require such a great allocation of resources that it would not be feasible for most investigations. Technology makes these formerly labor-intensive searches feasible for a much broader category of crimes.

Of course, these hyper-efficient technologies might also be used to monitor *private* information instead of public information. A homing device could easily be used to monitor someone's whereabouts inside their home, or a computer program could be designed to sift through every single e-mail sent by certain suspects. In these situations, the surveillance would fall into both the second category and either of the other two categories, and (perhaps) require different treatment under the law.

C. GOVERNMENT RESPONSES TO PRIVACY-ENHANCING TECHNOLOGY

As noted in Section II, the primary effect of new technology over the past century has been to dramatically increase the privacy of everyday citizens, by giving them more private ways to communicate and more secure ways to store and encrypt data, and by vastly increasing the breadth and scope of activities that can be accomplished within their own homes. Unfortunately, what has been good for individual privacy has also been good for criminals. Sally and Harry may not be sending love letters but instead may be planning to blow up a government building; the diary writer might be trying to hide illicit financial information in order to cheat on his taxes; the computer user may not simply be shopping for a book or printing up a pamphlet, but could also be trying to hack into secure databases, send child pornography, or print counterfeit checks. So, as technology has enabled individuals to live more private and secret lives, the government has been forced to turn to new surveillance technologies which enable them to investigate individuals using privacy-enhancing technology.

---

[54] *See infra* note 70 and accompanying text.

When looked at in this light, much of the new surveillance technologies used by the government over the past century shows that the state is constantly playing catch-up, trying to find new ways to overcome the increased use of privacy-enhancing technology by those conducting criminal activity. Conspirators who do not want to meet in public or risk sending letters through the mail can communicate by cell phone or e-mail, forcing the government to combat this technological concealment by attempting to tap the telephone transmission or intercept the e-mail. Criminals who want to conceal child pornography, fraudulent financial documents, or any other large volume of data no longer need to find warehouses or storage units to stash their boxes—they can simply use digital data (or scan and then destroy the existing hard copies) and stash it, perhaps in encrypted form, on a very small storage device. And just as innocent people can buy a book or print out their own pamphlet from their bedroom, crimes which once required sophisticated equipment and multiple co-conspirators, such as counterfeiting or producing of child pornography, can now be committed by a lone individual inside his home, where he receives the maximum protection available under the Fourth Amendment.

This category of "responsive surveillance" includes many of the more sophisticated surveillance technologies that are intended to intercept electronic communications—tracing telephone calls, tapping into phone lines, and intercepting or retrieving e-mails. This category also includes searches of more sophisticated storage techniques—such as creating and sifting through a bitstream copy of a suspect's hard drive. And it could conceivably include more aggressive surveillance measures that government agents employ in order to combat the wider and more dangerous array of criminal activity that might be taking place inside a home.

One example of these more aggressive measures is the recent case of *Kyllo v. United States*, in which government agents used a thermal imager to detect marijuana-growing heat lamps inside a suspect's home.[55] If Danny Lee Kyllo had sought to grow marijuana one hundred years ago, he would have been forced to do so outdoors in a field, where it could be seen by others. Even if Kyllo had attempted to hide the marijuana by locating the plants far inside his property,[56] concealed by trees or other crops, the

[55] Kyllo v. United States, 533 U.S. 27, 29-30 (2001).

[56] This hypothetical assumes the counterfactual premise that possession of marijuana was illegal one hundred years ago. In fact, possession of marijuana was legal in this country until the first states began to outlaw it in the second decade of the twentieth century. The federal government did not outlaw marijuana use until the 1930s. *See generally* Richard J. Bonnie & Charles H. Whitebread, II, *The Forbidden Fruit and the Tree of Knowledge: An Inquiry into the Legal History of American Marijuana Prohibition*, 56 VA. L. REV. 971, 1010 (1970).

Fourth Amendment did not prevent a law enforcement agent from venturing onto the property—even if he were trespassing—to view the marijuana.[57] Thus, the *Kyllo* case is an example of a defendant using technology—high-powered heat lamps—in order to better conceal his illegal actions, and the government then using another new technology—thermal imagers—in an attempt to counter the defendant's concealment.[58]

As the *Kyllo* example indicates, it is sometimes difficult to distinguish between the use of this "responsive" surveillance technology, and the first category of surveillance technology, which enables government agents to see, hear, or in some way gather information that they otherwise could not detect. Certainly, without modern technology, law enforcement officers could not listen in on our phone conversations, track our e-mails, search our hard drives, or measure the amount of heat emerging from our homes. But without modern technology to enable these activities in the first place, the suspects' conduct could be monitored using traditional surveillance methods. This distinction is important if we are examining how technology has altered the balance between privacy and criminal investigation, since the first category of surveillance technology unequivocally decreases privacy and increases the power of the state to investigate, while the responsive surveillance technology's effect on the balance is far more ambiguous. The distinction also matters legally, since courts and legislatures find it relatively easy to regulate surveillance technology that empowers state agents to do what was otherwise impossible, but tend to struggle when trying to regulate surveillance technology that is only useful in overcoming privacy-enhancing technology.[59]

Finally, it should be noted that in at least one area—encryption—privacy-enhancing technology has become so advanced that the government's attempts to catch up have proven futile. That is, there is no type of responsive surveillance technology that can be used to counteract the greater privacy enjoyed by individuals (including criminals) who make a serious effort to encrypt their communications.[60] As Professor Orin Kerr noted in a recent article, "[I]t becomes clear that the government will be

---

The first federal statute outlawing marijuana was the Marijuana Tax Act of 1937. *See* Marijuana Tax Act of 1937, Pub. L. No. 75-238, 50 Stat. 551 (1937) (repealed 1970).

[57] *See* Oliver v. United States, 466 U.S. 170, 179-81 (1984); Hester v. United States, 265 U.S. 57, 59 (1924).

[58] It is interesting to note that the thermal imager at issue in *Kyllo* did not actually detect the marijuana itself, but merely the technological device that the defendant used in order to grow the marijuana. *Kyllo*, 533 U.S. at 29-30.

[59] *See infra* notes 75-106 and accompanying text.

[60] *See* Kerr, *New Technologies*, *supra* note 19, at 530 (discussing the near impossibility of decrypting some complicated encrypted communications).

technically unable to decrypt any encrypted communication that is encrypted with anything other than a very short key, and that the decryption of even a short key would consume extraordinary amounts of government resources."[61] Thus, private communications for the sophisticated criminal are all but guaranteed, regardless of what methods the government uses to try to acquire the information.

