2001

What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance

Mark G. Young

Recommended Citation
Available at: http://ir.lawnet.fordham.edu/flr/vol70/iss3/12

This Article is brought to you for free and open access by FLASH: The Fordham Law Archive of Scholarship and History. It has been accepted for inclusion in Fordham Law Review by an authorized editor of FLASH: The Fordham Law Archive of Scholarship and History. For more information, please contact tmelnick@law.fordham.edu.
NOTE

WHAT BIG EYES AND EARS YOU HAVE!: A NEW REGIME FOR COVERT GOVERNMENTAL SURVEILLANCE

Mark G. Young*

Americans do not like the idea of being secretly watched; indeed, they have grown up with the idea that one of the hallmarks of a free society is that people do not have to take a walk in the woods to have private conversations.¹

INTRODUCTION

Several notable events in the past months have renewed with great urgency and vigor a long-standing national debate about the proper balance between the government's powers to maintain order and security and citizens' liberties as provided in the Constitution. A few days after the Super Bowl in January 2001, newspapers and television programs revealed that the Tampa Police Department, in conjunction with the National Football League and other law-enforcement agencies, surreptitiously scanned the faces of all the people who attended the game and, after converting certain measurements of their faces into sophisticated algorithms, relayed this information to computers which compared these algorithms to a database of known or suspected terrorists.² While there were those who voiced support for this surreptitious surveillance of Super Bowl patrons,³ several

---

* J.D. Candidate, 2002 Fordham University School of Law. This Note is in honor of my brother and with deep appreciation, admiration, and affection for my wife and parents. I also owe a debt of gratitude to several colleagues on the *Fordham Law Review*

2. Louis Sahagun & Josh Meyer, *Secret Cameras at Super Bowl Scanned Crowd for Criminals*, L.A. Times, Feb. 1, 2001, at A1 ("In a command post at Raymond James Stadium in Tampa, Fla., the digitized images of fans and workers were cross-checked against files of local police, the FBI and state agencies at the rate of a million images a minute."). Although the faces entered into the database were apparently for terrorist suspects, the 19 matches that resulted from this surveillance were mostly pickpockets and con artists. See id.
3. See John D. Woodward Jr., *And Now, the Good Side of Facial Profiling*,
prominent newspapers ran editorials sharply denouncing such a practice.4

On September 11, 2001, four commercial airplanes were hijacked—two of which were crashed into the World Trade Center and one into the Pentagon.5 In the wake of the tragedy of September 11, the attitude toward the propriety of widespread surveillance seems to have markedly changed.6 On the belief that vigorous surveillance is necessary to prevent similar future calamities, Congress and President George W. Bush launched proposals for expanding the powers of federal agents in several important respects, including the authority to conduct electronic surveillance.7 Although muted, there were also

Wash. Post, Feb. 4, 2001, at B4 (advocating a pragmatic, middle-ground approach to surveillance which recognizes the value of these techniques but which also attempts to minimize their privacy-intruding aspects).

4. See, e.g., Super Bowl Snooping, supra note 1; Super Day for Big Brother, Editorial, L.A. Times, Feb. 2, 2001, at B8. The New York Times published two letters to the editors that reflected this schism between views. See At the Game, Big Brother is Watching You, Letters to the Editor, N.Y. Times, Feb. 6, 2001, at A18. One letter-writer acquiesced in the need for the intrusion given the risk of terrorism, stating that “Terrorism is a threat of major proportions, and distasteful as it seems, surveillance of public places and tools of facial character recognition may be necessary.” Id. The other was distressed by the affront to the notion of privacy and the inability to “observe the observers.” This person stated: “When video and other high-tech equipment are used by government agencies to randomly and surreptitiously monitor citizens while they are out in public (and worse, capture their images), the expectation of being able to ‘observe the observers’ is violated.” Id.


6. Cf. Neil Munro & Peter H. Stone, A Tougher Balancing Act, 33 Nat'l J. 2852 (2001) (noting how the attack will likely lead to pressure and calls for increased law-enforcement capabilities, particularly in the area of surveillance, and stating that “[p]rivacy advocates now face a potentially insurmountable political problem: a wave of public disgust and fear that will likely help boost police budgets and surveillance authority nationwide”); David Barstow, Envisioning an Expensive Future in the Brave New World of Fortress New York, N.Y. Times, Sept. 16, 2001, at 16 (discussing how attitudes about security are likely to change); Marcia Coyle & Bob Van Voris, A New Landscape as U.S. Seeks to Protect Itself, Nat'l L.J., Sept. 24, 2001, at A4 (discussing likely changes in attitudes about security vis-à-vis privacy, and possible legislative measures); Linda Greenhouse, The Clamor of a Free People, N.Y. Times, Sept. 16, 2001, § 4 (Week in Review), at 1 (noting that due to recent events the balance between security and liberty “will now be recalibrated to reflect both new realities and new perceptions”).

7. See Lizette Alvarez, Spying on Terrorists and Thwarting Them Gains New Urgency, N.Y. Times, Sept. 14, 2001, at A17 (reporting the Senate's late-night passage two days after the attacks of an amendment with significant implications for the law of surveillance that was attached to an appropriations bill for the Department of Justice); Jonathan Krim, Anti-Terror Push Stirs Fears for Liberties: Rights Groups Urge To Seek Safeguards, Wash. Post, Sept. 18, 2001, at A17 (reporting the introduction by Attorney General John Ashcroft of a revised and expanded anti-terrorism legislative proposal). See infra notes 271-83 and accompanying text for a further discussion of these legislative proposals.

Shortly after passage of the USA Patriot Act, Attorney General John Ashcroft authorized the Bureau of Prisons to eavesdrop on communications between “inmates” and their attorneys upon a “specific determination that such actions are
strong reactions against these legislative measures and calls for the protection of civil liberties.\textsuperscript{8}

These conflicting views illustrate the battle as old as the country over the proper balance between granting the government authority to maintain order in society and restraining the government from reasonably necessary in order to deter future acts of violence or terrorism.” National Security; Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. 55,062, 55,064 (Oct. 31, 2001) (amending 28 C.F.R. pts. 500, 501); see also Neil A. Lewis & Christopher Marquis, \textit{Longer Visa Waits for Arabs; Stir over U.S. Eavesdropping}, N.Y. Times, Nov. 10, 2001, at A1. Characterizing the regulation as an interim rule and invoking the good-cause and the foreign-affairs exceptions to the notice-and-comment requirement of the Administrative Procedure Act, see 5 U.S.C. § 553(a)(1), (b)(B) (1994), Attorney General Ashcroft implemented the rule without public comment. 66 Fed. Reg. at 55,064-65. Although enacted to deter terrorism, the new rule potentially permits eavesdropping on attorney-client communications in other situations. For one, the regulation defines “inmate” broadly to include “all persons in the custody of the Federal Bureau of Prisons or Bureau contract facilities... D.C. Code felony offenders; and persons held as witnesses, detainees, or otherwise.” 66 Fed. Reg. at 55,065 (amending 28 C.F.R. § 501.1(c)) (emphasis added). Second, the standard articulated in the rule is broad and vague: “[A]ll communications between inmate and attorneys may be monitored, to the extent determined to be reasonably necessary for the purpose of deterring future acts of violence or terrorism.” 66 Fed. Reg. at 55,066 (amending 28 C.F.R. § 501.3(d)). Third, it is not clear that this provision is subject to any time limitations, since section 501.3(d) does not explicitly subject attorney-client eavesdropping to the time limitations for other “special administrative measures” contained in section 501.3(a). \textit{See id.} Nevertheless, the regulations require that the inmate and attorney be notified of the surveillance prior to its initiation, unless otherwise authorized by a court. \textit{Id.}

\textit{8. See Krim, supra note 7 (“A coalition of public interest groups from across the political spectrum has formed to try to stop Congress and the Bush administration from rushing to enact counterterrorism measures before considering their effect on Americans’ privacy and civil rights.”); see also Greenhouse, supra note 6 (querying “at what point do security measures start to corrode the very society they are designed to protect?” and noting that times of crisis, “deep insecurity, grief and anger,” which most test our commitment to the ideals of liberty, “in fact have often evoked the worst of our national instincts”); The Home Front Security and Liberty, Editorial, N.Y. Times, Sept. 23, 2001, § 4 (Week in Review), at 16 (stating that the legislative measure proposed by the Bush administration after the attack contained some useful steps, but warning that “many of the ideas being shopped by the Bush administration would reduce constitutional protections with no obvious benefit to national security”); The National Defense, Editorial, N.Y. Times, Sept. 12, 2001, at A26 (urging measures to counteract terrorism but cautioning about and advocating for the preservation of constitutional rights and stating “[t]here must be an exacting examination of how the country can face this threat without sacrificing its liberties”); Electronic Frontier Foundation, EFF Statement on Pro-Surveillance Criticism (Sept. 21, 2001), at http://www.eff.org/Privacy/Surveillance/20010921_eff_statement.html (explaining EFF’s opposition to some of the legislative measures to augment law enforcement’s surveillance capabilities—1) that the proposed changes are being considered and passed in great haste and with minimal discourse, 2) that the proposed changes, though putatively aimed at terrorism, are “broad ranging, permanent reductions in civil liberties and privacy of all Americans,” 3) that portions of the proposals “appear to be part of a general law enforcement ‘wish list’ rather than a specific response to terrorism,” and 4) that there is no indication that the present legal regime hampered law enforcement’s ability to detect or investigate the acts) (on file with the \textit{Fordham Law Review}).
intruding on personal liberties. Attempting to find and maintain a proper balance is critical given the potential risks facing our society, given increasingly sophisticated technologies, and given our substantial and growing dependence on communications, transactions, and other activities which leave some kind of data trail. Although new anti-terrorism measures most likely will be desirable and appropriate in light of the events of September 11, it is important to bear in mind that the government already possesses very substantial technological and legal capabilities, as this Note will discuss. While there likely will be support for exploiting electronic surveillance technologies in expanded or new ways to investigate and deter similar events, this Note urges caution. The government’s powers are already broad and deep, and the current regime for regulating them is fraught with profound problems; we risk throwing out the baby but keeping the bathwater if we expand the government’s surveillance capabilities without addressing the problems of the current regime and without ascertaining whether the failure to prevent this or future attacks is actually a function of restrictions on the use of surveillance.

Although this balance between government’s authority and citizens’ rights is the substance of the entire Constitution, the Fourth Amendment is the part of that venerable document that comes most into play when evaluating the boundaries, if any, of the government’s prerogatives of searching and seizing in the name of maintaining order and safety. The Supreme Court’s efforts to make the Fourth Amendment’s fundamental precepts meaningful in this era of highly sophisticated technology has been widely criticized, and even the Court appears to recognize weaknesses in its jurisprudence. This past term, the Supreme Court rendered its latest decision on the constitutionality of a modern surveillance technology in Kyllo v. United States. Although the Court’s holding in Kyllo—that the use of thermal imagers to detect unusual patterns of heat emanating from a house is a search, requiring a warrant—might indicate the Court’s ability to keep abreast of technological advances, a closer analysis of the entire system by which technologies are developed, used, and regulated, casts doubt on this important supposition.

The surreptitious surveillance at the Super Bowl in Tampa and the thermal imagers at issue in Kyllo illustrate several important aspects of modern covert surveillance technology. First, the Tampa police’s face-scanner and the thermal imagers were each deployed or used by a law-enforcement agency at its own discretion, with little or no knowledge by the general public and little or no involvement by a

9. See infra notes 421-22 and accompanying text.
12. See infra note 222 and accompanying text.
judicial or legislative branch. Second, the face-scanning at the Super Bowl shows how these technologies often involve the merging of several technologies—here, the merging of biometrics, computer databases and data-processing, and telecommunications—to create powerful synergies.

Part I.A of this Note describes several important surveillance technologies that the government is using or developing. This discussion attempts to convey the technological sophistication of modern surveillance and to identify the significant trends likely to affect the government's surveillance capabilities in the future. Part I.B explores the respective roles of the branches of the federal government in utilizing and regulating these surveillance technologies. These technologies and the entire system by which the government deploys and regulates them constitute what will be referred to throughout this Note as the surveillance regime.

Part II of the Note discusses several substantial problems with this regime, such as the weakness of the sanctions against abuses and the lack of any preemptive regulation. Further, this Part explores the problems of having Fourth Amendment protections turn on normative judgments by a panel of judges about "reasonableness" and "expectations of privacy." Finally—but perhaps most fundamentally—this Part then compares the regime with the Founders' original understanding of the Constitution in general and the Fourth Amendment in particular.

Based on the fundamental problems explored in Part II, Part III argues for a fundamental rethinking of this regime. Accordingly, it proposes an alternative regime, one which would permit governmental agencies to use these powerful technologies toward the paramount societal goal of maintaining domestic and international peace and security, while at the same time appropriately regulating their use and, in particular, minimizing their misuse.

At the heart of this proposal is the adoption by the Court of a rule that the use of a surveillance technology is per se unreasonable unless the executive agency or the Congress (or both) have clearly and overtly disclosed its intended usage and established the rules and regulations governing its use, especially measures to effectively prevent abuse or misuse. The function and purpose of such a rule would be to force the government, either the executive governmental agencies seeking to use these technologies or the Congress, to be accountable in its use of increasingly sophisticated and unobtrusive technologies and to bear the burden in the first instance of defining their reasonable use and of implementing measures to prevent misuse. The principle behind such a rule is that the Fourth Amendment's directive that the citizens' right against unreasonable searches and seizures "shall not be violated" is meaningless when the government's surveillance activities are virtually undetectable and unaccountable
and when the governmental agent's discretion has few realistic bounds. Although maintaining important oversight on the substance of the rights protected by the Fourth Amendment, the Supreme Court's primary role would be ensuring disclosure of the technology and its intended usage, articulation of a legitimate purpose, development of procedures and appropriate safeguards, and compliance with these procedures and safeguards.

It bears mentioning that this Note explicitly seeks to avoid turning this inquiry into an analysis of the right to privacy, as is often done and indeed as the Supreme Court has done.\(^\text{13}\) There is already substantial literature on the meaning of privacy and on whether privacy is a right that is constitutionally protected.\(^\text{14}\) Focusing on privacy places the burden on the citizen\(^\text{15}\) rather than on the government, which, this Note argues, is not only impractical but also contrary to the spirit and the letter of the Fourth Amendment specifically, and the Constitution generally.\(^\text{16}\) Requiring the citizenry to articulate and defend a "right to privacy" will, in the face of inexorable technological progress, lead to an increasingly meaningless Fourth Amendment. Therefore, the focus of this Note is on the government and its ability to articulate a legitimate purpose for its surveillance, to tailor the means closely to the purpose, and to construct sufficient safeguards against the misuse of these powerful technologies.

\(^{13}\) See infra notes 197-205 and accompanying text. The prevailing view currently is against recognizing a broad constitutional right to privacy. Despite language in the Ninth Amendment which on its face seems to allow—perhaps even encourage—the recognition of rights that were not specifically created in the Bill of Rights, this view is generally disfavored. See John Hart Ely, Democracy and Distrust: A Theory of Judicial Review 38 (1980) ("[T]he conclusion that the Ninth Amendment was intended to signal the existence of federal constitutional rights beyond those specifically enumerated in the Constitution is the only conclusion its language seems comfortably able to support."); see id. at 33-34 (describing the Ninth Amendment as the "old constitutional jester" and its disparagement in "sophisticated legal circles").


\(^{15}\) See infra note 414 and accompanying text.

\(^{16}\) See infra Part II.
I. THE REGIME IN THE UNITED STATES FOR COVERT SURVEILLANCE TECHNOLOGIES

In the context of surveillance technologies, it is worth taking stock of the familiar adage, "information is power." In the context of criminal prosecutions, information gained from wiretaps, for example, "can be powerful evidence of guilt,"¹⁷ and thus the allure of these technologies for crime-fighting is predictably and justifiably very strong. On the other hand, events such as Watergate serve as a reminder that the appetite for power and for information can at times be irresistible, and surveillance technologies can provide access to important information for nefarious use, such as to undermine or subvert political rivals or dissidents. In short and as this part of the Note will attempt to show, there are various uses for surveillance technologies, some of which are important, perhaps even vital, and warrant the technologies' robust use; however, there are other uses for the technology which pose grave risks. After describing the sophistication of several important surveillance technologies, this part of the Note will discuss the technologies' various governmental users and uses, and the current judicial and legislative rules that exist to constrain them.

A. The Technologies

Given the prominence in Americans' daily lives of highly sophisticated technological devices—from personal computers to cellular phones and from "smart homes" to global-positioning-satellite devices for boats and cars¹⁸—few people will be surprised that there is a wide array of highly sophisticated surveillance technologies. Further, since many of these sophisticated devices generally benefit users, it is easy to be lulled into a general perception that all technological advancement should be embraced and eagerly fostered.

This part of the Note will describe several important surveillance technologies—a comprehensive survey of all technologies with potential surveillance applications is beyond this Note's scope. While some of these technologies may be familiar, others, such as those used at the Super Bowl in Tampa¹⁹ which are designed to be unobtrusive, may be less well known or not commonly considered as a surveillance technology. The government's present capability for surveillance and monitoring is already very broad, sophisticated, and widely used; the

---


¹⁸. See infra notes 36, 41-42 and accompanying text for statistics on the use of personal computers and cellular telephones.

¹⁹. See supra note 2 and accompanying text.
uses and the capabilities will almost certainly continue to expand as the technologies continue to develop. This Note classifies the array of surveillance technologies into three categories: 1) technologies for intercepting communications, such as wiretaps; 2) technologies for enhancing perception, such as night-vision devices and thermal imagers; and 3) technologies for identifying and tracking, a broad category which includes location-tracking devices, biometric devices, and computer systems and databases.

1. Technologies for Intercepting Communications

The importance of telephonic communications for business, community, and culture is plainly evident. As one commentator described this phenomenon: "We are moving the fabric of our society into electronic channels as quickly as we can."\(^{20}\) Given the tremendous and growing reliance by U.S. citizens on telecommunications, it is important that the government's ability to protect the nation and to ensure that internal peace and safety keep pace with these large developments—i.e., that law enforcement be able to perform reasonable searches into and seizures of these communications. However, given this large reliance on telecommunications, it is equally important that citizens' privacy rights be robustly safeguarded.

Presumably, the American public is generally familiar with wiretaps and "bugs" which have existed for over a century and appear frequently in the news and in television shows, movies, and spy novels. Because these technologies are generally familiar, their continued effectiveness against people who know to be discreet has required that increasingly sophisticated and unobtrusive methods be created and perfected.\(^{21}\) Furthermore, the communications industry has changed


\(^{21}\) See infra note 40; cf., e.g., Evans v. State, 314 S.E.2d 421, 424 (Ga. 1984) (noting that "the simplest method of installing a tap... would have presented a serious risk of detection by criminal suspects, because it would have caused a drop in voltage measurable by equipment available to commercial gamblers"); Edward V. Long, The Intruders: The Invasion of Privacy by Government and Industry 21 (1966) (noting how people in Nazi Germany tried to evade the Gestapo's surveillance by conducting sensitive conversations in bathrooms or public parks).

Indeed, as part of the Communications Assistance for Law Enforcement Act ("CALEA") and at the request of the FBI, Congress required that communications service-providers permit law-enforcement agencies to conduct completely undetectable surveillance. See Office of Technology Assessment, U.S. Congress, Electronic Surveillance in a Digital Age 16 (1995), available at http://www.wws.princeton.edu/~ota/ [hereinafter OTA, Surveillance in a Digital Age]. The OTA report, which "relies heavily" on an FBI report entitled Law Enforcement's Requirements for Electronic Surveillance, see id. at 15 n.17, notes:

Intercepts must be undetectable by the intercept subject or other callers, and known only to the monitoring law enforcement agency and authorized personnel of the service provider responsible for setting up the intercept. In some cases, intercept subjects may use sophisticated equipment to detect
ELECTRONIC SURVEILLANCE

dramatically over the last few decades,22 pressuring law enforcement
to develop new technologies to enable its access to new means of
communications such as cellular telephones and e-mail.

Although there are occasional voices that question the value of
wiretapping,23 the prevailing view is aptly summarized by one
hornbook which states: “Wiretapping and eavesdropping are among
the most effective investigative techniques available to combat
crime.”24 The effectiveness of these means is quite self-apparent:

intercepts; nonetheless, service providers are obligated only to provide
transparency within the limits of their equipment based on industry
standards for transmission characteristics.

Id. at 22.

22. See infra notes 36, 41-42 and accompanying text. Regarding changes in the
telecommunications industry, the congressional Office of Technology Assessment
observed in 1995:

Technology has raced ahead, the structure of the industry has changed, the
number of carriers and services has multiplied; dependence on
communications for business and personal life has increased, computers and
data are becoming more important than voice traffic for business, and the
nation has become enthralled with mobile communication.

OTA, Surveillance in a Digital Age, supra note 21, at 1-2.

23. Forcefully articulating the view that the costs of wiretapping outweigh its
benefits, then-Attorney General Ramsey Clark stated in 1967 that:

Public safety will not be found in wiretapping. Security is to be found in
excellence in law enforcement, in courts and in corrections. That excellence
has not been demonstrated to include wiretapping.

Nothing so mocks privacy as the wiretap and electronic surveillance.
They are incompatible with a free society and justified only when that
society must protect itself from those who seek to destroy it.

1 Staff of Senate Subcomm. on Constitutional Rights, Comm. of the Judiciary, 93d
Cong., Federal Data Bases and Constitutional Rights: A Study of Data Systems on
Individuals Maintained by Agencies of the United States Government, at XXX
(Comm. Print 1974) [hereinafter Federal Data Banks and Constitutional Rights].
Senator Long stated in his 1966 book The Intruders, “Wiretapping and bugging are
undoubtedly helpful to the police in some instances. But experience indicates that
their value is limited.” Long, supra note 21, at 43. A substantial minority of members
on a commission to study and review Title III of the Omnibus Crime Control and Safe
Streets Act of 1968 in the mid-1970s concluded that
court-authorized surveillance had been used successfully in a limited number of
major cases, and has resulted in the conviction of only a few upper-
echelon crime figures; more frequently, however, court-authorized
surveillance has proved to be costly and generally unproductive, has served
to discourage the use of other investigative techniques, and, even under the
authorization and supervision of a court, has resulted in substantial invasions
of individual privacy.

Electronic Surveillance: Report of the National Commission for the Review of
Federal and State Laws Relating to Wiretapping and Electronic Surveillance, at xiii

24. 1 Clifford S. Fishman & Anne T. McKenna, Wiretapping and Eavesdropping §
1:1, at 1-3 (2d ed. 1995). In enacting Title III, the third of four findings that Congress
made was: “Organized criminals make extensive use of wire and oral
communications in their criminal activities. The interception of such communications
to obtain evidence of the commission of crimes or to prevent their commission is an
indispensable aid to law enforcement and the administration of justice.” Omnibus
"The jury hears from the horse's mouth that the defendant participated in the criminal activity as charged." As a result, the number of requests and authorizations for wiretaps (which includes telephonic, oral, or electronic intercepts) by state and federal law-enforcement agencies has steadily increased from 763 in 1989 to 1350 in 1999. Wiretaps were sought predominantly for narcotics-related offenses. Fifty-three percent of the 1350 wiretaps authorized in 1999 were for electronic intercepts (such as cell phones, e-mail, and pagers), thirty-one percent were for telephonic intercepts, five percent were for microphones, and eleven percent were for a combination of devices.
Since telephones are ubiquitous in homes and offices in the United States, they are typically located “close to the center of activity and discussion,” and are highly vulnerable to interception, they are highly suitable to easy and effective surveillance. However, in recent years, there have been several substantial changes in the technology of the nation’s telecommunications network, and these changes have affected surveillance in a variety of ways, both facilitating and impeding certain techniques.

According to the FBI, the proliferation of fiber-optics in many long-haul or high-bandwidth cables and the installation of highly sophisticated computerized “switches” have impaired their ability to execute lawful surveillance orders. On the other hand, the sophistication of these computerized switches also substantially benefits lawful surveillance orders.

As cellular telephones have become widely used, law enforcement has developed technologies to ensure access to these communications.
as well. Calls over cellular telephones, like calls over land-line telephones, are susceptible to interception at the telephone company's central office. In addition, a technology has been developed that allows a law-enforcement agent to eavesdrop on a specific person who is talking on cellular telephones in the vicinity of the agent. This technology, called "triggerfish," overcomes a reputedly common problem in tracking organized-crime or drug traffickers—namely their frequent changes in phones.


37. See supra note 31 and accompanying text. Since cellular telephone calls are carried over airwaves, they can be detected by anyone in the vicinity with a scanner that covers the particular frequency on which the call is being carried. See generally FCC, Fact Sheet: Interception and Divulgence of Radio Communications (June 1999), available at http://www.fcc.gov/Bureaus/Common_Carrier/Factsheets/investigation.html (on file with the Fordham Law Review). However, unlike a telephone call over a land-line which is carried from the premises to the central office by a specific and identifiable wire, the precise frequency assigned to a particular person will vary each time the user makes or receives a call, and will change to a different frequency if the caller moves from one cell site to another cell site during the conversation. See Cellular Telecomms. & Internet Ass'n, For the Consumer: Howitworks, at http://www.wow-com.com/consumer/howitworks/ (last visited Oct. 25, 2001) (on file with the Fordham Law Review). Furthermore, digital cellular telephone calls are encoded and encrypted and therefore more difficult to intercept between the handset and the cell-site than analog cellular phones or cordless telephones. See Market Sense: Cell Phones Facts Fiction Frequency, at http://www.fcc.gov/marketssense/cellphone.html ("If you are concerned about whether your conversation will be overheard, digital signals are considered more secure because the sophistication and complexity of a digital system makes interception of calls virtually impossible."). However, the encryption scheme commonly used for digital cellular telephony can be readily cracked by a standard desktop computer. See Diffie & Landau, supra note 20, at 26-27.

38. See Interview with Special Agent Styron, supra note 27.

40. See Michael Goldsmith, Eavesdropping Reform: The Legality of Roving Surveillance, 1987 U. Ill. L. Rev. 401, 410 ("The success of electronic surveillance prompted experienced targets to shift telephones continuously, carefully guard conspiratorial meeting sites, and frequently change the locations of meetings.").
41. The Department of Commerce found that "[a]s of August 2000, 116.5 million Americans were online—31.9 million more than only 20 months earlier. Internet users accounted for 44.4% of the U.S. population..." Nat'l Telecomms. and Info. Admin., U.S. Dep't of Commerce, Falling Through the Net: Toward Digital Inclusion 33 (Oct. 2000), available at http://www.ntia.doc.gov/ntiahome/digitaldivide.
than half of all U.S. households have computers, more than forty percent have access to the Internet, and there has been substantial growth in both of these measures in the last few years. Consequently, law-enforcement agencies are developing and using sophisticated technologies to intercept these electronic communications. As indicated above, the interception of electronic communications represents the most common use of authorized surveillance. Although several off-the-shelf software packages for monitoring or “sniffing” e-mail and Internet traffic exist, the technology most important in this context is Carnivore, which has been developed and deployed by the FBI to intercept electronic communications. Along with two other software programs that together comprise a suite of software known as DragonWare, Carnivore is a computer program that enables the FBI to “select and record a defined subset of the traffic on the network to which it is attached.” While Carnivore has sparked a strong reaction to secretive governmental surveillance of electronic communication, it

42. See id. at 1 (“In just 20 months, the share of households with Internet access soared by 58%, from 26.2% to 41.5%, while the share of households with computers rose from 42.1% to 51.0%. More than 80% of households with computers also have Internet access today, up from little more than 60% in 1998.” (footnote omitted)).

43. See Stephen P. Smith et al., IIT Research Institute, Independent Technical Review of the Carnivore System, at 4-2 (Final Report Dec. 8, 2000) (“Carnivore represents technology that protects privacy and enables lawful surveillance better than alternatives such as commercially available sniffer software.”) [hereinafter Independent Review of Carnivore].

44. Carnivore was originally called “Omnivore.” When the newspapers first reported about Carnivore in July 2000, several commented on the unfortunate name. The FBI recently gave Carnivore a new name: DCS1000. See Janet Kornblum, Citizens’ Concerns About Privacy Grow, USA Today, Apr. 3, 2001, at 3D. This Note will refer throughout to this technology as Carnivore.

45. Independent Review of Carnivore, supra note 43, at viii. “Packeteer is a tool used to process the collected packets; the main purpose of this process is to put together all of the packets that belong to one session. . . . CoolMiner is a web browser tool that is used to analyze the packet data that Packeteer put together.” Id. at 2-3.

46. Id. at 1-1.

47. The existence of Carnivore became known to the general public when an Internet service-provider “told a House Judiciary Committee in April [2000] that the FBI was requiring the company to install the system on its network to fulfill court-ordered surveillance of criminal suspects.” See Ann Harrison, Privacy Group Critical of Release of Carnivore Data, ComputerWorld, Oct. 9, 2000, at 24. Earthlink, the Internet service-provider, “resisted the installation of the secretive system because [Carnivore] caused performance problems on its network . . . [and because Earthlink] couldn’t examine the technology to determine if its capturing of e-mail, IP addresses and other traffic violated the privacy of other customers.” Id. This discovery aroused considerable controversy and criticism. Subsequently, Congress held hearings, and the Justice Department commissioned a study of Carnivore by the IIT Research Institute and the Illinois Institute of Technology Chicago-Kent College of Law, which published an unclassified report in December 2000. See Independent Review of Carnivore, supra note 43, at vii. The Department of Justice specifically asked the contractor to evaluate four issues. See id. The contractors, however, also integrated concerns and questions raised by privacy groups, such as “[a]ll potential capabilities of the system, independent of intended use [and controls on, and auditability of, the
is apparently not the only way in which the U.S. government monitors communication traffic over the Internet. There are reports that the National Security Agency ("NSA") has devised a system, called "Echelon," to monitor Internet traffic around the world.\(^4\) A second capability for the government to eavesdrop on citizens' computers has come to light recently: "key logger" systems, which record all keystrokes made on a target computer.\(^4\)

Although there were only fifty-eight reported authorizations for microphone-based interceptions,\(^5\) it seems safe to assume that the true usage of "bugging" devices is substantially higher.\(^5\) The technologies for intercepting oral communications, like the technologies for intercepting telephone conversations, have been around for many years\(^5\) and are highly developed.\(^3\) For example, body-worn microphones, which are useful for detecting and intercepting conversations where one participant consents to the surveillance (as in an informant or undercover agent)\(^5\) are becoming

---

entire process by the FBI, the DoJ, and the courts." Id. The contractors did not address the constitutionality of Carnivore nor the trustworthiness of the agents operating it. See id. at 1-2.


49. John Schwartz, F.B.I. Use of New Technology to Gather Evidence Challenged, N.Y. Times, July 30, 2001, at C7. After seizing, pursuant to an ordinary search warrant, the computer of an individual suspected of gambling and loan-sharking, the government was unable to gain access to the content of the computer because it had been carefully encoded. Id. The government then installed the key-logger system on the target's computer which uncovered the password on his encryption system. Id. Precise details of the technology and its use are presently not public and the government has resisted a judge's order to provide details of it. John Schwartz, U.S. Declines to Release Data in Trial, N.Y. Times, Aug. 25, 2001, at B1.


51. Cf. id. at 6 (noting that consensual searches, including the use of body mikes, do not have to be reported).

52. For example, Senator Long in 1966 described an array of bugging devices shown to a Senate Subcommittee holding hearings on governmental surveillance activities, including small microphones and transmitters hidden inside an olive. See Long, supra note 21, at 5-6.

53. Indeed, a telephone can be turned into a "bug" through a very small modification—so that a target's conversations can be intercepted even when the target is not talking on the telephone. See Berkel & Rapaport, supra note 30, at 476-85; Long, supra note 21, at 8.

54. Cf. Wiretap Report 1999, supra note 26, at 6 (noting that situations where "the interception of a communication to which a police officer or police informant is a party" are not covered by the reporting requirements of Title III).
more powerful and more discreet. Excellent microphones as small as 5 mm in diameter by 3 mm long are available with sensitivities such that they can pick up a whisper at approximately 7.5 meters (25 feet). Lasers make it possible to detect the minute vibrations in a pane of glass that are caused by the sound waves of the human voice.

There are pneumatic microphones which, when placed against an adjacent wall or window, \"allow\" sound to be overheard through solid surfaces up to 50 cm thick [20 inches]. Finally, although of limited use in covert surveillance given their bulkiness, parabolic and shotgun microphones have a potential range, under ideal conditions (no wind, clear line of sight), of three-quarters of a mile.

A close cousin to wiretaps and bugs is a technological device commonly known as a "pen register," which collects information (such as the telephone numbers dialed, the duration, and the time) about telephone calls placed to and from a target telephone for use in investigations and prosecutions of crimes. While less probative of guilt than a tape-recorded wiretap, these devices are helpful in showing associations between individuals which can be incriminating in prosecutions of conspiracy and organized crime. Further, the evidence gained from pen-registers can and is used to show probable cause necessary to obtain a surveillance order authorizing a wiretap.

55. According to one authority, one significant advance in covert audio surveillance has been the development of the \"electret\" microphone. Berkel & Rapaport, supra note 30, at 365. Electret microphones \"are much more resistant to shock and solid-borne vibration than other kinds of mikes, ... [minimize] the problem of clothing rustle, ... [and] perform well under temperature extremes.\" Id.

56. Id. at 358.

57. Id. at 435. The laser beam reflecting off the glass pane is picked up by a special receiver; thus, this technique will not be available if the receiver and laser cannot be properly aligned. Id. Furthermore, the efficacy of this surveillance technique is subject to certain environmental disturbances that cause the glass to vibrate such as air conditioners, traffic, and wind. Id.

58. Id. at 613.

59. Id. at 379.

60. Id. at 376-79, 612.

61. Strictly speaking, a pen register captures information about calls from the target telephone, while a so-called trap-and-trace device captures information about telephone calls to the target telephone. 18 U.S.C. § 3127(3)-(4) (1994). See generally U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000) (\"Pen registers record telephone numbers of outgoing calls ...; trap and trace devices record telephone numbers from which incoming calls originate, much like common caller-ID systems.\" (citing 18 U.S.C. § 3127)).

62. Cf. Diffie & Landau, supra note 20, at 192 (noting that in 1987 federal law-enforcement agencies such as the FBI and the INS requested the installation of only 91 trap-and-trace devices while in 1993, they requested over 2000).

63. See Annis, supra note 17, at 35 (\"Probable cause can be developed in part through pen registers [and] traps and traces .... A pen register and/or trap and trace section is an important part of the affidavit that develops probable cause. Once subscriber information provides names for the numbers being called by—or calling into—the target phone, ... it is an easy way to \"freshen\" the probable cause.\"); see, e.g., People v. Kramer, 706 N.E.2d 731, 733 (N.Y. 1998) (\"Based on the information
In theory, these dialed-number devices do not pick up the content of the communication, although, as will be discussed below, changes in technology and the forms of communication are blurring the line between "address information" and content.

2. Technologies for Enhancing Perception and Detection

During the Persian Gulf War in 1991, the American public learned of the effective use by the U.S. military of an image-intensification technology known as night-vision goggles. Night-vision goggles illustrate how modern technologies, often initially developed by and for the U.S. military but later adapted for civilian uses, are not only improving how well we see—beyond the rudimentary perception-enhancing technologies such as binoculars or flashlights—but are also creating new ways of "seeing."
A person's normal vision can be greatly enhanced by the use of technologies that improve how far we can see or that improve our ability to see in the dark. By amplifying small amounts of light, these devices permit viewing in nearly perfect darkness as if in day-time conditions. State police departments have used night-vision goggles while patrolling areas of high crime. In addition, these devices have proved particularly effective in assisting the surveillance of drug smuggling at night along coastlines.

In contrast to image intensification, thermal imaging (also known as forward-looking infra-red) operates completely independently of light. Instead, thermal imagers take advantage of the fact that all objects emit energy in wavelengths besides the ones that humans detect with our senses of sight, hearing, and touch. Thermal imagers detect the differences in the heat emitted by objects relative to other objects and convert these results into visual displays. Prior to the Supreme Court's Kyllo decision, a majority of courts to address the issue had held that the use of thermal imagers was not a search; these decisions often emphasized that thermal imagers are "passive" detection devices—i.e., they do not radiate anything into the subject, but rather merely detect what the object radiates, much like a camera. As Justice Scalia noted in Kyllo, some versions of the technology are relatively crude, while others are capable of "seeing"

---

detection range of the human eye." (emphasis added).

69. See id. at 5-1.
70. See id. at 8-36 to 8-37.
71. See id. at 8-37 to 8-47.
72. See id. at 6-3, 6-13 to 6-15.
73. See Kyllo v. United States, 121 S. Ct. 2038, 2041 (2001); Adcock, supra note 66, at 6-3, 6-13 to 6-15.
74. See Kyllo, 121 S. Ct. at 2041; Adcock, supra note 66, at 6-17.
75. The Fifth, Seventh, Eighth, and Eleventh Circuits had all previously held that the use of thermal imaging to detect heat emanating from houses was not a search under the Fourth Amendment. See United States v. Robinson, 62 F.3d 1325 (11th Cir. 1995); United States v. Myers, 46 F.3d 668 (7th Cir. 1995); United States v. Ishmael, 48 F.3d 850 (5th Cir. 1995); United States v. Pinson, 24 F.3d 1056 (8th Cir. 1994). Although panels of the Ninth and Tenth Circuits had ruled that such use of thermal imaging did constitute a search under the Fourth Amendment, see United States v. Kyllo, 140 F.3d 1249 (9th Cir. 1998); United States v. Cusumano, 67 F.3d 1497, 1510 (10th Cir. 1995), both of these decisions were later withdrawn. See United States v. Kyllo, 184 F.3d 1059 (9th Cir. 1999); United States v. Cusumano, 83 F.3d 1247, 1250 (10th Cir. 1996). The Ninth Circuit subsequently aligned with the four circuits that held this was not a search. See United States v. Kyllo, 190 F.3d 1041, 1043 (1999). However, a federal district court and a California appellate court ruled that warrantless thermal imaging violated the Fourth Amendment. See United States v. Field, 855 F. Supp. 1518 (W.D. Wis. 1994); People v. Deutsch, 44 Cal. App. 4th 1224 (Cal. Ct. App. 1996), appeal denied 1996 Cal. LEXIS 4001 (July 24, 1996). See generally Kyllo, 190 F.3d at 1048 (Noonan, J., dissenting). In addition, the highest courts of the states of Washington and Montana had ruled that thermal imaging violates their respective state constitutions. See State v. Siegal, 934 P.2d 176 (Mont. 1997); State v. Young, 867 P.2d 593 (Wash. 1994).
76. See, e.g., Kyllo, 190 F.3d at 1044-45, rev'd, 121 S. Ct. 2038 (2001).
through walls.\textsuperscript{77} In its cruder form, it is commonly used by law enforcement for detecting abnormal emissions of heat from houses that is often a tell-tale sign of the cultivation of marijuana.\textsuperscript{78} More sophisticated versions permit the police to conduct "remote frisks"\textsuperscript{79} and to detect various contraband.\textsuperscript{80} These thermal imagers, which have other important civilian uses besides law enforcement,\textsuperscript{81} are unaffected by lighting conditions and by the amount of clothing worn by the person,\textsuperscript{82} and are increasingly able to detect intimate details about the subject.\textsuperscript{83}

\textsuperscript{77} See Kyllo, 121 S. Ct. at 2044 n.3 ("The ability to 'see' through walls and other opaque barriers is a clear, and scientifically feasible, goal of law enforcement research and development."); see also Steven Salvador Flores, Note, Gun Detector Technology and the Special Needs Exception, 25 Rutgers Computer & Tech. L.J. 135, 139-40 (1999); Peter Eggleston, Video Meets Vision: A System That "Sees" Through Walls!, Advanced Imaging, Mar. 1, 2000, at 10.

\textsuperscript{78} See Adcock, supra note 66, at 7-9 ("[T]he US military is starting to surplus many of these older systems, transferring them to US law enforcement agencies for use in the war against drugs." (emphasis omitted)); see, e.g., Kyllo, 121 S. Ct. at 2041 (describing the process of using of a thermal imager to detect heat emissions from a house).