IV. THE CURRENT LEGAL REGIME REGULATING GOVERNMENT SURVEILLANCE POWER

New technologies of any kind pose a challenge for policymakers and courts. When legislators are regulating the use of a new technology, they need to determine the many different ways that the technology is being used in society, and which of those various uses are beneficial to society and which are not.[62] Similarly, judges frequently need to apply old law to a new technology, and in doing so, they must analogize between the uses of the

---

[61] *Id.* The technological advantage the encoder holds over the codebreaker is based on the fact that sophisticated codes are only decipherable with the encryption key. *See id.* This key is a series of binary numbers—generally hundreds of binary numbers strung together. *See id.* In order to decipher the code, the codebreaker must try every single possible key one at a time. *See id.* This is not so difficult for a key which is 4 or 8 binary numbers long (since there are only 16 or 256 possible keys, respectively). But every time the encoder adds another digit to the string of numbers, she doubles the number of potential keys that have to be tested by the codebreaker—thus easily reaching a number of potential keys beyond the capabilities of even the fastest supercomputer to try in any reasonable amount of time. *See id.* at 529-30. Kerr gives the example of a code using a key that was 128 digits long (thus creating 3.4×10^{38} possible keys), which would "take a supercomputer several million years" to decipher. *Id.* at 530. Even if supercomputers become sixteen times faster over the next few years, the encoder need only add four more digits to the key in order to keep the supercomputer busy for the same amount of time.

[62] The long-running debate about how to regulate the Internet (if at all) is a good example of the problem that new technology poses to policymakers. *See, e.g.*, David B. Brushwood, *Responsive Regulation of Internet Pharmacy Practice*, 10 ANNALS HEALTH L. 75 (2001); Paul Ehrlich, *Cyberlaw: Regulating Conduct on the Internet: Communications Decency Act § 230*, 17 BERKELEY TECH. L.J. 401 (2002); Christine Hurt, *Regulating Public Morals and Private Markets: Online Securities Trading, Internet Gambling, and the Speculation Paradox*, 86 B.U. L. REV. 371 (2006); C. Dianne Martin & Joseph M. Reagle, *An Alternative to Government Regulation and Censorship: Content Advisory Systems for the Internet*, 15 CARDOZO ARTS & ENT. L.J. 409 (1997); Alanna C. Rutherford, Sporty's Farm v. Sportsman's Market*: A Case Study in Internet Regulation Gone Awry*, 66 BROOKLYN L. REV. 421 (2000); Joel Sanders, *The Regulation of Indecent Material Accessible to Children on the Internet: Is It Really Alright to Yell Fire in a Crowded Chat Room?*, 39 CATH. LAW. 125 (1999). The Internet can be put to many different uses, mostly good, and some very bad. Effective regulation can only come about when lawmakers reach a consensus as to which uses are desirable and which are not.

new technology and more traditional activities which are expressly covered by the statute or by precedents.[63]

In this sense, our first and most unsettling category of surveillance technology has been the easiest for the legal system to adapt to. When government agents use new technology to gather information that has traditionally been considered private, legislatures generally step in to strictly regulate the activity, and in the absence of any express statute, courts will tend to apply the Fourth Amendment and bar the use of such technologies without a warrant. For example, Congress has barred the use of electronic eavesdropping devices unless government agents obtain a Title III order, which requires a greater showing than the probable cause requirement for obtaining a search warrant.[64] And after an inconsistent start during which the Supreme Court struggled to refine its Fourth Amendment doctrine,[65] in 1967 the Court decided *Katz v. United States*, which held that electronic eavesdropping violated the Fourth Amendment.[66] *Katz* established the "reasonable expectation of privacy" standard, essentially holding that if a surveillance device is gathering traditionally private information, its use will be subject to Fourth Amendment regulation.[67] Similarly, in the absence of statutory guidance, lower courts have consistently applied the Fourth Amendment to video surveillance of private areas.[68]

---

[63] *See, e.g.*, *Kyllo*, 533 U.S. 27 (analyzing the constitutionality of thermal imagers by comparing them to older technologies and precedents); Kerr, *Fourth Amendment in Cyberspace*, *supra* note 19, at 513-19 (using Supreme Court and Circuit Court precedent to argue that the government does not violate the Fourth Amendment when it decrypts ciphertext); Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275, 1281-84 (2002) (discussing problems with applying old law to new technologies); *see also infra* notes 65-106 and accompanying text.

[64] 18 U.S.C. § 2518 (2000). In order to obtain a Title III order, the government must show that: (1) normal investigative procedures have been tried and have failed, are unlikely to succeed, or are dangerous; (2) the surveillance will be conducted in a way that minimizes the interception of irrelevant information; and (3) there is probable cause to believe that the interception will reveal evidence of one of a list of specific predicate crimes. *Id.* § 2518(3), (5). The order must be authorized by a high-level Justice Department official and signed by a federal judge, and is limited to thirty days. *Id.* § 2516 (2000 & Supp. III 2003); *id.* § 2518.

[65] *See, e.g.*, United States v. Silverman, 365 U.S. 505, 512 (1961) (holding that a "spike-mike" which produced the same result as *Goldman*'s Dictaphone was a search because it touched the property of the defendant); Goldman v. United States, 316 U.S. 129, 135 (1942) (deciding that a Dictaphone placed against a wall adjoining the defendant's office was not a "search" because the government agents did not trespass onto the defendant's property).

[66] Katz v. United States, 389 U.S. 347, 351-53 (1967).

[67] *Id.* at 360 (Harlan, J., concurring).

[68] *See, e.g.*, United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986); United States v. Torres, 751 F.2d 875, 883 (7th Cir. 1984).

The only real dilemma that these new technologies pose for courts and legislators is whether the highly intrusive and potentially secret nature of these types of surveillance should lead them to create even *greater* restrictions against their use than they do for traditional searches. As noted above, the requirements for obtaining a Title III order authorizing the use of electronic listening devices is much higher than the standard for obtaining a search warrant, and federal courts have held that the Fourth Amendment imposes an identical standard for video surveillance.[69]

Thus, the law has kept pace with the first category of surveillance technology, recognizing these searches as hyper-intrusive and imposing extra requirements on government agents before they can use such devices. The second category of surveillance technology—devices that allow government agents to gather public information more efficiently—has been treated quite differently. The courts have essentially applied *Katz* and concluded that since there is no reasonable expectation of privacy in public activity, the Fourth Amendment does not apply to a surveillance of public areas, regardless of the method used to conduct the surveillance. Thus, law enforcement agents can attach a homing device to contraband and electronically trace a suspect along all the public roads on which he drives—but if he takes the contraband inside his private home, the agents may not continue to trace its whereabouts without a warrant.[70] Likewise, law enforcement agents do not need a warrant to conduct photographic or video surveillance of public areas because individuals have no reasonable expectation of privacy in public.[71] Finally, planes and even helicopters can fly over private fields searching for contraband, since the content of those fields is visible to the public from commercial airliners.[72]

The Court's decision not to apply the Fourth Amendment to any kind of surveillance of public areas has drawn its share of criticism.[73] But although the Court may sometimes show questionable judgment in deciding when an individual does or does not have a "reasonable expectation of privacy" (the flyover cases come to mind),[74] the rule itself is a sound one

---

[69] *See, e.g., Torres*, 751 F.2d at 883-85.

[70] United States v. Knotts, 460 U.S. 276, 282 (1983).

[71] *See* Harris v. United States, 390 U.S. 234, 236 (1968).

[72] *See* Florida v. Riley, 488 U.S. 445, 450-52 (1989); California v. Ciraolo, 476 U.S. 207, 213-15 (1986).

[73] *See, e.g.*, Christopher Slobogin, *Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002) (arguing that courts should interpret the Fourth Amendment to recognize the right to be free from video surveillance in public, and suggesting that courts should set up some guidelines for the use of such surveillance).

[74] Arguably the flyover cases misinterpret the "reasonable expectations" test—just because a new technology (in this case airplanes) has made it *possible* for everyday civilians

since the *Katz* doctrine leads inevitably to the conclusion that the Fourth Amendment is silent if surveillance takes place in public. There are really only two other options, both of which require abandoning the *Katz* test. Courts could apply the Fourth Amendment's warrant requirements to *all* public surveillance—even to a police officer observing illegal activity firsthand on a public street—but this would be an absurd rule. But the only other option would be for courts to distinguish between different kinds of technology that are used during the surveillance, and it is difficult to find a principled reason for any such distinction. Presumably a law enforcement agent could use a flashlight or a set of binoculars without needing a warrant; would a warrant be required if the officer used a video camera or a satellite to monitor public activity? At what point would the public observation be considered a "search" under the Fourth Amendment? And more importantly, why would the police officer's observations of a public activity ever be considered a "search"? Instead of installing one hundred video cameras throughout a public park, the police could hire one hundred extra police officers and station them in exactly the same locations. Although this would arguably be more intrusive than the cameras (and certainly more expensive for taxpayers), the hundred officers would gather the same information, and their presence would clearly be permissible under the Fourth Amendment.

Thus, courts and legislatures have found it relatively easy to deal with the first two categories of new surveillance technologies. Not surprisingly, it is the third category—remedial surveillance methods to counteract the vast array of privacy-enhancing technologies used by everyday citizens—which has given courts and legislators the most problems. There are at least two reasons for this difficulty: first, the difficulty in finding the proper analogy within traditional forms of surveillance; and second, the difficulty of determining and then maintaining the proper balance between privacy and law enforcement needs in an entirely new context.

Unlike the first category of modern surveillance, in which it is relatively easy to link the new technology to a traditional form of

---

to fly over fields and see what is growing in them does not mean that the new technology has *changed society* to the extent that it has changed our reasonable expectations about what information is private. Airplanes can be contrasted with electric lighting, which not only makes observation of activities at nighttime possible but also routine and commonplace (unlike flying over fields and looking down into them, which is possible but hardly routine or commonplace). Thus, it would be fair to say we no longer have a reasonable expectation of privacy in what we do at night in public, but we should still have a reasonable expectation of privacy in the contents of our fenced-in fields. *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1332-35 (2002).

surveillance, courts struggle to determine similar analogies for responsive technologies—and occasionally, they choose an analogy that is disastrously inappropriate. This is because it is not clear at first how society itself views the privacy-enhancing technology—in the words of *Katz*, do we have a "reasonable expectation of privacy" when we use a certain technology to communicate, store data, or conduct certain activities in our home? And if we do, what showing should the government be forced to demonstrate before invading that privacy?

The most infamous example of a court's failure to understand this third category of surveillance technology came nearly eighty years ago, when the Supreme Court considered the constitutionality of wiretapping telephones in *Olmstead v. United States*.[75] Here was a classic case of responsive government surveillance: the telephone had been around for over fifty years, and it was by then commonly used by individuals to communicate private messages from the sanctuary of their own homes. Unsurprisingly, criminals such as Olmstead were also able to use this new technology to hide their activities from government investigators more effectively.[76] In response, law enforcement agents began using their own kind of new technology—an instrument that could be connected to the telephone wires outside a person's home and allow the user to eavesdrop on the conversation. The Court, in evaluating this responsive technology, had no obvious pre-technology analogy to fall back on—when an individual uses a telephone, should he be treated as though he sent a sealed letter from his house to another individual? Or should he be treated as though he were speaking privately to another individual in his private home? Or should he be treated as though he was standing on his rooftop, shouting his message to an individual miles away? To us today, the answer may seem obvious,

---

[75] 277 U.S. 438 (1928).

[76] The *Olmstead* case itself involved a vast conspiracy of seventy-two individuals who were importing and selling liquor in violation of Prohibition. *Id.* The Supreme Court noted that the conspiracy was of an "amazing magnitude":

> [The conspiracy] involved the employment of not less than 50 persons, of two sea-going vessels for the transportation of liquor to British Columbia, of smaller vessels for coastwise transportation to the state of Washington, the purchase and use of a branch beyond the suburban limits of Seattle, with a large underground cache for storage and a number of smaller caches in that city, the maintenance of a central office manned with operators, and the employment of executives, salesmen, deliverymen dispatchers, scouts, bookkeepers, collectors, and an attorney. In a bad month sales amounted to $176,000; the aggregate for a year must have exceeded $2,000,000.

Id. at 456. Olmstead himself was the "leading conspirator and the general manager" of the business. *Id.* Given the geographic scope and the number of personnel involved in the conspiracy, there is no doubt that the telephone assisted Olmstead greatly both in carrying out his criminal actions and in concealing these actions from law enforcement.

but the Court took some time to determine to what, exactly, telephone conversations and wiretapping were analogous.

First, the Court considered and rejected the analogy to a sealed letter, noting that there was a "constitutional provision for the Postoffice Department," and the government had a relationship with "those who pay to secure protection of their sealed letters."[77] Thus,

> It is plainly within the words of the [Fourth] [A]mendment to say that the unlawful rifling by a government agent of a sealed letter is a search and seizure of the sender's papers or effects. The letter is a paper, an effect, and in the custody of a government that forbids carriage, except under its protection.[78]

So was the interception of the phone call akin to entering the house and eavesdropping on a conversation between two people inside the house? The Supreme Court rejected this analogy as well since the law enforcement agents never went inside the house itself:

> Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house "or curtilage" for the purpose of making a seizure.[79]

Thus, the only analogy left was that of the individual broadcasting his telephone communication to the world with no expectation of privacy: "The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house, and messages while passing over them, are not within the protection of the Fourth Amendment."[80]

Congress eventually stepped in to protect telephone conversations from unregulated government wiretapping,[81] but the damage done by the Court's poor choice of analogy continued. The focus on property rights that laid the foundation for *Olmstead* muddled the Court's analysis in later cases involving first-category surveillance technology like electronic eavesdropping devices.[82] It was ultimately a first-category surveillance case—*Katz v. United States*—in which the Court was finally able to set out

---

[77] *Id.* at 464.

[78] *Id.*

[79] *Id.* at 466.