\textsuperscript{79} One commentator described a thermal-imaging product as follows:

Millivision is intended to be used primarily by law enforcement officers, usually to conduct "remote frisks" of individuals to detect the presence of concealed weapons. A patrolman could operate the device from his car to examine an individual on the street from a substantial distance without having to leave the vehicle or physically "search" the individual—and without the individual's knowledge.

\textsuperscript{80} As of 1994, one thermal imager known as Millivision offered "the opportunity for rapid and remote detection of metallic and non-metallic weapons, plastic explosives, drugs, and other contraband concealed under multiple layers of clothing without the necessity of a direct physical search." Reducing Gun Violence: Before the Subcomm. on Crime and Criminal Justice of the House Judiciary Comm., 103rd Cong. (1994) (statement of Dr. G. Richard Huguenin of Millitech Corp.), available at 1994 WL 14190555 [hereinafter Huguenin Statement]. They were able to detect non-metallic items as small as a centimeter as of 1994. Id. The thermal imager detects these contraband items by detecting variations, even slight ones, between the heat radiated by different objects relative to other objects, such as the human body. See id.; see also Flores, supra note 77, at 138-39.

\textsuperscript{81} See Adcock, supra note 66, at 8-1 to 8-59 (discussing the various civilian applications of image intensification and thermal imaging); see also Kyllo, 190 F.3d at 1044 n.4 (noting other uses besides surveillance of thermal imagers), rev'd, 121 S. Ct. 2038 (2001).

\textsuperscript{82} See Huguenin Statement, supra note 80; Flores, supra note 77, at 138-39.

\textsuperscript{83} See T. Wade McKnight, Note, Passive Sensory-Enhanced Searches: Shifting the Fourth Amendment "Reasonableness" Burden, 59 La. L. Rev. 1243, 1265 (1999) ("[A] new device known as a radar skin scanner is capable of producing images so precise that the operator is able to tell whether or not a male subject has been circumcised." (citing a 1997 report in the American Bar Association Journal)). However, law enforcement can configure the devices to afford some measure of protection for the privacy of people scanned by the device; for example, it can be programmed to only show on the screen items that satisfy certain criteria. See Flores, supra note 77, at 139.

Millivision's manufacturer argues that privacy safeguards, such as an image understanding algorithm ('IUA'), will protect subjects from unnecessary
3. Technologies for Identifying and Tracking

a. Beepers

Beepers are devices that can be implanted in an object such as a car or a container that transmits a signal and that can be tracked using ground-based or satellite receivers.\(^8\) Beepers permit law enforcement to keep tabs on a suspect or contraband without the need for maintaining direct visual contact that might alert the suspect that he is being trailed or that might jeopardize the safety of a law enforcement officer.\(^8\) With the greater use of satellites and the evolution of global-positioning systems, the capabilities for monitoring increase.\(^8\) Further, advances in electronics have and will continue to reduce the size of these transmitters while increasing their range and effectiveness. The market for location-identifying services is expected to grow rapidly, from an estimated $600 million to $5 billion in three years, spurred in part by the use of this technology in cellular telephones.\(^8\) In addition, the Federal Communications Commission has proposed that cellular-service providers be able to more accurately locate callers, reputedly in order to locate callers making 911 calls.\(^8\) Further, it may not be long before tracking devices could be implanted under a person’s skin to track his movements or location.\(^8\) While such a device could have many invaluable uses—e.g., to track individuals suffering from Alzheimer’s disease—it is also possible to envision nefarious uses, for

---

\(^{84}\) See 1 Carr, \textit{supra} note 25, § 3.2(e)(2)(D), at 3-47 to 3-48 ("As an aid to physical surveillance, particularly of objects or suspects in moving vehicles, law enforcement officers often use small transmitting devices, statutorily defined as ‘mobile tracking devices’ and usually referred to as beepers.” (footnote omitted)). A “tracking device” is statutorily defined as “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117(b) (1994).

\(^{85}\) See 2 Fishman & McKenna, \textit{supra} note 24, § 28:2, at 28-5 to 28-6.


\(^{87}\) See id.

\(^{88}\) See id. ("[T]he Federal Communications Commission has determined that by the end of this year carriers will need to begin equipping either cell phones or their communications networks with technology that would allow authorities to determine the location of most callers to within 300 feet, compared with current systems that can locate them within about 600 feet.”).

\(^{89}\) See id. (discussing “a chip called Digital Angel that could be implanted beneath human skin, enabling his company to track the location of a person almost anywhere using a combination of satellites and radio technology”).
example to monitor the minute movements of a political dissident or rival.

b. Biometrics

Technologies that permit the identification of people through unique characteristics have evolved tremendously from the now-familiar fingerprint. The U.S. government and private-sector organizations such as banks are using these technologies which distinguish between people based on their irises or from the pattern of heat in their faces. Recently, DNA "fingerprinting" has received considerable attention from the highly publicized murder trial of O.J. Simpson and from a series of cases where reanalysis of DNA has exonerated approximately seventy wrongly-convicted people. In addition to freeing the innocent, however, DNA is proving to be a valuable tool for identifying and securing convictions of the guilty.

---

90. See Froomkin, supra note 48, at 1494.
91. See id.
93. A pamphlet distributed by the National Commission for the Future of DNA Evidence stated: "Recent advancements in DNA technology are enabling law enforcement officers to solve cases previously thought to be unsolvable." Nat'l Comm'n on Future of DNA Evidence, U.S. Dep't of Justice, What Every Law Enforcement Officer Should Know About DNA Evidence (on file with the Fordham Law Review). The pamphlet further explains: The saliva on the stamp of a stalker's threatening letter or the skin cells shed on a ligature of a strangled victim can be compared with a suspect's blood or saliva sample. Similarly, DNA collected from the perspiration on a baseball cap discarded by a rapist at one crime scene can be compared with DNA in the saliva swabbed from the bite mark on a different rape victim. Id.; cf Richard Willing, Criminals Try to Outwit DNA, USA Today, Aug. 28, 2000, at 1A (describing criminals' tactics for undermining effectiveness of genetic evidence). The article recounts how one prisoner smuggled a sample of his semen out of the prison and paid a woman to stage a fake rape to create the impression that he was accused of a crime actually committed by another person with exactly the same DNA—a "3 trillion to 1" chance. Id. The article later notes that advances in DNA-testing technology "make it difficult to ruin a crime scene by spreading strangers' DNA. Enough DNA to form a near-certain match is now routinely lifted from fingernail clippings, hair particles, tiny sweat stains and even dried saliva from old postage stamps." Id. A lawyer quoted in the article noted that "police can 'trap' [suspects] by lifting DNA from cigarette butts, beverage containers and even spittle left on interrogation room floors, even if the cops don't have enough evidence to get a search warrant." Id.
c. Computer systems and databases

Although the government maintains numerous databases and operates numerous computer systems, several are most germane here. Since 1967 the FBI has maintained the National Crime Information Center ("NCIC"), a centralized "computerized information system" that federal, state, and local law enforcement can quickly access via a "nationwide telecommunications network" to more efficiently exchange criminal-justice information. NCIC has grown considerably in scope from its origins as a resource to allow police to ascertain whether or not a suspect had a criminal record. According to the Department of Justice, NCIC not only contains "criminal history records on persons arrested and fingerprinted for serious or significant offenses," but also "records on wanted persons, stolen property,... and [certain] missing persons." NCIC was enhanced in 1999 by the inclusion of features, such as improved image-processing and the ability to perform instant background-checks.

The Treasury Department maintains the Financial Crimes Enforcement Network ("FinCEN"), which was created with little fanfare by an Executive Order in 1990. Although the main inputs to this system are the reports of financial transactions above $10,000, FinCEN also draws on a variety of other commercial and governmental databases. "At the heart of FinCEN is a powerful 'expert system'—a form of artificial intelligence that uses a set of rules


[T]he federal government has instituted a variety of data collection programs that compel the production, retention, and dissemination of personal information about every American citizen. Linked through an individual's Social Security number, these labor, medical, education and financial databases now empower the federal government to obtain a detailed portrait of any person: the checks he writes, the types of causes he supports, and what he says 'privately' to his doctor.

Id. at 1.


97. 1 The Department of Justice Manual, supra note 95, at 1-101.


99. See Bercu, supra note 96, at 389.

100. See id. at 394-95.

101. See id. at 396-97.
to emulate the thought processes of human experts who are skilled at solving a given sort of problem." Although FinCEN is justified largely on the basis of its ability to battle narcotics-trafficking by detecting money-laundering, its directors have sought broader application.

More recently, there has been a proliferation of databases containing genetic materials (DNA) of criminals. These databases are used to identify the perpetrators of later crimes by comparing characteristics of genetic evidence collected from a crime-scene with the database. The allure of DNA testing for criminal prosecutions is twofold. First, DNA tests are highly reliable in identifying a person: except for identical twins, the genetic "markers" in a person's genes are unique. Second, the information is easily converted to data for storage in a computer for very quick and efficient cross-reference with other samples.

B. The Role of the Government

Each of the three branches of the federal government plays an important role in the current legal regime of covert surveillance technologies in the United States. The various law-enforcement agencies within the executive branch are the prime developers and users of these technologies. The judiciary exercises direct oversight over the executive agencies and interprets how these technologies comport with the Fourth Amendment of the Constitution when their use is challenged in court. The Congress controls the various agencies' budgets and from time to time enacts legislation adding requirements beyond what, according to the Supreme Court, the

102. Id. at 394.
103. See id. at 390-91.
104. See Schumacher, supra note 92, at 1644 ("A DNA database is a computerized collection of DNA profiles capable of being used for criminal identification purposes. . . Essentially, a DNA test result derived from a crime scene sample can be checked against the digital profiles stored in the database.").
106. See id. The author claims: In the fairly near future, a standard item in the trunks of American police cruisers—perhaps even on each officer's belt—may be a DNA analyzer. As a suspect is arrested, police will quickly swipe the inside of his cheek with a cotton swab and pop the results into the scanner. Within minutes the machine will produce a stream of data describing the suspect's unique genetic structure. The data will be uploaded to state or national DNA databases to determine whether the suspect's DNA matches that of blood, sweat, semen, or similar bodily fluids found at the scene of unsolved crimes around the nation.
107. Id.; see also Nat'l Inst. of Justice, U.S. Dep't of Justice, The Future of Forensic DNA Testing: Predictions of the Research and Development Working Group 3 (2000) ("Portable, hand-held systems are now working in laboratory experiments; how soon these will be available for routine use is not clear.").
Constitution requires. This part of the Note describes in closer detail the roles that the three branches of government play in the use and the regulation of covert surveillance technologies.

1. Executive-Branch Agencies: The Users and the Uses

Accurately gauging the extent to which surveillance technology is used and may be used in the future is important in order to fashion an appropriate and considered scheme for regulating these technologies—indeed it is important for understanding the need for regulation. Further, since these agencies are the ones who would be bound by any regulation, it is important to consider the ends for which they use technology, and differentiate the relative societal interests of each of these ends. The risks of misuse inherent in the various applications of surveillance technologies by these agencies also deserve consideration.

Several important observations flow from the self-evident fact that executive-branch agencies are the governmental actors who develop and use new surveillance technologies: As the developers and users, these executive agencies are for all practical effect the first interpreters of the constitutionality of these technologies; as *Kyllo* and the surveillance at the Super Bowl in Tampa illustrate, these agencies and their agents decide in the first instance—and often in the only instance or an instance that lasts a long time—when and how the technology will be used.\(^7\) Already cabined off from direct political pressure, their accountability is further diminished by the fact that their activities—carried out in the name of law enforcement and national security—are statutorily shielded from disclosure.\(^8\) Furthermore, certain agencies are heavily involved in behind-the-scenes policymaking,\(^9\) and have exhibited an unwillingness to accede when the apparently prevailing view differs from their own.\(^10\)

---

\(^7\) See infra Part II.A.1.


\(^9\) One commentator explained that "the principal telecommunications regulatory body in the United States is the FBI. The FBI is taking on a major regulatory and policymaking role in determining the direction of technology." Stewart Baker, *Regulating Technology for Law Enforcement*, 4 Tex. Rev. L. & Pol. 53, 55-56 (1999). As Representative Bob Barr explained:

> This significant expansion of federal wiretap authority, sought for years by the FBI and other federal law enforcement agencies, was accomplished not through hearings, legislative mark-up, floor vote, and public input. Rather, it was itself born of a covert operation with nary a hearing. The provision appeared as a surreptitious and non-germane addition to legislation authorizing foreign intelligence activities.

There are numerous governmental agencies currently using surveillance technologies. This cast includes the intelligence agencies (such as the Secret Service, the Central Intelligence Agency, and the National Security Agency), various law-enforcement offices within the Department of Justice (such as the FBI; the Bureau of Alcohol, Tobacco, and Firearms; and the Drug Enforcement Agency), and numerous other agencies, including the Internal Revenue Service, the Immigration and Naturalization Services, the Environmental Protection Agency, the Bureau of Land Management, the Department of the Interior and the Forest Service, the Bureau of Prisons, and the U.S. Postal Service. A 1984 study by the authorized in Intelligence Authorization Act for 1999 § 604, Pub. L. No. 105-272, 112 Stat. 2397, 2413 (codified at 18 U.S.C. § 2518(11)(b))). According to a 1999 report published by the European Parliament, [b]etween 1993 to 1998, the United States conducted sustained diplomatic activity seeking to persuade EU nations and the [Organization for Economic Cooperation and Development] to adopt their "key recovery" system. Throughout this period, the US government insisted that the purpose of the initiative was to assist law enforcement agencies. Documents obtained for this study suggest that these claims willfully misrepresented the true intention of US policy. Documents obtained under the US Freedom of Information Act indicate that policymaking was led exclusively by NSA officials, sometimes to the complete exclusion of police or judicial officials.

Since 1993, unknown to European parliamentary bodies and their electors, law enforcement officials from many EU countries and most of the UKUSA nations have been meeting annually in a separate forum to discuss their requirements for intercepting communications. These officials met under the auspices of a hitherto unknown organisation, ILETS (International Law Enforcement Telecommunications Seminar). ILETS was initiated and founded by the FBI.  

Campbell, Surveillance Technology for Political Control, supra note 48, at ¶¶ 84, 85.  

110. In recent years, the FBI has lent particular influence to two other important initiatives: the Communications Assistance for Law Enforcement Act and the so-called "Clipper chip," an encryption technology for which law enforcement had a key, ensuring that law enforcement would be able to decode any communication. See Diffie & Landau, supra note 20, at vii. When the FBI submitted its "Clipper chip" technology for notice-and-comment rulemaking, the public input was overwhelmingly against it—with two favorable responses and 300 negative ones. See id. Nevertheless, the FBI continued to aggressively pursue and promote its technology. See Bruce Schneier & David Banisar, The Electronic Privacy Papers: Documents in the Battle for Privacy in the Age of Surveillance 320 (1997); see also Diffie & Landau, supra note 20, at 76.  

After lobbying for passage of CALEA, the FBI has continued to play a major role in its implementation. Pursuant to CALEA, the FBI and the Telecommunications Industry Association ("TIA"), the body that was setting the standards for the industry, conducted "extensive negotiations" before the TIA arrived at these standards, known as the J-Standard. See U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 455 (D.C. Cir. 2000). The FBI then requested that the Federal Communications Commission grant law enforcement nine additional capabilities beyond those included in the J-Standard. See id. at 456. The FCC granted four of nine proposed additional capabilities requested by the FBI, denied three, and granted two in part. Id.  

111. One indication of how many components of the federal government are involved in law enforcement in some respect is that the newly created Office of
congressional Office of Technology Assessment discovered that fifteen agencies used at least six types of surveillance technologies. In addition to these numerous agencies, two other large sectors play significant roles in the user portion of the surveillance regime. First, since surveillance technologies are highly valuable tools in battle—for example, detecting enemy troops and armaments at night or in difficult terrain—the U.S. military is a major consumer and developer of surveillance technologies. As mentioned elsewhere, several technologies initially developed by the military have been adapted for civilian purposes, including law enforcement. Second, law enforcement often relies on private-sector actors in significant ways. For example, private-sector actors such as banks, telephone companies, employers, and utilities collect and preside over much personal information, including information that law enforcement can use in gathering evidence of criminality. In fact, the assistance of telecommunications companies with law enforcement for wiretaps is now mandated by statute. Also, since the Court has ruled that surveillance of a person does not require a warrant if another person speaking with the target consents to or implements the wiretap himself, private citizens can and frequently are used for surveillance by law enforcement.

The license for, and prevalence of, surveillance is not the only important factor in understanding the extent of the problem and in


113. See Adcock, supra note 66, passim; see also Froomkin, supra note 48, at 1500-01 (discussing development by military of "smart dust," which is "ubiquitous miniature sensors floating around in the air").

114. See, e.g., supra notes 66-67, 81 and accompanying text.

115. Although the Constitution as a general rule does not reach the conduct of private persons, see 1 David S. Rudstein et al., Criminal Constitutional Law § 2.02, at 2-7 (2000), the role of these private-sector actors may take on a constitutional dimension through the state-actors doctrine, which states that when "a private party 'act[s] as an instrument or agent of the state' in effecting a search or seizure, he is subject to the restraints of the Fourth Amendment." Id. § 2.02[3], at 2-14.

116. See, e.g., Kyllo v. United States, 121 S. Ct. 2038, 2041 (2001) (noting that records of energy consumption were used to build the case against Kyllo); cf. Twight, supra note 94 (describing the substantial information collected by the government related to individuals' employment, finances, health, and education).


118. See United States v. White, 401 U.S. 745, 753 (1971) (holding in a plurality decision that a conversation transmitted from a wired informant to federal agents did not violate the Fourth Amendment and did not require a warrant). See generally 1 Carr, supra note 25, § 3.5, at 3-86 to 3-151.

119. See 1 Carr, supra note 25, § 3.5, at 3-88 ("Without question, consent surveillance is the most widely used and most frequently practiced mode of eavesdropping . . . ").
attempting to craft appropriate regulation; a second significant consideration is the various governmental purposes which surveillance technologies are deployed to serve—i.e., the agencies’ motivations for exploiting the capabilities of these technologies. According to standards recently promulgated by the American Bar Association (“ABA”), “[t]echnologically-assisted physical surveillance[120] can be an important law enforcement tool . . . [to] facilitate the detection, investigation, prevention and deterrence of crime, the safety of citizens and officers, the apprehension and prosecution of criminals, and the protection of the innocent.”[121] For example, less-than-covert surveillance technologies, such as metal detectors in government buildings, schools, and airports, are used to detect and deter crime. Similarly, several municipalities in the United States are experimenting with the use of closed-circuit televisions in high-crime areas.[122] After using the face-recognition system at the Super Bowl, Tampa deployed the system in other areas of the city,[123] and following the attacks on the World Trade Center, there were calls for instituting face-recognition at important landmarks in New York City.[124]

120. The technologies of physical surveillance—as contrasted to “communications surveillance” and “transactional surveillance”—for which these standards were specifically developed are “video surveillance; tracking devices; illumination devices; telescopic devices; and detection devices.” ABA Standards for Electronic Surveillance, supra note 67, at 2-3 (quotation marks in original omitted).

121. Id. Standard 2-9.1, at 21. The face-scanning technology used in Tampa illustrates technologies for detecting and preventing crime, while the thermal imager in the Kyllo case illustrates a technology for detecting, investigating, and prosecution; more advanced thermal imagers capable of seeing through walls and clothes illustrate a technology for detection and investigation of crime and for safety of officers; the X-ray machines in airports illustrate technologies for deterrence and the protection of the innocent.

122. See Froomkin, supra note 48, at 1476-77. For a description of the widespread use of closed-circuit televisions in the United Kingdom, see Jeffrey Rosen, A Watchful State, N.Y. Times, Oct. 7, 2001, § 6 (Magazine), at 38. Professor Rosen describes how the rapid proliferation of cameras—to perhaps 2.5 million cameras throughout the country in approximately 440 city centers—has been propelled by the fear of terrorism. See id. at 41. Although the cameras are not primarily being used to detect terrorists (because “few terrorists are suspected in advance of their crimes,” see id. at 42) and are not clearly leading to reduced crime rates (“[l]ast year, Britain’s violent crime rates actually increased by 4.3 percent,” see id. at 92), these cameras are nevertheless very popular. See id. at 41-42. Professor Rosen argues that the United States should “resist going down the same path,” because these systems have “subtle but far-reaching social costs” (such as intensified racial profiling and video voyeurism of women), while their benefits remain unproven. See id. at 92, 93.


124. See Barstow, supra note 6 (discussing measures that professionals recommended for deterring terrorist attacks against Times Square, Grand Central Terminal, the Statue of Liberty, and St. Patrick’s Cathedral). According to this article, the former police commissioner of New York City, Howard Safir, recommended “the installation of 100 or so surveillance cameras in Times Square[, which would] . . . be integrated with biometric facial imaging software, allowing the images of all pedestrians to be compared with photographs of known terrorists.” Id.
Unquestionably, there are manifestly valuable governmental and societal interests in exploiting these technologies.

In addition, surveillance technologies serve other useful private-sector\textsuperscript{125} and non-law-enforcement governmental purposes. Surveillance technologies are increasingly important for the efficient operation of governmental agencies and delivery of governmental services.\textsuperscript{126} Sophisticated and reliable ways to verify people’s identities aid the government in rooting out fraud and waste, and generally make the delivery of governmental services more efficient.\textsuperscript{127}

However, the ABA’s standards also point out that there are important differences in the values served by particular technologies and purposes and that these values should correlate to the “burden law enforcement must bear to justify a particular procedure.”\textsuperscript{128} As the ABA notes in its commentary,

[c]ertain techniques may be reasonable only with respect to a particular law enforcement interest. For example, certain techniques (e.g., at airport checkpoints) may be easier to justify for security purposes than for investigatory purposes. Similarly, certain measures (e.g., an electronic “frisk” of a person on the street based on reasonable suspicion) may be permissible for protective purposes but not for detection or deterrence reasons.\textsuperscript{129}

Another professional recommended that visitors or commuters traveling through Grand Central Station be channeled through passive metal detectors. \textit{Id.} \textsuperscript{125} See, e.g., \textit{supra} note 81.

\textsuperscript{126} In \textit{Whalen v. Roe}, 429 U.S. 589 (1977), the Court observed:

The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. \textit{Id.} at 605. However, the Court’s next comment—“The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures,” \textit{id.}—does not entirely square with a contemporaneous congressional report which found “a disturbing absence of laws to control the new information capabilities of government, [and] an equally disturbing absence of knowledge of what data banks the government had, what they contained, and what they were used for.” 1 Federal Data Banks and Constitutional Rights, \textit{supra} note 23, at III.

\textsuperscript{127} See 1 Federal Data Banks and Constitutional Rights, \textit{supra} note 23, at XVI (“As the planning, programming, and budgeting functions of federal agencies became more complex, the use of and demand for statistical data in machine-readable form also grew.”); Barr, \textit{supra} note 109, at 79 (“Domestic policy goals such as preventing the employment of illegal aliens, tracking the spread of diseases, and enforcing the payment of child support, have led to a government push for larger, more closely linked databases.”).

\textsuperscript{128} ABA Standards for Electronic Surveillance, \textit{supra} note 67, Standard 2-9.1(c) cmt., at 26-27.

\textsuperscript{129} \textit{Id.} at 26.
Presumably, following the ABA's reasoning, technologies that are particularly invasive, unaccountable, or susceptible to misuse can be used in only the most limited circumstances, if at all.

Several of the more important distinctions bear further consideration. For instance, it is important to draw distinctions between evidence-gathering, general intelligence-gathering, and intelligence-gathering for national security. For example, evidence-gathering is typically place- and person-specific and, though the invasion visited on the target is often high, this invasion will often be brought to light in the prosecution. By contrast, general intelligence-gathering is typically very unspecific; though the invasion on an individual may be small, it also may be very broad and the people surveilled may, for better or worse, be none the wiser. Because it is cloaked in the greatest secrecy, intelligence-gathering for national security can be simultaneously highly and broadly invasive; it is also highly unlikely that such surveillance will come to light.

Finally—but perhaps most importantly—is the risk that these technologies will be used improperly or illegally, whether for gathering evidence or intelligence. History is full of examples of the misuse of these technologies; since by their very nature their

130. See 1 Carr, supra note 25, § 1.2(b), at 1-6 to 1-7 (describing the common use of surveillance to gain information about criminal activities beyond use in prosecutions—to “determine the scope of a criminal organization, the extent and nature of its activities, and the identities of its participants”); cf. Diffie & Landau, supra note 20, at 114 (“In general, wiretaps appear to be of greater value in gathering intelligence than in developing evidence.”).

131. See Louis A. Chiarella & Michael A. Newton, “So Judge, How Do I Get That FISA Warrant?: The Policy and Procedure for Conducting Electronic Surveillance, Army Law., Oct. 1997, at 25, 27-29 (discussing distinctions between surveillance for counterintelligence, for law enforcement, and for domestic security); cf. Physical Searches for Foreign Intelligence Purposes: Hearing Before the Subcomm. on Legis. of the House Permanent Select Comm. On Intelligence, 101st Cong. 1 (1990) (comments of Chairman McHugh) (“[W]arrantless physical searches conducted in the United States for foreign intelligence purposes ... occur with some regularity and have for several years.”) [hereinafter Physical Searches for Foreign Intelligence]; id. at 5 (statement of Mary Lawton, Department of Justice) (“It is important to understand that the current provision for issuing judicial search warrants, Rule 41 of the Federal Rules of Criminal Procedure, is ill-suited to the field of intelligence gathering.”).

132. Cf. 1 Carr, supra note 25, § 1.2, at 1-7 (describing surveillance for the gathering of specific evidence as being at the “other extreme from open-ended and unrestricted strategic intelligence surveillance”); Chiarella & Newton, supra note 131, at 27 (“The subject of a law enforcement investigation eventually learns of or knows about any searches and surveillance, even if the collection of the evidence does not result in prosecution.”).

133. Cf. supra notes 44-48 and accompanying text (discussing Carnivore and Echelon).

134. See Chiarella & Newton, supra note 131, at 27 (“The subject of counterintelligence collection techniques will not learn of searches and surveillance conducted, except in those exceptional instances where the Attorney General later approves the use of the collected information as criminal evidence.”).

135. See Diffie & Landau, supra note 20, at 137-48 (discussing incidents of illegal surveillance of prominent political figures from the 1940s through the 1980s); Richard
effectiveness is a function of their surreptitiousness, this risk of abuse or misuse logically increases as the technologies become more discreet. As one commentator described:

[B]ecause of the surreptitious nature of many new surveillance techniques, individuals will be unaware when the techniques are in use, and thus will be unable to detect or prevent government abuse.

---

E. Morgan, Domestic Intelligence: Monitoring Dissent in America 3-10, 61-62 (1980) (discussing incidents of questionable or illegal activities, including surveillance, by the FBI, CIA, and U.S. military from World War II to Watergate); Report of the National Wiretapping Commission, supra note 23, at 163-64 (discussing illegal surveillance by the New York City Special Investigations Unit and by the Houston Police Department). In the early 1970s, several instances of illegal surveillance by federal agencies came to light. For instance, it was learned that under the direction of President Nixon, a group of federal agents called the “Plumbers” broke into the psychiatrist’s office of Daniel Ellsberg, who was responsible for leaking the documents relating to the U.S. government’s handling of the war in Vietnam, the so-called Pentagon Papers, to the New York Times and Washington Post. See Morgan, supra, at 5. William Ruckelshaus, appointed in 1973 by President Nixon to head the foundering FBI, “revealed that between mid-1969 and early 1970 the FBI had, at the direction of White House officials, installed without warrants seventeen wiretaps on government officials and newsmen in an effort to determine the source of leaks of foreign policy information.” Id. at 6. As evidence of potential or actual improprieties grew, special committees within the U.S. Senate (chaired by Frank Church) and the U.S. House (chaired by Otis Pike) were created to further investigate the extent of improper activities by federal agencies. See id. at 7-8. The Church Committee (the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities) eventually uncovered evidence that:

For the next thirty years [after World War II], the FBI engaged in extensive monitoring of radical politics, largely in response to three separate waves of domestic unrest: the perceived danger of domestic communism in the 1940s and early 1950s, the civil rights movement of the mid-1960s, and the anti-Vietnam war movement of the late 1960s and early 1970s.

Id. at 37. Other federal agencies, such as the CIA, NSA, IRS, Army, and Secret Service, were also employing a variety of “questionable and sometimes illegal practices” to monitor and manipulate “political dissent in this country.” Id. at 3; see also id. at 37-83. With regard to the activities of the U.S. Army, Morgan states:

The army began the Continental United States (CONUS) Intelligence Program in the summer of 1965 to provide early warning of civil disturbances that it might be called on to quiet. Two years later, the program was expanded to include collecting materials concerning the political beliefs and actions of groups and individuals active in the civil rights movement, the white supremacy movement, the black power movement, and the movement against the war in Vietnam....

The Church Committee Report in 1976 identified four general areas of army involvement in illegal or at least problematic domestic intelligence activity: the collection of information concerning the political activities of individuals and groups; the monitoring of domestic radio transmissions despite a Federal Communications Commission opinion that such monitoring was illegal; investigations of groups that the military considered threats to their own personnel and installations; and assistance rendered to other agencies—ranging from the Justice Department to local police forces—engaged in keeping track of militant dissent. See infra note 308 and accompanying text.
The checks on government surveillance that previously had limited government intrusion into our private lives will be severely reduced, and much that individuals have long considered private will be open to arbitrary and capricious police inspection. 137

2. Judicial Regulation

The second major part of the regime for surveillance technologies is the judiciary's role in interpreting the constitutionality of these technologies. Although covert surveillance can implicate other liberty interests, such as the First Amendment right of association 138 and the Fifth Amendment right against self-incrimination, 139 this Note focuses on the Fourth Amendment, whose prohibition against unreasonable search and seizure is by far the most significant constitutional provision in this context. 140 This evaluation by the courts occurs primarily on two levels: first, determining whether the use of a particular technology or police practice constitutes a search or seizure and thus comes under the Fourth Amendment; and second, enforcing constitutional requirements on a day-to-day basis, by issuing search warrants and ruling on the admissibility of evidence gained from surveillance in court. This part of the Note will review how the Supreme Court has interpreted the Fourth Amendment, first with respect to general principles relevant to surveillance technologies and second with respect to surveillance technologies specifically.

137. Bernstein, supra note 63, at 579.
138. See ABA Standards for Electronic Surveillance, supra note 67, Standard 2-9.1(b) cmt., at 24 (“[T]echnologically-assisted physical surveillance can implicate other values as well, including ‘freedom of association, speech, and travel,’ and, more generally, the ‘openness of society.’”); Froomkin, supra note 48, at 1506 (noting that “the First Amendment right to freedom of association imposes some limits on the extent to which the government may observe and profile citizens, if only by creating a right to anonymity in some cases”).
139. See OTA, Civil Liberties, supra note 112, at 9; cf. Telford Taylor, Two Studies in Constitutional Interpretation 64-67 (1969) (discussing the implication on the Fifth Amendment right against self-incrimination of the seizure and use of personal papers); Froomkin, supra note 48, at 1506-23 (analyzing the First Amendment aspects of electronic surveillance).

In Olmstead v. United States, the Court held that a wiretap did not violate the defendant's right against self-incrimination. 277 U.S. 438, 462 (1928). This was the same decision where the Supreme Court ruled that a non-trespass wiretap did not violate the Fourth Amendment. Id. at 466. Despite significant advances in the means for intercepting and recording a suspect's words and actions, the Olmstead ruling with respect to the implications of electronic surveillance for the Fifth Amendment remains valid. See 1 Carr, supra note 25, § 1.3(a), at 1-8 to 1-9; Taylor, supra, at 72-73. However, a full exploration of this interplay is beyond the scope of this Note.
140. See ABA Standards for Electronic Surveillance, supra note 67, at 6 (“The constitutional provision most relevant to regulation of physical surveillance is, of course, the Fourth Amendment . . . .”).
a. **Important Principles of Fourth Amendment Jurisprudence**

The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.\(^{141}\)

Although a complex area of constitutional law with many intricate contours, there are certain principles of Fourth Amendment jurisprudence which are most relevant and important for an analysis of surveillance technologies.

i. **Warrant Required for a Search or Seizure**

The Fourth Amendment consists of two clauses, the Unreasonableness Clause and the Warrant Clause.\(^{142}\) The Supreme Court's modern interpretation of the Fourth Amendment reads these two clauses together.\(^{143}\) Thus, the proper measure of reasonableness required by the Amendment for a search or seizure of a person or his or her personal effects by a government official\(^{144}\) is secured by a warrant, which is issued by a judge or magistrate.\(^{145}\) Furthermore, as the text of the Amendment clearly provides, the government official seeking the warrant must show, through sworn statements, probable cause and must specify in the application the person or items sought by the search or seizure.\(^{146}\)

The modern interpretation of the Fourth Amendment, therefore, places great emphasis on the intercession of a judge or magistrate, who is in theory impartial and dispassionate, to assure that a governmental agent does not conduct an unreasonable search or seizure.\(^{147}\) The probable-cause prerequisite to a warrant serves to

---

141. U.S. Const. amend. IV.
142. See Taylor, supra note 139, at 23, 42-43; Kevin J. Allen, Overview of the Fourth Amendment, 88 Geo. L.J. 883, 883 (2000); Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 762 (1994); Jennifer Y. Buffaloe, Note, "Special Needs" and the Fourth Amendment: An Exception Poised to Swallow the Warrant Preference Rule, 32 Harv. C.R.-C.L. L Rev. 529, 529 (1997) ("A small forest has been pulped by legal scholars debating whether the two clauses of the Fourth Amendment stand alone, or whether the second Warrant Clause modifies the first Reasonableness Clause by defining a reasonable search.").
143. See Amar, supra note 142, at 762.
144. Cf. supra notes 115-119 and accompanying text (discussing involvement in surveillance of non-governmental agents).
145. See 1 Rudstein et al., supra note 115, ¶ 2.08[1], at 2-307.
146. 1 Fishman & McKenna, supra note 24, § 1:5, at 1-10; see also Taylor, supra note 139, at 79-85 (noting the substantial differences between a search warrant and a surveillance order, and describing how Congress sought the constitutional acceptance of a surveillance order by favorable comparison to a search warrant).
assure that the power of law enforcement is not brought down upon a person unless there is a threshold showing of legitimate suspicion. Although the Court has upheld generalized or broad searches in certain extenuating circumstances, the Court looks with disfavor on these generalized searches.

ii. Exceptions to the Warrant Requirement

Even where the governmental action constitutes a search or seizure, the Court has carved out several exceptions to the warrant requirement. Although there are others, the exceptions to the requirement that a government obtain a warrant prior to a search or seizure most relevant in the context of electronic surveillance are (1) in instances of emergencies, (2) where a person consents to the search or seizure, (3) when the person or object is in plain view, and (4) "administrative" or "special" searches. Thus, just as a law-enforcement officer does not need to obtain a warrant to search a person's house if that person agrees to the search, a law-enforcement officer does not need to obtain a warrant to eavesdrop on a telephone conversation if one party consents. Similarly, the requirement is

---


148. See CRS, Constitution of the United States, supra note 147, at 1217-20

149. See, e.g., City of Indianapolis v. Edmond, 531 U.S. 32 (2000) (holding that a law permitting local police to randomly stop drivers to check for illegal drugs was a violation of the Fourth Amendment). In Edmond, the Court noted that it has upheld a limited number of programs where there was no individualized suspicion of wrongdoing—"where the program was designed to serve 'special needs, beyond the normal need for law enforcement.'" Id. at 37.

150. 1 Rudstein et al., supra note 115, ¶¶ 3.01, 3.02, 3.04, 3.05, 3.10, 3.11; cf. Amar, supra note 142, at 764-68 (describing several instances where warrants are not required for a search or seizure, including searches and seizures (1) incident to arrest, (2) in exigent circumstances, (3) made with consent, and (4) of objects in plain view). But see Physical Searches for Foreign Intelligence, supra note 131, at 19 (statement of Samuel Dash) (suggesting that consensual and administrative searches are "not truly exceptions").

151. 18 U.S.C. § 2511(2)(c) (1994) ("It shall not be unlawful ... for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."); id. § 2511(2)(d) ("It shall not be unlawful ... for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."). See generally 1 Fishman & McKenna, supra note 24, § 6:1, at 6-4. As the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance explained in its 1976 report, consensual surveillance is not a search within the meaning of the Fourth Amendment because consensual surveillance is meant to corroborate conversations rather than intercept them. See Report of the National Wiretapping Commission, supra note 23, at 10. A
relaxed where the delay in obtaining a warrant could jeopardize a person's life. Searches for contraband at airports, schools, and government buildings and courthouses are considered "administrative" searches and are generally treated differently under the Fourth Amendment than searches aimed at capturing criminals and finding evidence of criminal activity. Although the Supreme Court has not decided the constitutionality of x-ray screenings at airports, those lower courts that have addressed the question generally have upheld such searches as reasonable given the minor intrusion compared to the high threat to people and property posed by a potential hijacking. Finally, it is not considered a search if a law-enforcement officer can plainly see the object or person from a vantage point where the officer is legally allowed to be.

iii. Enforcement

Although the Fourth Amendment does not specify a remedy for its violation, compliance under current precedent is achieved through the exclusionary rule. Initially articulated in Boyd v. United States and later adopted in Weeks v. United States, the exclusionary rule provides that any evidence that the state secured by means violative of the Fourth Amendment—i.e., without a court-authorized search warrant—must be excluded from the trial against the suspect. However, as will be discussed below, the exclusionary rule remains controversial and courts and law enforcement in general bristle under it.