[80] *Id.*

[81] *See* Federal Communications Act of 1934, 47 U.S.C. § 605 (2000).

[82] *See supra* note 65.

a coherent doctrine for dealing with surveillance technology and the Fourth Amendment.[83]

But even in the post-*Katz* era, third-category surveillance technologies continue to give the Court problems. In 1979, the Court decided *Smith v. Maryland*,[84] another case in which the Court faced government use of responsive surveillance to counteract a criminal's use of privacy-enhancing technology. On March 5, 1976, Michael Smith robbed Patricia McDonough in Baltimore.[85] After the robbery, Smith began calling McDonough at her home, threatening her and using obscene language.[86] The police were able to trace Smith's license plate number, but still needed more evidence to link him to the various crimes.[87] Consequently, the police requested that the telephone company install a pen register on Smith's telephone line.[88] This device does not eavesdrop on the subject's telephone conversations, but instead merely records the phone numbers dialed for all the outgoing calls made from the telephone.[89] The pen register showed that Smith was indeed calling McDonough's house, and the police subsequently acquired a search warrant and recovered sufficient evidence to arrest Smith.[90]

Like Olmstead, Michael Smith was using privacy-enhancing technology to conceal his crimes from the police[91]—if he had lived one hundred years earlier and decided to threaten and verbally abuse his victim in her own home, he would have had to go to her house in person, an action that would have greatly increased his chances of being apprehended. After the first offense, the police would have almost certainly posted an officer near McDonough's house, and would likely have observed him returning to make future threats. But because Smith used a telephone, the police were

---

[83] Although *Katz* involved a defendant who was speaking on the phone, the device used by the law enforcement agents did not tap into the phone line but simply attached an electronic listening device to the outside of the phone booth the defendant was using. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring). Thus, the case did not involve responsive surveillance technology (such as a telephone wiretap) but simply first-category electronic bugging.

[84] 442 U.S. 735 (1979).

[85] *Id.* at 737.

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] *Id.*

[91] *Id.*

forced to respond with their own new technology—in this case, a device which could track outgoing telephone calls.[92]

As in the *Olmstead* case, the Court in *Smith* had to search for an analogy for the phone numbers of outgoing calls in order to determine whether law enforcement officers invaded a "legitimate expectation of privacy" when they used the pen register to obtain this information.[93] One obvious analogy to the phone numbers would be to the content of telephone calls themselves, which Congress deemed private information.[94] But the Court rejected this analogy, stating that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[95] The Court then quoted from one of its own recent decisions:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[96]

Instead, the Court reasoned that the phone numbers Smith dialed were akin to any other information that an individual turns over to a third party.[97] Smith could certainly not have any subjective expectation of privacy in these numbers, because "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[98] And society would not recognize any such expectation of privacy as "reasonable," because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[99] The Court then analogized the phone numbers dialed by Smith—information which he "voluntarily" gave to the telephone company—to financial information that a bank depositor gives to bank employees.[100] The Court also cited cases of

---

[92] *Id.*

[93] The Court made it clear that although the phone company installed the pen register, it did so at the request of the police, and so was acting as an "agent" of the police for the purposes of the Fourth and Fourteenth Amendment. *Id.* at 740 n.4.

[94] The Federal Communications Act of 1934 prohibited intercepting and disclosing any information passing over telephone lines. 47 U.S.C. § 605 (2000).

[95] *Smith*, 442 U.S. at 741.

[96] *Id.* (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

[97] *Id.* at 743-44.

[98] *Id.* at 742.

[99] *Id.* at 743-44.

[100] *Id.* at 744 (citing United States v. Miller, 425 U.S. 435, 442-44 (1976)).

giving financial information to an accountant[101] and giving information to an undercover government informant.[102]

It did not take long for this analogy—and the reasoning behind it—to prove to be dangerously short-sighted. Today everyone who sends an e-mail from anywhere in the world is "voluntarily" sending its contents to a number of Internet service providers as part of the communication process. Thus, under the *Smith* rationale, the Fourth Amendment does not protect the contents of e-mail communication.[103] Most modern communications networks cannot be utilized unless the user transfers information to organizations within the network's infrastructure,[104] and it is now obvious that the transfer of that required information is nothing like giving financial information to a bank or revealing information to a confidential informant. But this was not obvious to the Supreme Court in 1979, and as a result the Court chose a poor analogy to decide the case.

Courts and legislatures will continue to face this dilemma as they review the use of the growing number of responsive surveillance technologies. Although Congress has now stated that the contents of an e-mail message deserve the same level of privacy as a telephone call,[105] the wide diversity of privacy-enhancing technologies ensures that questions of first impression will continue to crop up. What level of protection should we give to information posted on a semi-public web site or a statement made in a password-protected chat room? What level of protection does information stored on network hard drives deserve? Even personal hard drives pose real challenges for courts. Is information on a hard drive analogous to information stored in a file cabinet? If so, is it "seizure" if the government merely copies the contents of the hard drive without taking it

---

[101] Couch v. United States, 409 U.S. 322, 323 (1973).

[102] United States v. White, 495 U.S. 745, 746-47 (1971).

[103] As was the case with wiretapping fifty years earlier, the United States Congress has stepped in to protect the content of e-mail messages. *See* Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986); 18 U.S.C. § 2510(12) (2000) (amending Title III so that the heightened standards apply to electronic messages as well).

[104] *See generally* Kerr, *Internet Surveillance*, *supra* note 15 (discussing the necessity of transferring information to an organization within three different communications networks: the postal service, the telephone, and the Internet). One example of this is web surfing. *See id.* at 613 n.29. In order to visit a website, a user types the website address into the browser. *Id.* The computer then sends out signals to the remote computer that hosts the website and the website sends a signal back. *Id.* In other words, "[c]ommunications networks require partial (and sometimes total) disclosure to the network provider" to help the provider deliver the contents. *Id.* at 628.

[105] *Id.*

away? Is it a "search" if the government merely retains a copy of the contents without looking at them?[106]

Thus, courts frequently struggle to analogize this third category of surveillance to a traditional search. And in the absence of such an analogy, it is difficult to balance an individual's privacy rights with law enforcement's duty to investigate crime. Fourth Amendment jurisprudence has always involved striking the proper balance between these two competing needs, and in the case of responsive surveillance, the individual (and the potential criminal) has already changed that balance by using the privacy-enhancing technology in the first place. Thus, courts must determine how much privacy an individual deserves when she is talking on the telephone, storing information in a network hard drive, buying a book over the Internet, or uploading pictures to a webpage accessible only to friends and family members. And on the other hand, how badly will it interfere with law enforcement officers' efforts if their attempts at counter-measures are curtailed? The Supreme Court struck the wrong balance in *Olmstead* when it misunderstood the level of privacy that society demanded for individuals who speak on the telephone. It struck the wrong balance again in *Smith* when it failed to anticipate the nature of developing communications networks, thus giving the government too much power to intercept private communications.