Initially the Fourth Amendment was enforced by civil damage suits against offending government officers, and this remedy still applies, at least in theory. As one prominent academic noted in an
influential critique of modern Fourth Amendment jurisprudence, the
common-law tort remedy for trespass was an effective way at the time
of the passage of the Constitution to discourage government officials
from exceeding their authority when searching and seizing.\(^{165}\) Indeed,
in fashioning a wiretap statute to comport with the Fourth
Amendment, Congress specifically provided in Title III that a citizen
aggrieved by illegal surveillance by either a private citizen or law
enforcement officer has criminal and civil causes of
action.\(^{166}\) Nevertheless, criminal prosecutions against police officers conducting
illegal searches, either physical or electronic, are “extremely rare”—as
are internal disciplinary actions.\(^{167}\)

iv. “Mere evidence” Rule

The government’s use of surveillance technologies has been
significantly affected by developments or shifts in constitutional
precedents in other, related areas. One of the most significant shifts
in this context is the repudiation of the so-called “mere evidence
rule,” according to which governmental agents can only search for or
seize contraband or criminal instrumentalities, but not for “mere
evidence.” Since the results of surveillance rarely is contraband or a
criminal instrument, the use of surveillance technologies is inherently
inconsistent with this rule.\(^{168}\)

Building on a famous quotation from one of the more celebrated
cases at the time of the country’s founding, the Supreme Court held in
1886 in *Boyd v. United States*\(^ {169}\) that a statute authorizing agents to
obtain by subpoena a person’s private papers was unconstitutional.\(^{170}\) The Court held that this law violated not only the person’s protection
against unreasonable searches and seizures as afforded by the Fourth
Amendment but also the person’s Fifth Amendment freedom from
self-incrimination.\(^{171}\) Writing for the Court, Justice Bradley explained

\[^{165}\text{See Amar, supra note 142, at 759, 774 (“[W]e must remember the historic role played by civil juries and civil damage actions in which government officials were held liable for unreasonable intrusions against person, property, and privacy.”). Professor Amar also notes that “any official who searched or seized could be sued by the citizen target in an ordinary trespass suit... If the jury deemed the search or seizure unreasonable... the official would be obliged to pay (often heavy) damages.” Id. at 774 (citation omitted).}\]

\[^{166}\text{See 18 U.S.C. § 2520(a) (1994).}\]

\[^{167}\text{See infra notes 349-353 and accompanying text.}\]

\[^{168}\text{See Taylor, supra note 139, at 52.}\]

\[^{169}\text{Boyd v. United States, 116 U.S. 616 (1886). Writing for the majority in Boyd, Justice Bradley quoted extensively from Lord Camden’s decision in *Entick v. Carrington*, see id. at 627-29, about which he said: “every American statesmen, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom, and considered it as the true and ultimate expression of constitutional law...” Id. at 626-27.}\]

\[^{170}\text{Id. at 634-35.}\]

\[^{171}\text{Id.}\]
that "compelling the production of [a person's] private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principals of a free government . . . [and] the instincts . . . of an American."\textsuperscript{172} Despite the Court "categorically and unanimously" reaffirming the "mere evidence rule"\textsuperscript{173} in 1921 in \textit{Gouled v. United States},\textsuperscript{174} courts found ways around this rule.\textsuperscript{175} Given the inherent tension between the "mere evidence rule" and surveillance, the Court reevaluated the proposition that there is a difference for purposes of the Fourth Amendment between "mere evidence" and the instrumentalities and fruits of a crime. In \textit{Warden v. Hayden},\textsuperscript{176} a case decided in 1967, the Court reversed the lower court's determination that clothing seized and used as evidence in the prosecution only had evidentiary value and so was not lawfully subject to seizure.\textsuperscript{177} The Court reasserted its repudiation of the "mere evidence" rule in a 1978 ruling that the police, armed with a warrant, could search for evidence even from people not suspected of a crime.\textsuperscript{178}

These rulings doing away with the "mere evidence rule" have smoothed over potential constitutional impediments to the use of these technologies. While scholars have noted that the "mere evidence rule" articulated in \textit{Boyd} and \textit{Gouled} did not rest securely on an accurate reading of history,\textsuperscript{179} the current view similarly fails to appreciate important historical nuances.\textsuperscript{180}

\begin{itemize}
  \item[b.] \textit{The Fourth Amendment and Surveillance Technology: The Reasonable-Expectation-of-Privacy Test}
  \begin{itemize}
    \item[i.] \textbf{History}

    In 1928, the U.S. Supreme Court decided \textit{Olmstead v. United States},\textsuperscript{181} its first ruling on the constitutionality of a modern surveillance technology, namely wiretapping. At that time, wiretapping was not new; soon after the development of the telegraph in the mid-nineteenth century, government officials and private
\end{itemize}
\end{itemize}

\textsuperscript{172} \textit{Id.} at 631-32.
\textsuperscript{173} See \textit{Taylor}, supra note 139, at 51.
\textsuperscript{174} \textit{Gouled v. United States}, 255 U.S. 298 (1921).
\textsuperscript{175} See \textit{Taylor}, supra note 139, at 51 (quoting \textit{Gouled}, 255 U.S. at 309). Professor Taylor noted that the existence of a rule prohibiting the use of "mere evidence" was often a surprise even to lawyers. \textit{Id.}
\textsuperscript{177} \textit{Id.} at 296-97.
\textsuperscript{179} See \textit{Taylor}, supra note 139, at 59; \textit{Amar}, supra note 142, at 765-76 & n.26.
\textsuperscript{180} Cf. \textit{Amar}, supra note 142, at 765, 803.
\textsuperscript{181} \textit{Olmstead v. United States}, 277 U.S. 438 (1928).
citizens figured how to intercept communications to their advantage, such as for bookmaking, stock manipulation, and newspapers scooping each other.182 Several states, including Washington where Mr. Olmstead and his co-conspirators were conducting an illegal liquor enterprise, had enacted laws to curb wiretapping.183 Still, federal agents installed wiretaps on eight of the suspects' phones and amassed extensive evidence of a large conspiracy to violate the National Prohibition Act.184 Noting the Fourth Amendment's reference to "material things"185 and the significance of physical invasions in prior Fourth Amendment cases,186 the Court held that wiretapping did not violate the Fourth Amendment so long as there was no physical invasion of the target's premises.187 Thus, Olmstead affirmed that the dispositive factor in the Court's analysis of the Fourth Amendment, even relating to electronic surveillance, was the presence or lack of trespass by the agents on a person's premises.188

A few years after Olmstead, Congress passed the Communications Act of 1934 which made any interception of any telephonic communication a crime.189 Significantly, Congress did not add a law-enforcement exception to this prohibition,190 and the Supreme Court subsequently held that federal and state law-enforcement agents were therefore barred from using wiretaps.191 Nevertheless, in clear contravention of the Supreme Court's interpretation of the

182. See Samuel Dash et al., The Eavesdroppers 23-25 (1959) (noting that newspapers stealing stories, gamblers stealing the results of horse-races, and stockbrokers stealing financial news were examples of early telegraphic wiretappers); OTA, Civil Liberties, supra note 112, at 31; Berkel & Rapaport, supra note 30, at 121-22; Long, supra note 21, at 36-37.

183. See Olmstead, 277 U.S. at 479-80 & n.13 (Brandeis, J., dissenting) (listing state wiretap statutes).

184. See id. at 471 (Brandeis, J., dissenting) (noting that the wiretaps spanned nearly five months during which time the federal agents amassed 775 pages of notes on conversations).

185. Id. at 464 ("The Amendment itself shows that the search is to be of material things—the person, his house, his papers or his effects.").

186. Id. at 464-65.

187. Id. at 466. See generally 1 Fishman & McKenna, supra note 24, § 1:3, at 1-4 to 1-6. Overhearing a conversation by pressing a listening device against a wall was permissible, see Goldman v. United States, 316 U.S. 129 (1942); while nailing or tacking a listening device into a wall crossed the threshold into the Fourth Amendment and thus required a warrant, see Clinton v. Virginia, 377 U.S. 158 (1964); Silverman v. United States, 365 U.S. 505 (1961).

188. See generally 1 Fishman & McKenna, supra note 24, § 1:3, at 1-4 to 1-6. Thus, overhearing a conversation by pressing a listening device against a wall was permissible, see Goldman v. United States, 316 U.S. 129 (1942); while nailing or tacking a listening device into a wall crossed the threshold into the Fourth Amendment and thus required a warrant, see Clinton v. Virginia, 377 U.S. 158 (1964); Silverman v. United States, 365 U.S. 505 (1961).

189. See 1 Carr, supra note 25, § 1.3(b), at 1-8 to 1-9.

190. See OTA, Civil Liberties, supra note 112, at 32.

191. See generally 1 Fishman & McKenna, supra note 24, § 1:3, at 1-4 to 1-5. In 1937 the Supreme Court ruled in Nardone v. United States, 302 U.S. 379 (1937), that this prohibition applied to federal law enforcement agents, thus making it illegal for them to use wiretaps under the Act. See id. at 383. The Court later extended this interpretation to state law enforcement as well in Benanti v. United States, 355 U.S. 96, 100 (1957).
Communications Act, federal and state agents continued to wiretap phones. Given evidence and growing public awareness that illegal wiretapping by the police was a rampant practice, the Supreme Court revisited the constitutionality of wiretapping in the mid-1960s, this time reaching a different result.

In 1967 in *Berger v. New York*, the Court held unconstitutional a New York statute that authorized surveillance in certain circumstances. This decision's analysis of the constitutional implications of a wiretap was substantially the basis for Title III of the Omnibus Crime Control and Safe Streets Act, subsequent legislation establishing parameters for the lawful use of wiretapping by law enforcement. Later that year, the Court decided the watershed case *Katz v. United States* which repudiated trespass as the dispositive factor in surveillance jurisprudence and which held that wiretapping was a search under the Fourth Amendment. The Court exclaimed that "the Fourth Amendment protects people, not places," and reasoned that a warrant was required before law-enforcement officers could eavesdrop on telephone calls that Katz was making from a public pay phone.

---

192. *See OTA, Civil Liberties, supra note 112, at 32 (describing how wiretapping continued even after the Nardone decision); see also Long, supra note 21, at 79-101 (discussing the policies and practices of wiretapping by federal agencies of the 1920s through 1950s).

193. *See OTA, Civil Liberties, supra note 112, at 32-33. Samuel Dash's 1959 book, The Eavesdroppers, brought to the public's attention the extent of wiretapping within the New York Police Department. See Physical Searches for Foreign Intelligence, supra note 131, at 15 (comments of Samuel Dash) ("I conducted the first nation-wide investigation of wiretapping and bugging, electronic surveillance in 1959 and wrote the book, "The Eavesdropper." That book, I believe, played a significant role in changing the Supreme Court's decisions overturning Olmstead and ultimately leading to the Katz decision and the Congress' decision to enact Title III of the Safe Streets Act of 1968.").


196. *See 1 Fishman & McKenna, supra note 24, §§ 1:4, 1:6, at 1-6 to 1-7, 1-10 to 1-11.*


198. The Court explained:

> We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.

199. *Id. at 351.*

200. *See id. at 353-57. See generally 1 Fishman & McKenna, supra note 24, § 1:4, at 1-7 to 1-8.*
ii. Constitutionality of Other Surveillance Technologies

In addition to marking a substantial departure from its prior precedents, *Katz* was significant in a second respect. In subsequent cases involving the issue of whether a certain surveillance technology constitutes a search or seizure, the Court has adopted the analytical framework articulated by Justice Harlan’s concurrence in *Katz*.\(^{201}\) Justice Harlan opined that the Fourth Amendment’s reach turned on two factors: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”\(^{202}\) The Court has used this two-part reasonable-expectation-of-privacy rubric for determining whether other technologies are searches or seizures. In *Smith v. Maryland*,\(^{203}\) the Court held that the use of pen registers—devices that tell law enforcement details about the telephone numbers dialed to or from a target telephone—did not implicate the Fourth Amendment because a person does not have a “legitimate” expectation of privacy in numbers that he dials.\(^{204}\)

In a series of cases regarding the constitutionality of aerial surveillance, the Court has attempted to add more nuance to this analysis, by exploring the significance of whether the search was of an area akin to an “open field” or to the “curtilage” of a house and whether the surveillance revealed intimate details.\(^{205}\) In *Dow Chemical Company v. United States*,\(^{206}\) the Court found that despite extremely rigorous efforts by Dow to protect its large facility from observation,\(^{207}\) aerial photographs taken by the Environmental Protection Agency with sophisticated cameras and without a warrant did not violate the Fourth Amendment.\(^{208}\) Significant to the result the Court reached was that the area targeted by the surveillance was more akin to an “open field” than the “curtilage” of a private house.\(^{209}\)

More recently, the Court has backed off the curtilage/open fields distinction as the dispositive factor\(^{210}\) for evaluating the

---

201. *See* *Kyllo v. United States*, 121 S. Ct. 2038, 2042-43 (2001) (noting that Court has employed Justice Harlan’s formulation from his concurrence in *Katz* for determining the constitutionality of pen registers and aerial surveillance).


204. *See supra* note 61 and accompanying text.


208. *See id.* at 241-42 (Powell, J., concurring in part and dissenting in part).

209. *Id.* at 239.

210. *Id.* (“We conclude that the open areas of an industrial plant complex with numerous plant structures spread over an area of 2,000 acres are not analogous to the “curtilage” of a dwelling for purposes of aerial surveillance; such an industrial complex is more comparable to an open field ...”).

211. *Cf.* *United States v. Dunn*, 480 U.S. 294, 301 (1987) (implying that anything within a home’s curtilage was within the ambit of the Fourth Amendment).
constitutionality of a search. In *Florida v. Riley*\(^{212}\) and *California v. Ciraolo*,\(^{213}\) the Court held that surveillance of an area manifestly within the curtilage did not implicate the Fourth Amendment because they were naked-eye searches that any member of the public could have made just as easily as the law-enforcement officers did and thus did not require a warrant.\(^{214}\)

Another important factor in the Court's result in the aerial-surveillance line of cases is that the observations occurred in places where the officers or any other person (at least in theory) had a legal right to be.\(^{215}\) This reasoning has also generally been central in other cases involving surveillance with familiar or relatively simple technologies, such as binoculars\(^ {216}\) and flashlights.\(^ {217}\) Similarly, the Supreme Court's decisions in *United States v. Karo*\(^ {218}\) and *United States v. Knotts*\(^ {219}\) book-end the constitutional aspects of location-identifying technology.\(^ {220}\) Together, these decisions indicate that law enforcement can track a person's movements with the use of a beeper

---

214. In *Ciraolo*, the police, acting on a tip that a suspect was growing marijuana, were able to observe marijuana plants while flying over the target's home in a fixed-wing aircraft at an altitude of 1000 feet. 476 U.S. at 209.
215. In *Riley*, a police officer, flying in a helicopter from 400 feet, was able to look in through openings in the roof and sides of a greenhouse and observe "what he thought was marijuana growing in the structure." 488 U.S. at 448. Riley's greenhouse was located on a five-acre plot of land in rural Florida and was "obscured from view from surrounding property by trees, shrubs, and [a] mobile home." *Id.*
216. The Court in *Ciraolo* explained:
   The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible. . . . The observations by Officers Shutz and Rodriguez in this case took place within public navigable airspace. . . . *Ciraolo*, 476 U.S. at 213-14); *see also Dow Chemical*, 476 U.S. at 239; *Riley*, 488 U.S. at 449 ("As a general proposition, the police may see what may be seen 'from a public vantage point where [they have] a right to be.'" (quoting *Ciraolo*).)
217. *See 1 Rudstein, supra* note 115, § 2.03[1][f], at 2-82 ("The use of binoculars, a telescope, or other optical aid that merely enlarges does not constitute a 'search' within the meaning of the Fourth Amendment when the police use the device to observe individuals, objects, or activities exposed to public view.").
without resort to a warrant unless and until it monitors activity inside a house.\textsuperscript{221}

As discussed elsewhere, the Supreme Court recently ruled in \textit{Kyllo v. United States} that the use of thermal imagers to detect unusual patterns of heat emission from homes—which is often indicative of indoor marijuana cultivation—was a search.\textsuperscript{222} Several things about this decision bear noting. First, in stark contrast to \textit{Dow Chemical}, where the Court went out of its way to downplay the sophistication of the camera used to make the aerial surveillance,\textsuperscript{223} Justice Scalia in \textit{Kyllo} partially premised his ruling on the recognition that there are substantially more sophisticated versions of the device at issue.\textsuperscript{224} Second, he heavily emphasized the importance of a house in determining whether an activity is a search, explaining that “[i]n the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes.”\textsuperscript{225} In addition, citing favorably a case from the pre-\textit{Katz} era,\textsuperscript{226} this decision may portend that trespass is being reestablished as the dispositive factor in Fourth Amendment jurisprudence, thus marking a full departure from the notion stated in \textit{Katz} that “the Fourth Amendment protects people, not places.”\textsuperscript{227} Third, the reasonable-expectation-of-privacy rubric and the curtilage/open fields dichotomy were markedly muted, and the opinion sharply criticized the intimate-details analysis for failing to provide sufficient practical guidance to citizens and to police officers about where the threshold between reasonable and unreasonable lies.\textsuperscript{228} These features suggest that the Court may be

\textsuperscript{221} \textit{See} \textit{Karo}, 468 U.S. at 714 (holding that the Fourth Amendment is implicated when beeper tracks an object into a private dwelling); \textit{Knotts}, 460 U.S. at 285 (holding that the Fourth Amendment is not violated when beeper tracks an object on a public highway). \textit{See generally} 2 Fishman & McKenna, supra note 24, §§ 28:1, 28:2, at 28-2 to 28-6; Jennifer Gruda, \textit{Electronic Surveillance}, 88 Geo. L.J. 990, 1011-12 (2000).

\textsuperscript{222} \textit{Kyllo} v. United States, 121 S. Ct. 2038, 2046 (2001) (“Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”).

\textsuperscript{223} \textit{See} \textit{Dow Chemical Co. v. United States}, 476 U.S. 227, 240-43 (1986) (Powell, J., concurring in part and dissenting in part) (describing in fuller detail Dow's efforts to maintain secrecy of its compound and the highly sophisticated camera used by EPA to photograph the compound).

\textsuperscript{224} \textit{See Kyllo}, 121 S. Ct. at 2044 (“While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.”).

\textsuperscript{225} \textit{Id.} at 2045; \textit{see also} \textit{id.} at 2041-42 (“At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.’ With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.” (quoting \textit{Silverman v. United States}, 365 U.S. 505, 511 (1961)).

\textsuperscript{226} \textit{See id.} at 2041, 2043 (citing \textit{Silverman}).

\textsuperscript{227} \textit{See supra} note 199 and accompanying text.

\textsuperscript{228} \textit{See Kyllo}, 121 S. Ct. at 2045 (“Limiting the prohibition of thermal imaging to ‘intimate details’ would not only be ‘wrong in principle; it would be impractical in
repudiating the doctrine and progeny of *Katz* and returning to a Fourth Amendment jurisprudence that is rooted in trespass.

3. Legislative Oversight and Regulation

The third major participant in this regime for surveillance technology is Congress. Although under the long-standing principle of judicial review, Congress cannot take away protections that the Supreme Court deems the Constitution requires, it can and does give shape to these requirements, including from time to time augmenting the protections. This part of the Note reviews principal laws related to surveillance that Congress has enacted, in particular the laws regulating wiretapping and privacy-related laws.

A few years after the Supreme Court ruled that a non-trespassory wiretapping did not violate the Fourth Amendment, Congress enacted the Communications Act of 1934, which created a blanket prohibition against the interception of communications, with no exception for law enforcement. Similarly, when the Court in *Berger v. New York* noted certain deficiencies in New York's wiretap statute, the U.S. Congress shortly thereafter codified these parameters in Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III—as the federal wiretap statute is commonly known—remains the core legislation governing the use of wiretapping.

a. **Title III, EPCA, FISA: Wiretapping and Interception of Electronic Communications**

Title III prohibits wiretapping generally, but creates an exception under which law enforcement can legally intercept oral, electronic, and wire communications in certain limited situations and under strict constraints. In enacting Title III, Congress expressly sought to

---

application, failing to provide 'a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.'" (quoting Oliver v. United States, 466 U.S. 170, 181 (1984)).


230. *See supra* notes 181-188 and accompanying text.

231. *See supra* notes 189-191 and accompanying text.


234. 18 U.S.C. § 2517. *See generally* 1 Carr, *supra* note 25, § 2.2, at 2-4 to 2-5; 1 Fishman & McKenna, *supra* note 24, § 1:6, at 1-10. Although Title III also applies to private citizens, the focus here is on the regulations created by this legislation on government agents.
accommodate both the need for effective law enforcement and the need to protect citizens' right to privacy. Title III was enacted amid strong evidence of widespread surveillance by police.

A surveillance order, the authorization that Congress created for law enforcement to legally conduct a wiretap, bears many similarities to a search warrant, which it is essentially modeled after. Nevertheless, a wiretap differs in key respects from an ordinary search—it is broader in time and place and it is harder to describe with much specificity the item that is sought. Describing a surveillance order as a "super search warrant," one assistant attorney general explained:

It is not an ordinary search warrant because it allows the search to be conducted over a particular instrument, no matter where that instrument may be in the United States (and even outside the jurisdiction of the court), and the search is allowed to span a 30-day period with the approval of the court.

Thus, Title III places analogous but more rigorous requirements on law enforcement. For example, a wiretap authorized under Title III

---

235. See § 801, 82 Stat. at 211. In enacting Title III, Congress made four findings, the fourth of which was that:

To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused.

Id. at 211-12. See generally 1 Fishman & McKenna, supra note 24, at § 1:6, at 1-10 to 1-11.

236. See supra note 193 and accompanying text; cf. supra note 135.

237. See Taylor, supra note 139, at 79-80; see also 1 Carr, supra note 25, § 2.5(a), at 2-20 to 2-21 (comparing conventional and electronic searches); Annis supra note 17, at 34 (same).

238. See 1 Fishman & McKenna, supra note 24, § 1:5, at 1-8 to 1-10; Taylor, supra note 139, at 83.

239. Annis, supra note 17, at 33.

240. Id. at 33-34. Although a surveillance order can be granted only for thirty days, see 18 U.S.C. § 2518(5) (1994), it can—and very often is—extended for additional thirty day periods. See Wiretap Report 1999, supra note 26, at 8. According to the Wiretap Report 1999:

A total of 1,367 extensions were requested and authorized in 1999 (an increase of 17 percent). The average length of an extension was 29 days, up from 27 days in 1998. The longest federal intercept occurred in the Western District of Texas, where the original 30-day order was extended nine times to complete a 289-day wiretap used in a narcotics investigation. Among state wiretaps terminating during 1999, the longest was used in a racketeering investigation in New York County, New York; this wiretap required a 30-day order to be extended 16 times to keep the intercept in operation 510 days. In contrast, 19 federal intercepts and 77 state intercepts each were in operation for less than a week.

Id.
requires that a high-ranking official within the U.S. Attorney General’s office submit an application to a federal judge or magistrate specifying, inter alia, 1) the facts showing probable cause that a crime is, was, or would be committed, that the particular communications will be used for the commission of the crime, and that the particular facility will be used in the commission of the crime; 2) the type of communication to be intercepted; and 3) a statement that other procedures have failed, will likely fail, or are too dangerous. Thus, Congress intended that law-enforcement agents seeking a warrant for this “super search” would have to meet an onerous burden.

To keep the wiretap statute current in the rapidly and profoundly changing telecommunications environment, Congress subsequently has amended Title III several times, the most significant of which are the Electronic Communications Privacy Act of 1986 (“ECPA”) and the Communications Assistance for Law Enforcement Act of 1994 (“CALEA”). Congress passed the ECPA in response to the proliferation of new “electronic communications,” such as e-mail and stored voice-mail and e-mail messages. With CALEA, Congress

---

241. 18 U.S.C. § 2518(1); see also Annis, supra note 17, at 35.
242. The process of obtaining judicial authorization for a wiretap, from the perspective of the law-enforcement officers who draft these applications, can be onerous. For an instructive discussion of the process and pitfalls of applying for an electronic wiretap, see Annis, supra note 17, at 35-39, and Monica Bachner, So You’ve Always Wanted to do a Wiretap: Practical Tips If You Never Have, USABulletin, Sept. 1997, at 40, excerpts reprinted in 9 Department of Justice Manual § 9-60.202A, at 9-1214.42 (1987). These articles explain that defense attorneys will generally pounce on mistakes or omissions in an application and seek to exclude the evidence. See Annis, supra note 17, at 35 (“[T]he necessity requirement seems to be one of the areas of concentrated effort in the defense bar’s attempts to suppress the results of super search warrants.”).
243. See generally 1 Fishman & McKenna, supra note 24, § 1:6, at 1-10 to 1-12. Since 1968, Congress has expanded the crimes for which a wiretap is authorized from 26 to nearly 100. See Rosen, The Unwanted Gaze, supra note 178, at 37. For a general discussion of the federalization of crimes, see John S. Baker, Jr., State Police Powers and the Federalization of Local Crime, 72 Temp. L. Rev. 673 (1999), which describes the expanding federal criminalization of local crimes, the reasons for the trend, and its consequences for the courts.
246. See generally 1 Fishman & McKenna, supra note 24, § 1:9, at 1-19 (noting that “the overall result [of the ECPA] was a significant improvement in the law”). Congress also codified the rules generally in practice by law enforcement for pen registers and trap-and-trace devices. Congress created for law enforcement the ability to conduct “roving wiretaps,” which allow the government to listen in on any telephone line a targeted person is likely to use, rather than allowing for a tap only on a particular phone known to be used by the person and which is the specific subject of the court-ordered tap. See generally 1 Fishman & McKenna, supra note 24, § 1:9 at 1-19 to 1-20. (The phrase “roving wiretap” does not appear in the statute. See Goldsmith, supra note 40, at 411.)
made it illegal to intercept communications over cordless telephones.247

Alongside Title III is the Foreign Intelligence Surveillance Act of 1978248 ("FISA"), which Congress enacted in response to lingering questions about whether surveillance by executive agencies in carrying out their national-defense function were covered by Title III.249 In United States v. United States District Court250 (commonly known as Keith), the Supreme Court held that the interposition of a judge was necessary for surveillance by executive-branch intelligence agencies for domestic national security.251 The decision did not mandate the application of Title III procedures for such surveillance for national security,252 and invited Congress to craft other protective procedures.253 Although the president's powers are at their greatest when acting for national security, nevertheless in light of Watergate and revelations by the Church Committee on abuses by federal intelligence agencies,254 Congress has mandated the president to get a surveillance order to conduct a wiretap for national security purposes.255 FISA created a seven-member special court to review applications for wiretapping for national-defense purposes.256 With FISA, Congress required the Attorney General to apply for a warrant to conduct electronic surveillance and show probable cause for domestic intelligence purposes.257 Thus, although the standard for

---

249. Despite the urging of a sizeable minority on a commission to review the wiretap laws, see Report of the National Wiretapping Commission, supra note 23, at 177 (Minority Report, James Abourezk et al.) (criticizing the majority opinion for "fail[ing] to address the subject of electronic surveillance for national security purposes"), the majority believed that national security surveillance was not covered by Title III and chose not to include national-security surveillance in its investigation. See id. at 27 ("The Commission did not undertake a study of... electronic surveillance for national security purposes because Title III specifically excludes electronic surveillance for national security purposes from its scope."). In response, the Minority notes that Title III is actually neutral on the president's authority to order surveillance for national security and that Congress empowered the Commission to investigate such sensitive matters. See id. at 177-78 (Minority Report, James Abourezk et al.).
251. Id. at 323-24.
252. Id. at 322 ("[W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case.").
253. Id. ("Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.").
254. See supra note 135 and accompanying text.
255. See 2 Fishman & McKenna, supra note 24, § 27:4, at 27-6 to 27-9; Chiarella & Newton, supra note 131, at 29-32.
256. See 2 Carr, supra note 25, § 9.3(a), at 9-6.
257. See id.
getting a surveillance order to wiretap for intelligence purposes is lower than a surveillance order for law-enforcement purposes, nevertheless, Congress has sought to require some level of accountability and to not cede totally unfettered discretion to intelligence agents.

b. Privacy statutes

An additional contribution by Congress to this surveillance regime takes the form of privacy-protection statutes, such as the Video Privacy Protection Act,\(^{258}\) the federal Privacy Act of 1974,\(^{259}\) the Fair Credit Reporting Act, and the Privacy Protection Act of 1980,\(^{260}\) in response to the Supreme Court’s ruling in Zurcher v. Stanford Daily.\(^{261}\) The Freedom of Information Act\(^{262}\) ("FOIA") is also an important measure which requires federal agencies to make certain information available to the general public and which empowers citizens to request additional specific information from these agencies.\(^{263}\) While this statute assures some measure of governmental accountability to the public, it also contains several exemptions that permit law-enforcement agencies to not disclose information.\(^{264}\)

---


259. Pub. L. No. 93-579, 88 Stat. 1896, tit. 5, § 552 (1974) (codified as amended at 5 U.S.C. § 552a (1994)). This statute "places limits on the types of information federal agencies may collect on individuals." Diffie & Landau, supra note 20, at 136. Congress later enacted the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988), to amend and modernize the Privacy Act because it was increasingly out of date with modern computing and record-keeping. See Gellman, supra note 258, at 146. However, according to Gellman, the Act’s core purposes have not been effectively carried out for a number of reasons: "[l]ack of administrative oversight, changing technology and record-keeping practices, and limited congressional attention." Id. at 147. In particular, the Office of Management and Budget ("OMB"), which is charged with oversight of the Privacy Act, has been criticized for not keeping up its responsibilities under the Privacy Act. Id. at 146.


263. See Gellman, supra note 258, at 147 (describing how FOIA "permits any person to request records in the possession of a Federal agency" and noting how FOIA has an important privacy component because the courts have interpreted it to exclude the disclosure of personal information).

264. See id. (noting that there are nine exemptions to the requirement that a federal government agency disclose requested information, including "national security information" and "law enforcement investigatory records"); see, e.g., Master
Although these and other enactments\(^{265}\) have created some additional protections for the privacy of communications, the overall trend seems to be the legislative erosion of privacy interests.\(^{266}\) For example, when Congress brought "electronic communications" within the scope of Title III, it did not impose the exclusionary rule on evidence procured in violation of its provision. Second, the ECPA created the power for law-enforcement to conduct "roving wiretaps," where the government is relieved of specifying "the nature and location of the facilities from which or where the communication is to be intercepted\(^{267}\) if specification is impractical.\(^{268}\) The Department of Justice prevailed on Congress to create this capability for person-dependent rather than telephone- or place-dependent surveillance in response to the effective use of evasive techniques by suspicious targets, such as switching telephones.\(^{269}\) Third, CALEA mandated that providers of telecommunications services make their systems wiretap-ready for law-enforcement surveillance and set aside $500 million dollars for companies to retrofit their systems for this purpose.\(^{270}\)

---

\(^{265}\) See Gellman, supra note 258, at 143 tbl.7.3, 151 (listing or mentioning as privacy-related legislation the Cable Communications Policy Act of 1984, the Family Educational Rights and Privacy Act (the "Buckley Amendment"), the Video Privacy Protection Act of 1988 (the "Bork Bill"), the Right to Financial Privacy Act, the Alcohol and Drug Abuse Patient Record Confidentiality Laws, the Telephone Consumer Protection Act, and the Driver's Privacy Protection Act of 1994).

\(^{266}\) Since 1968, Congress has slowly permitted lower-level personnel in the Attorney General's office to apply for wiretaps and has greatly expanded the crimes for which a wiretap can be authorized. See 18 U.S.C. 2516(1) (1994 & Supp. V 1999); supra note 243 and accompanying text.


\(^{268}\) See Goldsmith, supra note 40, at 411 n.61 (citing Department of Justice Memorandum from William Weld, Assistant Attorney General, Criminal Division to All United States Attorneys and Strike Force Chiefs, Dec. 15, 1986, at 10-11). Goldsmith argues that "[i]n many cases, roving surveillance reflects a broadened application of the particularity requirement rather than an exception thereto." Id. at 411 n.61 (emphasis added).

For interception of oral communications, a roving wiretap can be obtained without specification of location by convincing a judge that "specification is not practical." 18 U.S.C. § 2518(11)(a)(iii). For interception of wire or electronic communications, a roving wiretap can be obtained without specification of location by "showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility." Id. § 2518(11)(b)(ii). All applications for roving wiretaps must be approved by an official within the Department of Justice who is an Associate Attorney General or higher. Id. § 2518(11)(a)(i), (b)(i).

\(^{269}\) See Goldsmith, supra note 40, at 410.

c. Legislative Proposals After the Terrorist Attack of September 11

Shortly after the hijacking attacks, there was a flurry of legislative measures aimed at combating terrorism. Alarmed by this haste and lack of thoughtful deliberation, legislators and advocacy groups of both traditionally liberal and conservative stripes challenged the wisdom, motives, and the constitutionality of certain provisions.

271. On September 13, two days after the attack, the Senate attached an amendment, entitled the Combating Terrorism Act of 2001, to an appropriations bill for the Justice Department. See Senate Amendment 1562, 147 Cong. Rec. S9401 (daily ed. Sept. 13, 2001). See generally Alvarez, supra note 7. Several days later, Attorney General John Ashcroft introduced a more comprehensive legislative agenda which included nearly identical provisions to Senate Amendment 1562, the Combating Terrorism Act. See Krim, supra note 7.

272. Apparently, Congress was pressured to act quickly on the bill submitted by Attorney General Ashcroft. See Krim, supra note 7 ("The White House is pushing for Capitol Hill to act by the end of the week, according to a congressional source."); Robert E. Pierre, Wisconsin Senator Emerges as a Maverick, Wash. Post, Oct. 27, at A8 (reporting that Senator Russell Feingold, Democrat of Wisconsin and the only senator to vote against the legislation, explained that "the bill's title—the 'USA Patriot Act'—was part of the 'relentless' pressure to move it swiftly"). For example, Senate Amendment 1562 was passed hastily and with virtually no debate. See Krim, supra note 7 (noting that the amendment was passed by a voice vote late at night).

273. See Krim, supra note 7 ("A coalition of public interest groups from across the political spectrum has formed to try to stop Congress and the Bush administration from rushing to enact counterterrorism measures before considering their effect on Americans' privacy and civil rights."); Robin Toner, Bush Law-Enforcement Plan Troubles Both Right and Left, N.Y. Times, Sept. 28, 2001, at A1. One highly controversial provision of the proposed legislation, which would have permitted the attorney general to detain legal immigrants suspected of being involved in terrorism for indefinite periods without filing charges, was dropped. See id.; Robin Toner & Neil A. Lewis, House Passes Terrorism Bill Much Like Senate's, but with 5-Year Limit, N.Y. Times, Oct. 13, 2001, at B6 [hereinafter Toner & Lewis, House Passes Terrorism Bill].

274. Several commentators criticized the proposals, suggesting that portions of the draft legislation had little if anything to do with terrorism and instead were items on the Department of Justice's "wish list" of new law-enforcement capabilities. See The Home Front: Security and Liberty, supra note 8 ("[O]ther proposals from the attorney general do not seem to provide tools agents really need. In fact, some amount to a wish list of things that the Justice Department and the Federal Bureau of Investigation have unsuccessfully lobbied for in the past and that do not make sense now. Other provisions suffer from a blunderbuss approach."); Erwin Chemerinsky, Giving Up Our Rights for Little Gain, L.A. Times, Sept. 27, 2001, at 17 ("Atty. Gen. John Ashcroft's plan for fighting terrorism seems to include all the bad ideas for greater law enforcement powers that have been rejected over the years.").

These commentators implied that the Department of Justice was exploiting the present situation to enact measures that it had sought unsuccessfully prior to and irrespective of the specific occurrence. See Pierre, supra note 272 ("This is not a bill that is carefully tailored to the terrorism problem. The whole tenor of the debate was 'Let's grab as much as we can' given the fear of terrorism." (quoting Senator Russell Feingold)). An editorial in the New York Times observed that "Congress went down a similar path after the 1995 Oklahoma City bombing." The Home Front: Security and Liberty, supra note 8. The Antiterrorism and Effective Death Penalty Act "which passed by a wide margin, broadened the government's ability to detain and deport legal immigrants, even though immigrants had nothing to do with the
Nevertheless, the Congress enacted and President Bush signed into law the USA Patriot Act\textsuperscript{275} in less than two months and with overwhelming support.\textsuperscript{276} The bill contained several provisions that significantly changed the law regarding the government's ability to conduct surveillance.\textsuperscript{277} First, the USA Patriot Act makes terrorism a predicate act for which a wiretap under Title III can be authorized.\textsuperscript{278} Second, it modified Title III, FISA, and the federal statute related to pen registers so that there would be explicit legal authorization to permit surveillance of e-mail and Internet communications—i.e., for the use of Carnivore.\textsuperscript{279} Third, the Act authorizes the use of a "roving wiretap" under FISA.\textsuperscript{280} Fourth, the Act lowers the threshold for which surveillance pursuant to FISA is permitted,\textsuperscript{281} and expands the bombing.” Id.; cf. Greenhouse, \textit{supra} note 6 (noting that times of crisis most test our commitment to our ideals but that “times of deep insecurity, grief and anger . . . in fact have often evoked the worst of our national instincts”); Harvey A. Silverglate, \textit{Let's Not Trade Freedom for Security}, Nat'l L.J., Sept., 24, 2001, at A26 (urging that the administration, the “police agencies,” and Congress not pass “draconian legislation” which will have “severe limitations on civil liberties [and] no appreciable increase in security,” as occurred when Congress enacted the Antiterrorism and Effective Death Penalty Act, which “has all but eviscerated the ancient writ of habeas corpus”).


\textsuperscript{277} Id.

\textsuperscript{278} USA Patriot Act, § 201 (amending 18 U.S.C. 2516(1)); see Krim & O'Harrow Jr., \textit{supra} note 276. The USA Patriot Act also authorized law enforcement to conduct wiretapping for crimes related to computer fraud and abuse. See USA Patriot Act, § 202.

\textsuperscript{279} USA Patriot Act, §§ 214, 216 (amending 50 U.S.C. §§ 1842, 1843 and 18 U.S.C. §§ 3121, 3123, 3127); see also 147 Cong. Rec. S10999 (statement of Patrick Leahy). Senator Leahy explained:

I have long supported modernizing the pen register and trap and trace device laws by modifying the statutory language to cover the use of these orders on computer transmissions; to remove the jurisdictional limits on service of these orders; and to update the judicial review procedure, which, unlike any other area in criminal procedure, bars the exercise of judicial discretion in reviewing the justification for the order. The USA Act, in section 216, updates the pen register and trap and trace laws only in two out of three respects I believe are important, and without allowing meaningful judicial review.

147 Cong. Rec. S10999 (emphasis added).

\textsuperscript{280} USA Patriot Act, § 206 (amending 50 U.S.C. §§ 1805(c)(2)(B)). The “roving wiretap” can now be obtained upon a showing that “the actions of the target of the application may have the effect of thwarting the identification of a specified person.” Id.; see also 147 Cong. Rec. S10998 (statement of Patrick Leahy).

\textsuperscript{281} USA Patriot Act, § 218 (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)). Previously, “the secret procedures and different probable cause standards under FISA [could] be used only if a high-level executive official certifies that 'the purpose’ is to obtain foreign intelligence formation.” See 147 Cong. Rec.
ELECTRONIC SURVEILLANCE

Time-periods for which the Foreign Intelligence Surveillance Court can authorize surveillance in the United States of "an agent of foreign power." \(^{282}\) Fifth, the Act allows for so-called "sneak-and-peak warrants," in which law-enforcement officers are permitted to delay notifying a target that a search or seizure has been conducted. \(^{283}\) Sixth, the Act also lowers the firewalls that have been erected between law-enforcement and national-security agencies, by permitting greater sharing of information gained through surveillance. \(^{284}\) Finally, the Act subjects several provisions to a four-year sunset. \(^{285}\)

The first part of this Note has described the regime in the United States for surveillance technologies—i.e., the technologies, the respective roles of the branches of government, and the rules

---

282. USA Patriot Act, § 207 (amending 50 U.S.C. §§ 1805, 1824); 147 Cong. Rec. S11003 (statement of Patrick Leahy). Senator Leahy explained:

"[T]he bill changes the initial period of the surveillance from 90 to 120 days and changes the period for extensions from 90 days to one year. The initial 120-day period provides for a review of the results of the surveillance or search directed at an individual before one-year extensions are requested."

283. USA Patriot Act, § 213 (amending 18 U.S.C. § 3103a); 147 Cong. Rec. S11002 (statement of Patrick Leahy). Senator Leahy explained sneak-and-peak warrants as follows:

Two circuit courts of appeal, the Second and the Ninth Circuits, have recognized a limited exception to this requirement [that a person be notified of a search]. When specifically authorized by the issuing judge or magistrate, the officers may delay providing notice of the search to avoid compromising an ongoing investigation or for some other good reason. However, this authority has been carefully circumscribed.

First, the Second and Ninth Circuit cases have dealt only with situations where the officers search a premises without seizing any tangible property. . . .

Second, the cases have required that the officers seeking the warrant must show good reason for the delay. Finally, while the courts have allowed notice of the search may be delayed, it must be provided within a reasonable period thereafter, which should generally be no more than seven days. . . .

. . . . [T]he bill prohibits the government from seizing any tangible property or any wire or electronic communication or stored electronic information unless it makes a showing of reasonable necessity for the seizure. . . . Second, the provision now requires that notice be given within a reasonable time of the execution of the warrant rather than giving a blanket authorization for up to a 90-day delay. What constitutes a reasonable time, of course, will depend upon the circumstances of the particular case. But I would expect courts to be guided by the teachings of the Second and the Ninth Circuits that, in the ordinary case, a reasonable time is no more than seven days.

Id. at S11002-03.


285. USA Patriot Act, § 224.
regulating the technologies' use. This part has attempted to convey both the real-world application of these technologies and the capabilities for surveillance and monitoring of citizens with these technologies. Large technological advances—in electronics and in computer processing and storage, among other fields—have enabled the development of powerful yet unobtrusive devices. These sophisticated technologies have greatly increased the government's ability to eavesdrop on communications, to identify particular persons, and to monitor the locations, activities, and habits of its citizens. The next part of the Note identifies and discusses several significant practical problems with this regime; it also includes a comparison of the modern jurisprudence of surveillance with the original understanding of the Constitution generally and the Fourth Amendment specifically.

II. PROBLEMS WITH THIS REGIME

As the discussion in Part I makes clear, the government and especially law-enforcement agencies have access to very powerful technologies for surveillance and monitoring of citizens—and it seems certain that technological advances will continue to augment these substantial capabilities. Already, the law is struggling and failing to keep pace with these developments in surveillance, as many commentators have noted.286 Having described the technologies, their usage, and the various rules regulating them, Part II of the Note identifies and analyzes practical and theoretical problems with the current regime in the United States for surveillance technologies. Part II.A focuses on the shortcomings in the regime's ability to properly regulate the use of these technologies. Part II.B discusses several key differences between the original understanding and the current interpretation of the Constitution generally and the Fourth Amendment specifically.