V. THE PROPER BALANCE

One prominent Fourth Amendment scholar argues that the Fourth Amendment is a "mechanism for regulating the information flow between individuals and the state,"[107] and that privacy is merely a "vital byproduct of Fourth Amendment rules, not its goal."[108] But in the wake of *Katz*, privacy must be considered the focus of any Fourth Amendment inquiry—in other words, it is more accurate to state that the Fourth Amendment is a mechanism for regulating the flow of *private* information between

[106] Professor Orin Kerr dealt with these questions in the context of digital technology searches, noting that under current precedent (derived from a pre-digital era), law enforcement agents do not commit a search or a seizure if they copy the contents of your hard drive and store the contents on their own computers. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 558-60 (2005). Kerr notes that this is a "troublesome result." *Id.* at 560. "The idea that the government could freely generate copies of our hard drives and indefinitely retain them in government storage seems too Orwellian—and downright creepy—to be embraced as a Fourth Amendment rule." *Id.*

[107] *Id.* at 535.

[108] *Id.* at 585.

individuals and the state.[109] The level of regulation (in other words, the level of protection) is dependent upon the level of privacy that we want to give to the information. If the information is intimately private, the Fourth Amendment should afford it the greatest level of protection and require a significant showing on the part of the government before allowing law enforcement to gather it—regardless of the type of technology used to gather the information. Courts have already followed this path in applying the protections of the Fourth Amendment to such hyper-intrusive searches as video cameras in private spaces,[110] surgical procedures to remove evidence from a defendant,[111] and no-knock search warrants.[112] They should also apply this standard to intercepting telephone calls, intercepting e-mail communications, and eavesdropping electronically. Indeed, courts likely would already have done so if Congress had not already created a heightened standard through statute.[113] The next level down would be gathering information in which the individual has a reasonable expectation of privacy, but which does not involve intercepting personal conversations or secretly monitoring activities inside one's one home—that is, gathering private but not intimately private information. In these cases, mere probable cause should be sufficient to overcome the individual's privacy interests. This standard would apply for searches of most private areas, whether information is stored in file cabinets or hard drives. And finally,

---

[109] The *Katz* standard states that government surveillance is a "search" if it infringes on the target's "reasonable expectation of privacy." United States v. Katz, 389 U.S. 347, 360 (1967) (Harlan, J., concurring). The language of the Fourth Amendment does not focus solely on information generally, but also on private information: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

[110] *See, e.g.*, United States v. Torres, 751 F.2d 875, 883-84 (7th Cir. 1984) (interpreting the Fourth Amendment to require the government to meet the heightened Title III requirements before video surveillance can be authorized).

[111] *See, e.g.*, Winston v. Lee, 470 U.S. 753, 759-62 (1985) (setting out special factors that courts should consider in determining whether a surgical procedure on the defendant is "reasonable").

[112] *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 929-36 (1995) (acknowledging that a silent-entry search warrant is a heightened intrusion and authorizing such a warrant only if the government makes a showing beyond probable cause, such as proving that silent entry is necessary to prevent violence, or that evidence would likely be destroyed if notice were given); *see also* Richards v. Wisconsin, 520 U.S. 385 (1987). For an overview of the legal standards governing each of these types of "hyper-intrusive" searches, see generally Ric Simmons, *Can* Winston *Save Us from Big Brother? The Need for Judicial Consistency in Regulating Hyper-Intrusive Searches*, 55 RUTG. L. REV. 547 (2003).

[113] *See, e.g.*, 18 U.S.C. §§ 2510-22 (2000) (codifying both Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which regulates interception of oral and wire communications, and the Electronic Communication and Privacy Act of 1986, which regulates interception of electronic communications).

there should be one (or more) categories of information that are only semi-private, which the Fourth Amendment should regulate but that would require a lesser showing than probable cause—for example, phone numbers that are dialed on the telephone, addresses of e-mails that are sent, and information posted on password-protected blogs. This is information that is not fully public, but that individuals are aware can be seen or recorded by others. And finally, if the information is public, the Fourth Amendment does not regulate the information flow at all.

Others have proposed such a "sliding scale" of Fourth Amendment and statutory protection before.[114] The critical (and challenging) task for courts in the context of regulating responsive technology is determining the appropriate level of privacy for the various kinds of communication and

---

[114] Professor Kerr has compiled a comprehensive categorization of the existing legal thresholds for government surveillance:

> (1) No Legal Process: The government can acquire the information without process or order;
>
> (2) Subpoena: The government must obtain a subpoena, such as a grand jury subpoena, duces tecum or an administrative subpoena, before acquiring the information. The subpoena compels the provider to disclose the information to the government;
>
> (3) Relevance Court Order: The government must obtain a court order before acquiring the information but can obtain the order merely by certifying to the court that the information likely to be obtained is relevant to a law enforcement investigation;
>
> (4) Articulable Facts Court Order: The government must obtain a court order before acquiring the information, and to obtain the order must offer specific and articulable facts establishing reasonable grounds to believe the information to be obtained is both relevant and material to an ongoing criminal investigation;
>
> (5) Probable Cause Search Warrant: The government must obtain a search warrant before acquiring the information. The search warrant requires "probable cause," which in the criminal context means that the government must offer facts establishing a likelihood that a crime has occurred and that evidence of the crime exists in the location to be searched;
>
> (6) "Super" Search Warrant: The government must obtain a special search warrant before acquiring the information that adds the threshold requirements beyond those of ordinary search warrants (e.g. requiring the government to exhaust all other means of obtaining the information, requiring special authorization); and
>
> (7) The Government May Not Acquire the Information by Any Legal Process: The law may forbid the government from acquiring the information regardless of the legal process.

Kerr, *Internet Surveillance*, *supra* note 15, at 620-21 tbl.2.

Thus, courts and legislatures have already categorized many different levels of protection for information, and the task for future courts and legislatures is to decide where to place any new method of surveillance. In my proposal, anything occurring in the public belongs in category (1), receiving no protection; intimate private activity belongs in category (6), which requires a showing greater than a warrant; standard private activity belongs in category (5), which merely requires a warrant, and the "semi-public" information would be placed in categories (2)-(4), depending on how private the information actually is.

data storage used by individuals in a world of privacy-enhancing technology.

If we properly focus on *private* information, we must first acknowledge that standards of privacy have changed in the twenty-first century.[115] Individuals put an unprecedented amount of private information into the public arena—both intentionally and unintentionally. Many individuals choose to use what we have termed "privacy-enhancing technology" in precisely the opposite way—to make their private lives more public. Diaries which were once kept hidden under mattresses are now posted on blogs, along with personal pictures and messages from friends. Telephone conversations that used to occur in homes or private phone booths are now carried out on the street and in malls, stores, and other public areas. This intentional use of technology to reduce one's own privacy diminishes the difficulty of the Fourth Amendment analysis: if an individual willingly discloses private information about himself and thereby makes it available to law enforcement, the conflict between the individual's privacy and law enforcement's need to gather information disappears.

Of course, much of the loss of privacy in our society is not due to our own personal choice. Because of the ease of information transfer in modern life, records that used to be public only in theory are now public in practice—from how much you paid for your house to how much money you gave to your Congressman's campaign fund.[116] Meanwhile, companies buy and sell lists of consumer purchases and preferences, maintaining this

---

[115] Shaun Spencer has suggested that as advances in technology have made more intrusive surveillance possible, individuals' expectations of privacy have incrementally diminished. *See* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002). For example, when employers monitor employees' telephone and e-mail use in the workplace, they diminish the expectation of privacy in the workplace. *Id.* at 860. Likewise, if merchants continually sell consumers' information, they diminish consumers' expectation of privacy in that personal information. *Id.* According to Spencer's theory, this encroachment and erosion "proceeds so gradually that it seems like the inevitable price of progress." *Id.* at 861.

[116] For example, in Franklin County, Ohio, an interested neighbor (or any other person in the world) can go to the Franklin County Auditor's website and simply type in his neighbor's name to discover a myriad of information about his neighbor's home, including the price for which his neighbor bought the home and the current appraisal. *See* Joseph W. Testa, Franklin County Auditor, http://franklin.governmaxa.com/propertymax/rover30.asp (last visited Apr. 21, 2007). To learn who is contributing to a federal political candidate, one need only visit the Federal Election Commission's website and either type in the candidate's name or type in an individual's name to see to whom that individual is contributing. *See* Campaign Finance Data Disclosure Search, http://www.fec.gov/finance/disclosure/disclosure_data_search.shtml (last visited Apr. 21, 2007).

commercial yet personal information on vast computer databases.[117] Many social commentators have decried this loss of privacy—but again, the problem is not caused by new technology, but by the initial determination of what kind of information should be public and what should be private. It may be troubling that government agents can more easily get access to public information when it is posted on the web instead of buried in a file cabinet in a remote county courthouse—but the response to this concern is not to limit technology. Instead, perhaps we need to change the law to limit the amount of public information that is available. And if the ease of compiling and transferring consumer information between companies has led to abuses of the information, such transfers could be banned.

As it turns out, society seems to be moving in the opposite direction—changing the laws to make more and more information public. For example, criminal records have traditionally been kept confidential—but now individuals who have been convicted of a sex offense have their names posted on public websites, along with their address and details of their crime,[118] while drunk drivers are forced to purchase distinctive license plates so that everyone on the road knows of their crime.[119]

In the end, the threat to privacy is not caused by the advanced surveillance technology being used by the government, but by the inability of courts (and, to a lesser degree, legislatures) to determine the appropriate level of privacy for the different kinds of information being gathered. Ironically, courts and policymakers find it relatively easy to set this level of privacy for the most intrusive kinds of technology—our first category—because the information being gathered is unambiguously intimate. The challenge arises when individuals use privacy-enhancing technology to make formerly public information private or quasi-private. When law enforcement attempts to collect that kind of information, it is difficult to tell

---

[117] Tom Zeller, Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1 (discussing "big data brokers" that collect and sell consumer information).

[118] Federal law requires each state to implement such a sex offender registry and to participate in the national sex offender registry. 42 U.S.C. § 14071. The national sex offender registry, like most state registries, is available online for public viewing. *See* Dru Sjodin National Sex Offender Public Registry, U.S. Dept. of Justice, http://www.nsopr.gov (last visited Apr. 21, 2007) (enabling a person to look up sex offenders by zip code or other information and view the offender's name, address, picture, classification, offenses, and even the offender's "victim preferences"). Some states go beyond the minimum federal mandate and require local authorities to actively inform the community of sex offenders living in that community by going door-to-door or mailing information about the offender directly to the affected community. *See, e.g.*, D.C. CODE § 22-4011 (2006) (allowing active notification); N.J. STAT. § 2C:7-8c (2006) (requiring active notification to the affected community when risk of re-offense is high).

[119] *See, e.g.*, OHIO REV. CODE § 4503.231 (West 2006).

what level of protection it deserves. Courts and legislatures will have to continue to deal with these questions on a case-by-case basis, and mistakes will be inevitable due to rapidly changing technological and social norms. Judges and policymakers, however, will be more likely to come to the right conclusions if they begin their inquiry by considering the type of information that is being gathered and then determine the appropriate level of privacy for that type of information.

There are two relatively clear reforms that should be made. The first is to re-visit the *Smith v. Maryland* doctrine, which currently gives no Fourth Amendment protection to any communication (other than a traditional letter) which is entrusted to a third party in the communications network. Even though Congress has stepped in to cover Internet transmissions and stored messages, there is no reason why the Fourth Amendment itself should not also protect these communications, which most of society views as deserving of the highest level of privacy.[120]

At the other extreme, some privacy-enhancing technology makes it possible to hide information from law enforcement agents so effectively that they can *never* obtain the information they seek, regardless of how badly they need it or what kind of showing they make to a judge. In these situations, just as when surveillance technology makes it impossible to hide information from the government, Congress should intervene to maintain the proper balance between an individual's right to privacy and the needs of law enforcement. The current level of encryption technology makes it possible for citizens and criminals to hide all of their stored data and mask the contents of all of their communication,[121] thus enabling individuals to obtain a level of privacy which we would almost certainly not want to create by law if we had a choice: complete immunity from government surveillance, regardless of the showing made by the government. It would make sense to restore the balance by requiring everyone who uses a complex encryption device to deposit the key to the encryption in escrow[122]—law enforcement agents could not gain access to the key unless they made a sufficient showing to a court, which would depend on the level of privacy that the encrypted information warranted.

---

[120] Bellia, *supra* note 18, at 1458 (arguing that government agents should have to obtain a warrant before seizing e-mail messages stored by a third party).

[121] *See infra* notes 60-61 and accompanying text.

[122] *See* D. Forest Wolfe, Comment, *The Government's Right to Read: Maintaining State Access to Digital Data in the Age of Impenetrable Encryption*, 49 EMORY L.J. 711, 719 (2000).

VI. OTHER EFFECTS OF TECHNOLOGY ON PRIVACY

In addition to enhancing the privacy of many everyday activities and increasing the surveillance power of law enforcement, technology has affected privacy in a number of other ways. Although at least one of those ways has indirectly led to a loss of privacy, other effects have the potential to result in greater protections from government intrusion.

A. THE TRUE THREAT THAT TECHNOLOGICAL ADVANCES POSE TO PRIVACY

In one sense, new technology has indirectly caused a loss of privacy, but not in the way that most people realize. Simply put, technology has exponentially increased the damage done by certain crimes. A child pornographer who wants to distribute his goods in the past was limited by very real practical constraints as to the number of pictures he could distribute and the number of people to whom he could distribute them. Today, computers and e-mail make these limits obsolete. A teenage vandal in past eras might break store windows or spray-paint graffiti on walls. Today, that same teenager might write a computer virus and cause thousands or millions of dollars worth of damage.[123] An anarchist in the nineteenth century might seek to assassinate a president or plant dynamite in an opera house[124]—his twenty-first century counterpart has the ability to destroy cities with a nuclear weapon or poison an entire society with chemical or biological agents.