286. As Professor Lewis Katz observed in 1990, "the Court has permitted police surveillance powers to grow almost unchecked to their present epic proportions...[and that police] may use any number of sophisticated surveillance techniques without judicial authorization or review." Lewis R. Katz, In Search of a Fourth Amendment for the Twenty-first Century, 65 Ind. L.J. 549, 549 (1990). In 1969, Professor Telford Taylor noted that "old habits and notions of personal privacy...are in grave danger of burial under an avalanche of new surveillance devices." Taylor, supra note 139, at 19; see also Froomkin, supra note 48, at 1463 ("I will argue that both the state and the private sector now enjoy unprecedented abilities to collect personal data, and that technological developments suggest that costs of data collection and surveillance will decrease, while the quantity and quality of data will increase."); infra note 423 and accompanying text; cf. Kyllo v. United States, 121 S. Ct. 2038, 2043 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."); Rosen, The Unwanted Gaze, supra note 178, at 58 ("[T]he Supreme Court's response to the growth of new technologies of monitoring and surveillance...has proved to be distressingly passive at every turn.").
A. Practical Problems with this Regime

1. Limited and Post-hoc Judicial or Political Evaluation

The first problem with this regime is that not all surveillance technologies are judicially or politically scrutinized, and those that are scrutinized are done after the technology has been in use for a while. In promulgating standards for electronic surveillance, the ABA cited several reasons that motivated the development of the standards. First, the ABA noted the prevalence of surveillance and the likelihood of greater reliance on it. Second, "traditional legal doctrine does not necessarily answer many of the novel questions raised by the use of technologically-assisted physical surveillance," such as the accountability of government agencies in using surveillance technology. Third, "when the courts have tried to regulate technologically-assisted physical surveillance by the police, their efforts have not resulted in a consistent body of case law." The significance of this pattern is that it increases substantially the already broad discretion that law-enforcement officers and agencies have.

A technological device known as "Sentor" illustrates how sophisticated technologies are deployed and exploited without pre-clearance and often with few rules governing their use. Sentor, which is currently in use in drug enforcement and border patrols, is a device which picks up and analyzes the air surrounding a person for traces of narcotics.

While the Sentor is frequently used without a warrant, no court has yet ruled on whether its warrantless use violates the Fourth Amendment's "reasonable expectation of privacy" standard. Peter Bober has asserted, however, that for purposes of Fourth Amendment analysis, the courts are likely to examine this new device by analogy to drug-sniffing canines. Citing Penny-Feeney's

287. See ABA Standards for Electronic Surveillance, supra note 67, at 5.
288. Id. at 6.
289. Id.
290. See Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 415 (1974) (noting the immense discretion of police officers on the street and how little controls are placed on them); see also infra text accompanying notes 360-61.

The "Sentor," a device... which looks like a large flashlight, is pointed at the suspect and, when switched on, vacuums in large quantities of air (and dust) from the area surrounding his or her body. It is then inserted into a larger machine, which heats the samples and through high-speed gas chromatography separates the chemical compounds contained therein, including those found in cocaine, heroin, and other narcotics. Id. (footnotes omitted).
interpretation of United States v. Place, Bober concludes that the Supreme Court, if presented with the issue, is likely to find that warrantless use of the Sentor does not constitute a search.292

Thus, a law-enforcement agent's resort to a warrant when employing this technology at present is optional; further, despite features which make Sentor potentially more intrusive than drug-sniffing dogs—in particular, that these specially trained dogs only smell drugs and other contraband while Sentor detects non-criminal details293—it is likely that this technology will be judicially approved by favorably comparing it to similar but less intrusive surveillance methods. This pattern of analogizing has been used by courts to allow the use of other surveillance technologies.294

Although the Supreme Court has ruled on the constitutionality of several technologies,295 by definition it does so after the fact, and often many years after the technology has been in use. For example, although the Supreme Court first ruled on wiretapping in 1928, the ability to wiretap was discovered and exploited a half century earlier, shortly after the invention of telegraphy and telephony.296 The ultimate decision by the Supreme Court on the constitutionality of thermal imaging occurred several years after this technology was adopted from its military lineage for use in civilian law enforcement.297

While the Court's dicta have strongly hinted at the constitutionality of image-enhancing technologies such as binoculars or night-vision goggles, the Court has never squarely addressed their constitutionality.298 In particular, the Court in United States v. Lee299 analogized a searchlight to marine or field glasses and concluded that neither was a search,300 and reviewed the use of binoculars approvingly in On Lee v. United States.301 In recent cases involving image-enhanced searches, such as Dow Chemical and most recently Kyllo, the Court has stressed that a key consideration is whether the

292. Id. at 138 (footnotes omitted) (citing Peter Joseph Bober, The "Chemical Signature" of the Fourth Amendment: Gas Chromatography/Mass Spectrometry and the War on Drugs. 8 Seton Hall Const. L.J. 75 (1997)).
293. See id. at 135, 138 (discussing analytical differences between drug-sniffing canines, FLIR, and Sentor).
294. See id. at 135 (discussing how courts have analogized FLIR to drug-sniffing canines).
295. See generally 2 Fishman & McKenna, supra note 24, §§ 29:1 to 29:7, at 29-3 to 29-14. Besides wiretapping and thermal imagers, the Court ruled in Smith v. Maryland, 442 U.S. 735 (1979), that the use of pen registers is not a search.
296. See Berkel & Rapaport, supra note 30, at 122 (noting that the New York Police Department was wiretapping telephones by 1895).
297. See supra Part I.A.2.
298. See 2 Fishman & McKenna, supra note 24, § 29:8, at 29-14.
300. Id. at 563. Justice Brandeis, one of the Court's champions of privacy rights, wrote the opinion in Lee. See id. at 560.
technology is in general use by the general public.\textsuperscript{302} Similarly, as the technology of wiretapping continues to progress, the constitutionality of these innovations are not scrutinized anew, but rather assumed to be legitimate based on analogies to technologies for which there is precedent. For example, the Congress authorized and the FBI developed a technology for the interception of electronic communications—Carnivore—by enfolding it within the rules of Title III. When the FBI uses its Carnivore software for monitoring the Internet communications of a target, it hews to the rules of Title III when searching the full content of the target's communications and adheres to the statutory requirements for pen-registers when searching only for information about who and when.\textsuperscript{303} Therefore, the extent, if any, to which these new technologies implicate the Fourth Amendment in new and unprecedented ways, or which require different strictures to ensure reasonableness, may never be considered.

To be sure, this post-hoc and limited scrutiny of surveillance technology merely reflects the nature of our judiciary, which generally decides specific controversies between specific parties involving specific events that have already occurred.\textsuperscript{304} Nevertheless, there are aspects of surveillance and technology that makes judicial and political scrutiny less likely. The very essence of most of these technologies is to be transparent and unobtrusive; their effectiveness logically correlates to the inability of the target to detect the surveillance.\textsuperscript{305} The inability to notice when a technology is being used is compounded by the fact that the existence of several of these technologies is not widely known. For example, several months after the controversial and highly publicized revelation in 2000 that the FBI had developed and deployed Carnivore,\textsuperscript{306} only twenty percent of

\begin{thebibliography}{9}
\bibitem{302} See Kyllo v. United States, 121 S. Ct. 2038, 2043, 2046 (2001).
\bibitem{303} See Independent Review of Carnivore, \textit{supra} note 43, at 3-1 to 3-2.
\bibitem{304} Although the judiciary increasingly fashions injunctive, forward-looking remedies for controversies between less specific parties over events that have not yet happened, this type of prospective, general rulemaking is typically the province of the legislature.
\bibitem{305} See \textit{supra} note 21; see also Office of Technology Assessment, U.S. Congress, Criminal Justice, New Technologies, and the Constitution 9 (May 1988). This report explains:

Many new science-based technologies have similar effects which could degrade constitutional protections:

- They increase the ability of government to observe, control, or intervene in the affairs of an individual singly, rather than with large groups or the public as a whole; this could erode the effectiveness of constitutional restraints based on common law formulations.

- They allow investigation or surveillance at a distance, or out of sight of both the subject and concerned public interest groups; generally raising the level of surveillance and narrowing the expectation of privacy in society.

\textit{Id.}

\bibitem{306} See \textit{supra} notes 44-47 and accompanying text.
\end{thebibliography}
Americans knew what Carnivore was. While this transparency significantly benefits crime-fighting, it also increases the risk of misuse, since it greatly decreases accountability.

As the incident at the Super Bowl aptly illustrates, the full measure of the impact of these surveillance technologies is their capability when integrated with other technologies, in particular computer storage and processing. A prime example of the significant synergy of multiple surveillance technologies is the "Echelon" worldwide Internet-monitoring system purportedly operated by the U.S. National Security Agency. As Professor A. Michael Froomkin described in a recent law-review article, Echelon consists of technology which recognizes specific pre-determined voiceprints, "so-called dictionary programs that flag messages with interesting references or word patterns," and voice-recognition software to translate spoken words that can be sorted, analyzed, and retrieved using sophisticated search methods.

The significance of these synergies is that the government can monitor its citizens or conduct surveillance more efficiently and more effectively. Given that costliness has been one important factor...

307. After the controversy about Carnivore, a recent survey by the Pew Internet & American Life Project found that only one in five respondents had heard of Carnivore. See Kornblum, supra note 44.

308. See Diffie & Landau, supra note 20, at 153 ("[T]he very invisibility on which electronic surveillance depends for its effectiveness makes it evasive of oversight and readily adaptable to malign uses.").

309. See supra note 2 and accompanying text.

310. See Froomkin, supra note 48, at 1468-69 ("Databases multiply the effects of sensors. . . . Equally important, databases make it possible to create new information by combining existing data in new and interesting ways."); see also id. at 1477 ("Cameras are also an example of how technologies can interact with each other to multiply privacy-destroying effects. . . . In the near future, however, human observers will become much less important as the task of analyzing still photos and videos will be mechanized."). As one commentator noted about the phenomenon of these synergies:

While surveillance and information technologies each create privacy concerns in their own right, recent technological advances have blurred the distinction between these two formerly separate categories. Surveillance technology now can generate personal information, while personal information can be used for surveillance-like purposes. Merging these two fields of technology heightens privacy concerns beyond the point that either category invokes separately.


311. See Froomkin, supra note 48, at 1482-83 ("The NSA recently received a patent on a computerized procedure that produces a topical summary of a conversation using a 'tree-word-list' to score the text. The patent describes a 'preprocessing' phase that removes 'stutter phrases' from a transcript. Then, a computer automatically assigns a label, or topic description, to the text. The method promises to allow computerized sorting and retrieval of transcripts and other documents based upon their meaning, not just keywords." (footnotes omitted)).
restraining the use of wiretapping,\textsuperscript{312} advances in voice-recognition or text-scanning techniques create the possibility of more affordable means to monitor a wider selection of people.\textsuperscript{313}

Even if so inclined, the courts would be hard-pressed to craft and recraft rules and regulations that keep up with modern surveillance, given the fast pace at which existing technologies are improved and new technologies developed.\textsuperscript{314} In fact, the courts and the Congress have substantially contributed to this gap between technology and regulation.\textsuperscript{315}

Carnivore, the FBI's Internet-sniffing program, illustrates one aspect of how technology is outstripping the law: Technologies which have been deemed not to implicate the Fourth Amendment can be improved or modified so as to enable their use in much more intrusive ways.\textsuperscript{316} Carnivore operates in one of two modes, either "full," which

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{312} See Diffie & Landau, supra note 20, at 193-94.
\item \textsuperscript{313} See id.
\item \textsuperscript{314} Cf. People v. Kramer, 706 N.E.2d 731, 734 (N.Y. 1998) ("The technology moves faster than the law and it is important to law enforcement authorities, but it cannot be allowed to outpace the array of checks and balances and protections affecting these privacy intrusions, important to individuals and society at large."). Despite this observation about technology and the law, the New York Court of Appeals in Kramer went on to soften a rule the court had devised five years earlier for ensuring the appropriate legal use of pen-register devices that also could be modified to intercept telephone conversations. See infra notes 324-327 and accompanying text.
\item \textsuperscript{315} See supra notes 243-47 and accompanying text for a discussion of measures the Congress has taken to steadily loosen the rules on wiretapping since it first enacted Title III in 1968. Similarly, the courts have identified several circumstances, such as the search or random drug-testing of students by school administrators, where the requirements imposed for conducting a search are less stringent. See Buffaloe, supra note 142, at 533-42 (discussing cases of administrative or special-needs searches, where the Supreme Court has dispensed with the requirement that a search be based on probable cause).
\item One commentator recently described seven ways that Title III and the ECPA's "balanced legislative scheme have been watered down by Congress itself and by the judiciary:" 1) the four-fold expansion of crimes for which wiretaps can be used, 2) the steady increase in authorizations and the almost non-existent instance in which a wiretap request has been denied, 3) the steady increase in the average length of a wiretap and the number of calls intercepted (both nearly doubling from 1980 to 1996), 4) the erosion of the requirement that other techniques first be exhausted, 5) the lack of enforcement of the requirement that the surveillance be minimized, 6) the low rate of acceptance of motions by defendants to suppress, 7) the 100% approval for wiretaps under FISA and the increasing reliance by law enforcement on FISA for criminal matters due to its "more flexible" standards. See James X. Dempsey, \textit{Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy}, 8 Alb. L.J. Sci. & Tech. 65, 75-78 (1997). These trends illustrate how wiretapping is no longer perceived as an extraordinary technique to be used in limited situations and under stringent constraints—as it was when Title III was enacted in 1968. See id.
\item \textsuperscript{316} As Justice Scalia noted in \textit{Kyllo}, the thermal imager at issue in that case was a relatively rudimentary version of the technology. See supra note 77 and accompanying text. Had the minority garnered one more vote—i.e., so that the use of a thermal imager on a house would not have constituted a search—it seems likely that law-
reveals the entire message, including both content and addressing information; or "pen," which reveals just the addressing information in the electronic message.\textsuperscript{317} These distinctions are significant,\textsuperscript{318} and, accordingly, there are different standards that the FBI operator of Carnivore must meet depending on whether the operator is using the program in "full" or "pen" mode.\textsuperscript{319} However, Carnivore contains two features which together make it impossible for anyone scrutinizing a Carnivore search to determine which mode the operator was using. First, the operator can easily switch between "pen" and "full" modes by merely selecting a radio button on the computer screen;\textsuperscript{320} second, the program does not keep track of the search.\textsuperscript{321} In effect, the operation of Carnivore in conformity with the law is entirely at the discretion of the operator, since the operator's actions are untraceable and unaccountable. Thus, the oversight by a judge of the FBI's surveillance activities, upon which the \textit{Independent Technical Review of the Carnivore System} places considerable reliance for ensuring its proper use,\textsuperscript{322} can be easily circumvented.\textsuperscript{323}

Similarly, pen registers can be easily modified to collect not only addressing information but also the content of telephone conversations.\textsuperscript{324} When initially confronted with this issue, the New enforcement agents would have interpreted the decision as the green light to use the more sophisticated version of thermal imagers.

\textsuperscript{317} Independent Review of Carnivore, supra note 43, at ix.

\textsuperscript{318} See supra notes 203-05 and accompanying text for a discussion of the Supreme Court's ruling in \textit{Smith v. Maryland}, a few years after \textit{Burger} and \textit{Katz}, that the use of pen registers does not implicate the Fourth Amendment because a person does not have a subjective expectation of privacy in the telephone number he or she dials.

\textsuperscript{319} According to FBI policy, an operator must adhere to the stricter requirements of Title III of FISA when using "full" mode and must follow the less stringent procedures of 18 U.S.C. §§ 3121-3124 when using "pen" mode. See \textit{Independent Review of Carnivore}, supra note 43, at 3-1 to 3-5.

\textsuperscript{320} See id. at xi; see also id. at xiv (recommending "separate versions of Carnivore for pen register and full content collection").

\textsuperscript{321} See id. at ix ("All users are logged in as 'administrator' and no audit trail of actions is maintained."); see also id. at xiii ("IITRI did not find adequate provisions (e.g., audit trails) for establishing individual accountability for actions taken during use of Carnivore.").

\textsuperscript{322} See id. at 3-6 ("Judicial involvement is pervasive, and minimizes the risk that electronic surveillance will be unnecessary, overbroad, or too lengthy."). The report also cites internal checks developed by the FBI (such as "intensive training for personnel") and oversight by Congress as additional assurances of proper usage. See id.

\textsuperscript{323} Furthermore, the report noted that "the advertised functionality provides ample capability to perform unauthorized surveillance"—such that the contractor did not evaluate whether there were any additional capabilities hidden in the source code. See id. at xi.

\textsuperscript{324} See People v. Kramer, 706 N.E.2d 731, 733 (N.Y. 1998) ("The pen register devices... had the capacity to intercept and record either digital or aural transmissions, depending on whether they were set for 'audio off' or 'audio on.' The switch from one mode to the other could be accomplished by a technician adjusting a switch . . ."); People v. Bialostok, 610 N.E.2d 374, 378 (N.Y. 1993) (holding that it was improper for the police to install devices that were allegedly used only as pen
York Court of Appeals devised a *per se* rule that any pen register that had the capability of being modified to intercept conversations had to meet the stricter requirements of wiretaps under New York law. In *People v. Bialostok*, Acting Chief Judge Simons wrote for an unanimous court:

This Court has consistently recognized the "insidiousness of electronic surveillance" .... As we said [in *People v. Gallina*, 66 N.E.2d 216 (N.Y. 1985)], "that no unauthorized eavesdropping may have occurred is beside the point, because it is the potential for abuse that is the focus of analysis." In light of ... the potential for abuse embodied in the technology used here, we distinguish this more sophisticated technology from earlier pen registers. The traditional pen register [considered in *Smith v. Maryland*] was, to large extent, self-regulating. Neither through police misconduct nor through inadvertence could it reveal to anyone any information in which the telephone user had a legitimate expectation of privacy. The same is not true of the device used here. This is a technology that has the capacity, through willful use or otherwise, to intrude on legitimately held privacy, and it is the warrant requirement, interposing the Magistrate's oversight, that provides to citizens appropriate protection against unlawful intrusion.

However, the Court of Appeals has since replaced Bialostok's *per se* rule with a fact-specific, case-by-case approach in which judges weigh such factors as the ease with which the device can switch between pen and full modes ("digital to audio capability") and "its susceptibility to evasion of statutory, precedential, and even constitutional protections."

2. Sanctions Against Misuse Are Weak

It is one thing for the Constitution to proclaim that any governmental search and seizure must be reasonable; it is another to ensure compliance. As mentioned above, the principle mechanism for ensuring compliance with the dictates of the Fourth Amendment is the exclusionary rule, whereby evidence obtained by improper means is excluded from a criminal prosecution of the individual subject to an

---

325. See *Bialostok*, 610 N.E.2d at 378 (holding that pen registers that could be modified to monitor telephone conversations required a warrant based on probable cause under N.Y. law and that evidence gathered with a modifiable pen register should have been suppressed even when the pen register was not used to intercept conversations). In its recently promulgated standards on electronic surveillance, the ABA recommended that "[w]hen a particular surveillance device makes use of more than one regulated technology and the technologies are governed by differing rules, the more restrictive rules should apply." ABA Standards for Electronic Surveillance, *supra* note 67, Standard 2-9.1(d)(iii).

326. *Bialostok*, 610 N.E.2d at 377-78 (internal citations and alterations omitted).

327. *Kramer*, 706 N.E.2d at 737.
improper search or seizure.\textsuperscript{328} A second protection is the possibility of criminal and civil sanctions against government agents who violate a person's rights. However, both of these mechanisms are extremely porous, particularly when applied to the use of surveillance technologies, ultimately making the protections of the Fourth Amendment quite ephemeral.\textsuperscript{329}

The first mechanism for preventing abuse of high-tech surveillance, the exclusionary rule, suffers from several serious shortcomings. Because courts and law enforcement perceive that the exclusionary rule often operates to exclude highly relevant and powerful evidence of guilt,\textsuperscript{330} they have crafted several ways around the austere rule. For

\textsuperscript{328} For example, in \textit{Katz} v. \textit{United States}, 389 U.S. 347 (1967), the law-enforcement officers' surveillance tapes were excluded as violative of the Fourth Amendment even though they apparently took all diligent precautions short of obtaining a search warrant. \textit{Id.} at 354; see Stephen Saltzburg, \textit{National Security and the Fourth and Fifth Amendments}, in John Norton Moore et al., \textit{National Security Law} 1001, 1003 (1990) ("\textit{Katz}... illustrates the preference for a warrant even where executive officials conducted themselves otherwise reasonably without judicial supervision.").