The political reaction has been predictable: the increased potential for damage caused by these new technologies has led policymakers to conclude that the government should be given more power to investigate suspected criminals. Some of this reaction is a legitimate response to the new dangers, while some is hypercharged political posturing. The result is a significant shift in the balancing act between individual privacy rights and law enforcement's power to investigate crime. For example, the threat of international terrorism is so dangerous that the federal government began tracing all of our outgoing international telephone calls without court approval.[125] In a recent pair of cases, the threat of terrorism on public transportation has led the Second Circuit to broaden the "special needs"

---

[123] One of the most destructive crimes in history was the creation of the "I Love You" virus in 2000, which infected 45 million computers and caused an estimated $10 billion of damage in this country alone. *See* Cybercrime: Piercing the Darkness, http://library.thinkquest.org/04oct/00460/ILoveYou.html (last visited Apr. 21, 2007).

[124] *See For Jihadist, Read Anarchist-The anarchists*, ECONOMIST, Aug. 20, 2005.

[125] Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2006, at A1.

exception to the probable cause and warrant requirement of the Fourth Amendment, allowing suspicionless searches and seizures of all riders on subways and ferries.[126] Of course, this shift towards increased government power is evident everywhere, not just in the realm of the Fourth Amendment—the same terrorist threat led the federal government to begin holding suspects in detention without a charge, denying them access to lawyers, and trying them in special tribunals with different rules of evidence in order to protect "national security."[127]

B. THE PROMISE OF THE NEXT GENERATION OF SURVEILLANCE TECHNOLOGY

Although it may seem counterintuitive, improved surveillance technology could actually help to increase individual privacy in the future in two ways, by allowing for more refined and less intrusive searches and by increasing the monitoring of law enforcement.

1. Raising the Standards of Reasonableness

Newer generations of surveillance technology should be able to be far more discriminating in what they are searching for, and to search for it more quickly and less invasively—thus allowing for narrower and less intrusive searches. We already have examples of surveillance technology that conducts authorized searches more quickly and with less invasion of privacy than traditional methods—for example, metal detectors and x-ray machines at airports. In these contexts, the law enforcement agent has the right to search the individual with a more time-consuming and more invasive pat-down, and also has the right to sift through the contents of a suitcase one by one. By using this new technology, the agent actually *enhances* the individual's privacy.

The potential for more narrowly targeted searches is even greater in the digital realm. Instead of manually searching through a target's e-mail account and reading all of the incoming and outgoing communications, the government can use software that can sift through and copy only those messages with incriminating words or specific names, thus letting the innocent ones pass through without any human ever reading them.[128] As

---

[126] Cassidy v. Chertoff, 471 F.3d 67 (2d Cir. 2006) (ferries); MacWade v. Kelly, 460 F.3d 260 (2d Cir. 2006) (subways).

[127] *See, e.g.*, Linda Greenhouse, *Justices Are Urged to Dismiss Padilla Case*, N.Y. TIMES, Dec. 18, 2005, at A14.

[128] The government first created its own software for this purpose—the much-maligned "Carnivore" device, which was re-named "DCS1000" in 2001. *See* Jennifer DiSabatino, *FBI's Carnivore Gets a Name Change*, COMPUTERWORLD, Feb. 12, 2001,

technology progresses, law enforcement may begin using surveillance tools that are so narrowly targeted that they only alert their human user if they sense illegal activity, much like a drug-sniffing dog only reacts when contraband is present. Examples of these "binary" surveillance tools are a gun detector that can see through clothing but whose only output is a light that comes on when the unmistakable outline of a gun is detected; or sophisticated software that can sift through e-mail messages and detect the presence of child pornography, at which point it will copy the image and the sender's e-mail address.[129]

These new devices will increase privacy (since they are less likely to intercept innocent communications or reveal innocent private communication) but not decrease law enforcement's power to investigate—in fact, they will make investigations more efficient. A logical next step in the development of Fourth Amendment jurisprudence might be to adjust the determination of what is a "reasonable" search based on the surveillance technologies available—a broader, more invasive search which was permissible decades ago may no longer be reasonable if law enforcement has access to devices which can make the search narrower or less invasive. In fact, the Title III requirements for wiretapping and electronic eavesdropping already lay the foundation for this kind of shifting standard, since in order to receive such an order, government agents must demonstrate inter alia that they are conducting the surveillance in such a way as to minimize the interception of irrelevant information.[130] For example, if a government agent is seeking a Title III order to intercept all the messages from an e-mail account, a judge may well ask why the agent cannot instead hook up a device that will sift through the messages mindlessly and only retain those that are incriminating.

Unfortunately, outside of the Title III context, in which least intrusive means and minimization are built into the statutory test, courts so far do not seem to be sympathetic to these arguments. In a recent Second Circuit case, commuters challenged the U.S. Coast Guard's practice of randomly

---

http://www.computerworld.com/softwaretopics/software/story/0,10801,57633,00.html. DCS1000 was attached to a specific Internet service provider, where it hunted for e-mail messages to and/or from the target individual. *Id.* When it found an e-mail message that met its programmed criteria, it copied the e-mail and stored it before sending it on its way. *Id.* In 2005, the FBI abandoned the use of DCS1000 and now uses commercially available software. *See FBI Ditches Carnivore Surveillance System*, ASSOCIATED PRESS, Jan. 18, 2005, *available at* http://www.foxnews.com/story/0,2933,144809,00.html. To use DCS1000 or any of its commercial replacements, the government must obtain a Title III order. *See* 18 U.S.C. §§ 2510-22 (2000).

[129] *See* Simmons, *supra* note 74, at 1351-57.

[130] 18 U.S.C. § 2518(5).

searching carry-on bags and vehicles on public ferries.[131] Plaintiffs argued that metal detectors could be used as a less intrusive way of satisfying the government's goal of protecting the ferries from terrorists.[132] The Second Circuit rejected that argument, noting that, "The Supreme Court has repeatedly stated that reasonableness under the Fourth Amendment does not require employing the least intrusive means to accomplish the government's ends."[133] In other words, the "reasonableness" of a search is unrelated to whether the government could have accomplished the same goal using a less intrusive technology.

Ultimately, perhaps, the widespread availability of less intrusive and more narrowly tailored methods of surveillance may lead courts to include these factors in their tests for reasonableness. Until then, it will be up to legislatures to create such requirements, either by directly mandating the method of surveillance which is appropriate under certain conditions, or by creating statutes like Title III that expressly cite these as factors which must be satisfied before a search can be conducted.

2. Watching the Watchers

The second way in which new surveillance technology can enhance privacy is by using technology to monitor the activities of law enforcement. A recurring problem in regulating the practice of law enforcement agents in the criminal procedure context is not the legal rules that govern the situation but simply determining exactly what happened. Most fact patterns in disputes about appropriate police conduct involve two witnesses—the police officer and the suspect—and in most cases the suspect's version of the story will carry very little weight for the judge who is deciding a suppression motion. This has led to at least the potential (and in some situations the reality) of abuse on the part of law enforcement officers. If a police officer testifies that he read the *Miranda* rights to the defendant before the interrogation began, or that the defendant failed to ask for a lawyer before confessing to the crime, there is generally little that a defendant can do to persuade the judge otherwise. This is not to say that most police officers lie about their actions during an interrogation, but rather that the lack of effective monitoring inevitably leads to suboptimal conduct on the part of the police.

Nowhere in criminal procedure is this potential for abuse greater than in the search and seizure context, because officer discretion is greatest at

---

[131] *Cassidy*, 471 F.3d 67.

[132] *Id.* at 80.

[133] *Id.* (citations and internal quotations omitted).

that stage of the investigatory process. Police officers pull over cars after allegedly observing erratic driving; they arrest suspects after allegedly seeing the suspect drop a bag of drugs onto the sidewalk; they conduct a *Terry* stop on the basis of alleged suspicious activity. Many of the most scathing critiques of law enforcement conduct have nothing to do with the legal standards themselves; rather, they center on the serious potential for violation of these standards and subsequent perjury on the part of the law enforcement officer.[134] Unmonitored police conduct in this area poses a significant threat to individual privacy, especially among the poor and minority groups, since they tend to live in high crime areas where police are more likely to bend the law in order to further their investigation.

New technologies offer great promise in this area. For example, in the context of interrogations, introducing a tape recorder or video camera into the interrogation room can serve as an effective way of monitoring police conduct by deterring most abuses and detecting those that do occur. In the search and seizure context (the context most applicable to individual privacy), there is not yet a technological "magic bullet" which can ensure police compliance—but there is progress being made. More and more police cars are being equipped with dashboard video cameras, so that the allegedly erratic or reckless driving of a suspect (and the police conduct during the traffic stop itself) can be recorded and thereby monitored. In fact, as video technology gets cheaper and smaller, it will soon become feasible to record everything a police officer driving a squad car sees and hears—as well as everything that police officer does during the traffic stop. The next step would be to develop some way of making an audio and video record of *all* police observations and conduct while on duty, whether in a squad car, walking a beat, or responding to a call inside a home or a store—for example, some kind of miniature video recorder attached to the uniform of every officer. The technology for making these records for each of the million-plus law enforcement officers does not yet exist, but such a possibility is not inconceivable within ten or twenty years. More to the point, there is no reason why we would *not* want to do this once it becomes technologically and economically feasible. Such a policy would prevent

---

[134] *See* Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1041-48 (1996) (discussing surveys and other data which support the notion that police, with prosecutors' knowledge, regularly lie in warrant applications and in suppression hearings to cover up lack of probable cause or failure to properly follow *Miranda* rules). One set of commentators, in response to evidence suggesting a high rate of police "testilying," suggested liberalizing rules of evidence to allow defendants more ability to impeach police officers' testimony. *See* Gabriel Chin & Scott Wells, *The "Blue Wall of Silence" as Evidence of Bias and Motive to Lie: A New Approach to Police Perjury*, 59 U. PITT. L. REV. 233, 272-99 (1998).

abuses on the part of law enforcement, provide judges at the suppression hearing a clear, neutral factual record of how the investigation was conducted, and—not incidentally—provide excellent substantive evidence for the actual criminal trial itself.

Just as improved surveillance technology can lead to more narrowly targeted surveillance, these monitoring technologies can lead to improved police conduct, thus enhancing individual privacy. Once again, we can encourage steps in this direction by enacting laws which promote or require law enforcement to use such devices. In the interrogation context, for example, at least four states have required that all custodial interrogations must be electronically recorded.[135] Legislatures and courts can and should begin to create the same kind of requirements for the search and seizure context, thus ensuring that law enforcement officers follow the laws that already exist.

VII. CONCLUSION

It is true that in some ways, technology has given the government the ability to invade our privacy in new and troubling ways. Listening and even looking through walls; flying over our open fields and backyards; implanting hidden microphones and cameras in our homes and offices—in all of these ways, emerging technology has given the government a great advantage in its search for criminal activity and made everyone a little less secure in their homes. It is also true that other kinds of technology have allowed the government to conduct otherwise onerous public surveillance much more quickly and efficiently, thus making our conduct in public and our public information more vulnerable to government monitoring.

But in many other ways, technology has increased our privacy quite dramatically, and what at first seem to be insidious methods of eavesdropping and snooping—wiretapping phones, monitoring e-mails, searching computer hard drives—are actually simply remedial measures on the part of the government in an attempt to maintain the appropriate balance between individual privacy and effective law enforcement.

When evaluating the current laws regulating surveillance technology, we should first ask: What level of privacy does the type of information deserve? Privacy-enhancing technologies muddle this question a bit, since they create methods of data storage and communication that have never been seen before and are therefore hard to categorize. But commentators

---

[135] Steven A. Drizin & Marissa J. Reich, *Heeding the Lessons of History: The Need for Mandatory Recording of Police Interrogations to Accurately Assess the Reliability and Voluntariness of Confessions*, 52 DRAKE L. REV. 619, 620 (2004) (noting that Alaska, Minnesota, Illinois, and Maine require the recording of all custodial interrogations).

who worry about new surveillance technology eroding our privacy should keep a couple of points in mind. First, thanks in large part to new technologies, by most measures we have more privacy today than at any other time in history. Second, as technology has changed the way we communicate and store information, as well as the way in which the government can spy on our behavior, the law has adapted to these changes, usually weighing in to protect the privacy of innocent civilians and would-be criminals.

There are some glaring exceptions to this rule, particularly with regard to responsive surveillance technology, when courts have struggled to determine the appropriate level of privacy for a new method of communication. But in other areas, such as encryption technology, anonymous e-mail accounts, and the use of disposable cell phones, current technologies create much greater levels of privacy than we have seen in the past, allowing individuals to keep communications and data hidden from the government to an unprecedented degree and perhaps requiring government intervention to *reduce* the amount of privacy provided.

Finally, courts and legislatures should be aware of the ways to encourage the use of technologies which will both increase privacy and increase security. Stricter requirements for certain kinds of surveillance can force law enforcement officers to use technology that provides more narrowly tailored and less intrusive searches, while increased monitoring of law enforcement behavior can prevent police misconduct as well as provide better evidence of criminal activity. Contrary to popular belief, new technologies are not the cause of eroding privacy in our society—but if prodded in the right direction, they could be a big part of the cure.