A Special Committee of the American Bar Association that assessed the validity of this perception that the exclusionary rule "seriously handicaps law enforcement" concluded that:

\textquote{[T]he prosecutors and police the Committee interviewed... do not believe that the Fourth Amendment rights or their protection via the exclusionary rule are a significant impediment to crime control. The exclusionary rule is applied to only a relatively small percentage of arrests and searches made by the police. A number of observers, including police officials, also report that the demands of the exclusionary rule and the resulting police training on Fourth Amendment requirements have promoted professionalism in police departments across this country. Thus, the exclusionary rule appears to be providing a significant safeguard of Fourth Amendment protections for individuals at modest cost in terms of either crime control or effective prosecution.}

Special Committee on Criminal Justice in a Free Society, ABA, Criminal Justice in Crisis 11 (1988).


The case of \textit{Master} v. \textit{FBI}, 926 F. Supp. 193 (D. D.C. 1996), illustrates the difficulty of pursuing either criminal or civil sanctions against a law enforcement agency suspected of illegal wiretapping. The plaintiffs, suspecting that members of the Cleveland police had conducted illegal wiretaps on them, sought help from the FBI to investigate. \textit{Id.} at 194-95. After being told by the FBI on several occasions and at several levels that the claim was without merit, Master filed a request pursuant to the Freedom of Information Act. \textit{Id.} at 195. When the FBI withheld from the plaintiffs certain documents that it indicated were responsive to the request, the plaintiffs sought an \textit{in camera} review of these records. \textit{Id.} The court rejected this request and dismissed the plaintiffs' case. \textit{Id.}

\textsuperscript{330} See CRS, Constitution of the United States, \textit{ supra} note 147, at 1264-65 ("For as long as we have had the exclusionary rule, critics have attacked it, challenged its premises, disputed its morality."). As Professor Amar wrote:

The exclusionary rule renders the Fourth Amendment contemptible in the eyes of judges and citizens. Judges do not like excluding bloody knives, so
example, courts have created several exceptions to the rule—such as the good-faith exception,\textsuperscript{331} the independent-source doctrine,\textsuperscript{332} and the plain-view doctrine—whereby evidence obtained without a proper search warrant and thus in violation of the Fourth Amendment is still admitted into evidence against a suspect. Second, judges are loathe to exclude highly valuable—usually highly incriminating—evidence based on a technical violation of a warrant.\textsuperscript{333} Further, the exclusionary rule is inapplicable in judicial proceedings such as criminal sentencing, grand jury proceedings, and civil tax proceedings and thus illegally obtained evidence is admissible for "collateral uses."\textsuperscript{334}

In theory, the government must receive authorization from a neutral judge to conduct an activity that the Court has deemed a

they distort doctrine, claiming the Fourth Amendment was not really violated. In the popular mind, the Amendment has lost its luster and become associated with grinning criminals getting off on crummy technicalities.

Amar, supra note 142, at 799.

331. See CRS, Constitution of the United States, supra note 147, at 1267; see, e.g., United States v. Hall, No. 99-6056, 2001 U.S. App. LEXIS 8836 (6th Cir. May 2, 2001). The good-faith exception to the exclusionary rule derives from United States v. Leon, 468 U.S. 897, 923 (1984), where the Supreme Court permitted the admission of evidence obtained by the police "through objective good faith reliance on a facially valid warrant that is later found to lack probable cause." Carmen R. Parcelli, The Exclusionary Rule, 88 Geo. L.J. 1043, 1046 (2000). "The Court concluded that a 'good faith' exception to the exclusionary rule was proper because under such circumstances suppression would not advance the exclusionary rule's goal of deterring official misconduct." Id.

332. See Costello v. United States, 365 U.S. 265, 278-80 (1961) (holding that defendant's admission of past bootlegging was admissible when questioner got information both from illegal wiretap and grand jury transcript); see, e.g., Hoover v. Leonardo, 91-CV-1211, 1996 U.S. Dist. LEXIS 22549 (E.D.N.Y. June 17, 1996). See generally Parcelli, supra note 331, at 1053 (gathering cases on development of the independent-source doctrine). In the context of powerful clandestine surveillance, this exception seems poised to swallow the rule: How can the assertion by a police officer that an important piece of evidence was discovered independently and properly rather than from an illegal wiretap ever be tested or contested? See Buffaloe, supra note 142, at 530-31 ("[T]he newly created 'special needs' exception to the warrant and probable cause requirements . . . is so broad and far-reaching that it is poised to turn the warrant preference rule on its head."); cf. Melvyn Zarr, The Bill of Rights and the Police 33-34 (2d ed. 1980) ("This phenomenon [of police lying] is well known among members of the Bar and the police. In a ludicrously high number of cases, the police have overcome a defendant's motion to suppress illegally seized narcotics by testifying that the defendant, when approached by the police officers, reached into his pocket, dropped the narcotics on the ground and attempted to flee."); James Sterngold, Police Corruption Inquiry Expands in Los Angeles, N.Y. Times, Feb. 11, 2000, at A16 (revealing that "perhaps 100 cases might have been tainted by planted evidence, false testimony or other police abuses").

333. See, e.g., United States v. Squillacote, 221 F.3d 542, 554-57 (4th Cir. 2000) (holding that FBI agents remaining in premises overnight for six nights even though warrant authorized a search from 6 a.m. to 10 p.m. did not violate warrant and even if it did exclusion would be inappropriate).

334. Parcelli, supra note 331, at 1055.
search or seizure and thus under the Fourth Amendment. However, the exclusionary rule is “only effective if there is a proceeding in which the government desires to use the evidence. As long as the evidence is used outside the courtroom, exclusion is not an available sanction.” Thus, the exclusionary rule is meaningless where the purpose of surveillance is information-gathering—as, for example, against political dissidents and rivals or to lead law enforcement to admissible evidence. Indeed, Watergate, one of the most notorious examples of illegal wiretapping in American history, occurred a mere four years after Congress enacted Title III.

The extent to which technologies that are deemed to be a search or seizure are used for intelligence-gathering purposes, and without a warrant, is impossible to know; nevertheless, several privacy-rights advocates have pointed out that although the total number of authorized wiretaps nationally, both federal and state, in 1999 was 1350, the FBI sought, pursuant to CALEA, the capacity to simultaneously intercept 136,000 conversations, for wiretaps and dialed-number recorders in the Los Angeles area alone.

The effectiveness of the exclusionary rule is borne out by history, which is replete with instances of discomforting abuse by law-enforcement agents, especially in the area of clandestine surveillance. As Professor Akhil Reed Amar noted in an influential

335. See supra note 242 (discussing the law-enforcement officer’s perspective on the process and pitfalls of applying for an electronic wiretap). From 1989 through 1999, federal and state law enforcement officials sought authorization for 11,615 wiretaps, of which three were denied. See Wiretap Report 1999, supra note 26, at 32 tbl.7.

336. Saltzburg, supra note 328, at 1028.

337. See Diffie & Landau, supra note 20, at 157-65; Thomas I. Sheridan III, Electronic Intelligence Gathering and the Omnibus Crime Control and Safe Streets Act of 1968, 44 Fordham L. Rev. 331 (1975) (discussing dichotomy between criminal evidence and intelligence and applicability of Title III); cf. Independent Review of Carnivore, supra note 43, at 3-7 (“Note, however, that the availability of an exclusionary rule does not offer direct protection for those not suspected of criminal or foreign intelligence activity who may be caught within the web of surveillance.”).

338. C.f. infra note 501.


340. See Froomkin, supra note 48, at 1484. The FBI had originally sought more capacity (one percent of the total capacity at any given time) but modified its request after arousing controversy. See id.

341. In 1973, Justice Douglas stated that “we live in a regime where the ‘dirty business’ of wiretapping runs rampant” and described the “commonplace” practice of wiretapping as a “disease.” Heutsche v. United States, 414 U.S. 898, 898-99 (Douglas, J., dissenting); see also Dash et al., supra note 182, at 35-285 (describing electronic-surveillance practices by municipal police departments in the U.S. through the mid-1950s); supra note 135 & 193 and accompanying text.

The history of custodial interrogations is also instructive on this theme: Evidence over many years that police officers interrogating suspects in their custody were compelling confessions (often false) eventually led the Court in 1966 to take a very close look at the constitutionality of these custodial interrogations. In the landmark decision Miranda v. Arizona, Chief Justice Warren writing for the Court
law review article on the Fourth Amendment, "[t]hreats to the 'security' of Americans come from both government and thugs."342 The revelation in the late 1950s and 1960s about rampant surveillance by police departments was followed by more discoveries by a congressional committee in the late 1960s and early 1970s that the FBI also conducted widespread illegal wiretapping against prominent political figures and dissidents.343 According to two commentators, "[t]he history of the last five decades shows that attacks on privacy are not an anomaly. When government has the power to invade privacy, abuses occur."344

In an article on ethics, a lawyer in a U.S. federal intelligence agency provides insight into the culture of the intelligence community and its attitude toward civil liberties.345 The author describes the "enormous gap between two almost incompatible ethical (and legal) frameworks: the due process, human rights-oriented constitutional structure of U.S. domestic law, and the grey, harsh realities of power politics."346 The author describes the "enormous pent-up hostility in the intelligence community toward lawyers and legalistic restrictions."347 In addition,

carefully described the possibility of abuse of these inherently coercive interrogations. See 384 U.S. 436, 445-58 (1966). Cases since Miranda underscore the need for continued vigilance. In Cooper v. Dupnik, an innocent suspect was intentionally deprived of his right to counsel and his right to remain silent by police officers who, under pressure to catch a notorious rapist, resorted to terror to elicit a confession. See 963 F.2d 1220, 1225-26 (9th Cir. 1992). Officers described "creating the illusion of hopelessness," mocking the suspect's rights, and lying about evidence to "create stress." Id. at 1225. The Ninth Circuit observed, "[t]his case is an example of officials who deliberately choose to ignore the law and the Constitution in favor of their own methods. For victims caught in their snare, the Constitution of the United States becomes a useless piece of paper." Id. at 1252.

Cooper also illustrates how difficult it is to discipline police officers for manifestly abusive investigative tactics, given the occasional tendency of courts to acquiesce in such misconduct. The Ninth Circuit chided the lower court for its analysis of a suspect's legal rights and its conclusion that the police's behavior did not shock the conscience. See id.

342. Amar, supra note 142, at 818; see also United States v. Kirschenblatt, 16 F.2d 202, 203 (2d Cir. 1926) (Hand, J.) (quoted in Taylor, supra note 139, at 65); cf. 1 Fishman & McKenna, supra note 24, § 1:2, at 1-3 ("To many observers, however, surreptitious monitoring of private conversations conjures images of Nazi Germany, the Soviet Union, and fictional equivalents. The Watergate scandal of the 1970s should suffice to destroy any illusions that the United States is somehow inherently immune from the misuse of these techniques.").

343. See United States v. United States District Court (Keith), 407 U.S. 297, 299 (1972) ("Successive Presidents for more than one-quarter of a century have authorized [electronic] surveillance [in internal security matters] in varying degrees, without guidance from the Congress or a definitive decision of this Court."); supra note 135 and accompanying text.


346. Id.

347. Id. at 91-92 (quoting Richard Willard, Attorney General William French Smith's Counsel for Intelligence Policy).
the author hints at the possibility and the proclivity of agents to side-step procedures designed to ensure oversight.\textsuperscript{348}

A second, though infrequently used mechanism by which the Fourth Amendment is enforced—namely, civil and criminal sanctions against agents—is similarly fraught with problems.\textsuperscript{349} Specifically, it is extremely difficult to mount a successful lawsuit just to find out about illegal surveillance,\textsuperscript{350} let alone to recover damages for infringement.\textsuperscript{351} Professor Saltzburg notes several substantial hurdles to pressing a civil or criminal claim of illegal surveillance. First, it is difficult to learn about illegal surveillance with sufficient certainty to warrant litigation; second, FOIA requests are often easily defeated because of executive privilege; third, the president enjoys absolute immunity against damages, while other executive officers are also immune “unless it is absolutely plain that they violated clearly established legal principles;” and fourth, the case may not be justiciable.\textsuperscript{352} Unlike private citizens culpable of illegal surveillance, police officers can claim the common-law defense of good faith, while “[f]ederal officers are entitled to qualified immunity based on an objectively reasonable belief that a warrantless search later determined to violate the Fourth Amendment was supported by probable cause or exigent circumstances.”\textsuperscript{353}


In other legal contexts, the question of reasonableness is typically decided by the jury, as representatives of the general public—such as the reasonableness in the context of tort claims.\textsuperscript{354} In the late

\textsuperscript{348} Id. at 91 (“Ignoring counsel’s advice and thereby, circumventing the entire Office of General Counsel, is eminently possible in such an organized, tightly compartmentalized society.”); see also Diffie & Landau, supra note 20, at 3 (stating that police and intelligence agencies that conduct wiretapping “regard their activities as a natural prerogative of the state, necessary for an orderly society”); Duncan Campbell, COMINT, privacy and human rights (Paper 3, May 5, 2001) http://www.heise.de/tp/deutsch/special/ecb/7748/l.html (“Sigint [signals intelligence], which comprehensively attacks the privacy of such communications, remains—unlike domestic wiretapping in most countries—unregulated and beyond the reach of most national jurisdictions.”) (on file with the Fordham Law Review).

\textsuperscript{349} See Amsterdam, supra note 290, at 360, 448 n.138 (“The substantive fourth amendment rules are enforceable, to some extent, by civil and criminal actions against officers who violate them. But such actions are seldom maintained, nor are they, as a practical matter, maintainable [due to ‘assorted legal difficulties . . . and a familiar litany of practical impediments’]; and the primary instrument for enforcing the fourth amendment has long been the exclusionary rule . . . .”).

\textsuperscript{350} See supra note 329 (discussing Master v. FBI, 926 F. Supp. 193 (D. D.C. 1996)); see also Saltzburg, supra note 328, at 1028. Intuitively, it will become increasingly difficult for citizens to know when, where, and how the government is tracking their movements and words as the modern means for surveillance become increasingly smaller and more powerful. See supra note 305 and accompanying text.

\textsuperscript{351} See Saltzburg, supra note 328, at 1029.

\textsuperscript{352} Id. at 1028-29.

\textsuperscript{353} See CRS, Constitution of the United States, supra note 147, at 1258.

\textsuperscript{354} Cf. Amar, supra note 142, at 818 (“‘Reasonableness’ is largely a matter of
eighteenth century, the question of the reasonableness of a search or seizure by a governmental agent was decided by juries. However, since then, the role of juries has been largely read out of Fourth Amendment jurisprudence and has been replaced by judges instead, who predominantly decide the reasonableness of searches and seizures by authorizing search warrants and decide how broadly the Constitution sweeps as technological advances create new surveillance and monitoring capabilities for the government generally and law enforcement in particular. However, the appropriateness of having the judiciary gauge the general public's perception about what is a search or seizure and what is a reasonable search or seizure has been called into question.

common sense, and the jury represents the common sense of common people.

Other commentators have stated:

We believe that the term "reasonable" in the Fourth Amendment is infused with meaning by a societal convention about the proper scope of the government's power to conduct searches and seizures, or, turning the concept around, a convention about the scope of privacy against these governmental intrusions. We will call this the "Fourth Amendment privacy convention." To let judges decide what "reasonable" means is implicitly to conclude that judges are better suited to perceive this convention than juries. This proposition is not self-evident.


See Amar, supra note 142, at 771-72. Professor Amar notes that juries continued to play this role through the nineteenth century as well. See id. at 818 n.228.

See supra note 286 and accompanying text. Three rules in particular bear out that the judiciary has permitted this increase in governmental surveillance power: First, the courts have weakened the common-law requirement that the subject of a search be given notice of the search at the time of or shortly afterwards. See 1 Carr, supra note 25, § 2.5(c)(4), at 2-33 to 2-38 (describing how Congress and the courts have dulled the notice component of searches and seizures). In its Berger decision, the Supreme Court "acknowledged the obvious fact that pre-surveillance notice would eliminate the likelihood of success." Id. § 2.5(c)(4), at 2-33. The wiretap law Congress enacted shortly after Berger permits the target to be notified within 90 days, see 18 U.S.C. 2518(8)(d) (1994), and "courts have generally treated the ninety-day maximum as a minimum requirement." 1 Carr, supra note 25, § 2.5(c)(4)(B), at 2-35. Further, what the government is required to notify the target of under Title III is "little more than a notification of the fact that surveillance occurred"—in contrast to the detailed written inventory of all items seized for non-surveillance searches and seizures. Id. § 2.5(c)(4)(C), at 2-36 to 2-37. Second, the courts have greatly expanded the use of warrants—making judge-issued warrants the measure of the reasonableness of a search or seizure and expanding warrants to allow the gathering of "mere evidence"—which enables law-enforcement officers to collect more information while increasing their immunity from civil or criminal sanctions for improper searches and seizures. See supra notes 350-353 and accompanying text. Third, the exclusionary rule, which is the primary mechanism for compliance with the Fourth Amendment, is limited in scope—i.e., its effect exists only when the evidence or information improperly gathered will be used in court and courts have carved out numerous exceptions—and it is weakly applied. See supra notes 330-337 and accompanying text.

See Rosen, The Unwanted Gaze, supra note 178, at 62-63 ("It's not surprising that Supreme Court justices, who are secluded in a marble palace and have spent most of their careers in the cosseted solitude of lower courts and universities, aren't terribly good at predicting how much privacy ordinary Americans expect in the
In this high-technology age, linking the protections of the Fourth Amendment to a person's reasonable expectation of privacy is a prescription for the inexorable and continued erosion of the right protected by the Fourth Amendment. Professor Amsterdam articulated this premise in an article in 1974; he noted that a subjective expectation of privacy could easily be eroded by government announcing a new surveillance technique on television. In Kyllo, the Court acknowledged the criticism of the reasonable-expectation-of-privacy test: "The Katz test... has often been criticized as circular, and hence subjective and unpredictable." Professor Lewis R. Katz has argued that the Supreme Court has "permitted police surveillance powers to grow almost unchecked to their present epic proportions." According to Professor Katz, "[a] partial cataloging of the surveillance techniques declared to fall outside the scope of fourth amendment protection reads like an arsenal of government power one might associate with the authority of a police state."

Given the judiciary's tendency to overestimate the governmental interest vis-à-vis the citizenry's liberty interest when confronted with the issue in the context of criminal prosecutions, several workplace.

358. See Amsterdam, supra note 290, at 384. The Court subsequently addressed Professor Amsterdam's hypothetical in a footnote to Smith v. Maryland, 442 U.S. 735 (1979). Justice Blackmun explained:

Situations can be imagined, of course, in which Katz' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

Id. at 740 n.5.

359. Kyllo v. United States, 121 S. Ct. 2038, 2043 (2001); see also Julie, supra note 291, at 132 ("Another common criticism of Katz's reasonable expectation of privacy test is that it is circular; as the argument goes, the Supreme Court protects only those expectations that are reasonable, while the only expectations that are reasonable are those which the Supreme Court is willing to protect.").

360. Katz, supra note 286, at 549.

361. Id. at 551.

362. See Rosen, The Unwanted Gaze, supra note 178, at 34 ("Judges have a natural tendency to favor the state when balancing the interests of prosecutors against the interests of criminals, and any society that ties its privacy to the rights of the accused is a society in which the legal protections for privacy will quickly evaporate.").
commentators have called for the reinsertion of the perspective of the general public. As one commentator recently wrote:

In many cases, people have an objectively valid expectation of privacy that the Court, by judicial fiat, has deemed unjustifiable. We need more independent mechanisms for protecting privacy—such as grand juries or other popularly accountable bodies—which can balance the claims of the police against the privacy of individuals . . . .”363

According to other commentators, “only society can resolve the normative antimony between the Fourth Amendment security against government action and the security against crime that depends, in part, on government action.”364

B. Constitutional Problems with the Regime

The Court’s jurisprudence of the Fourth Amendment, both with specific respect to modern surveillance technologies and generally, has been criticized by many commentators365—indeed the Supreme Court recognizes the inconsistency of the jurisprudence in this area.366 As one prominent constitutional scholar wrote, “[t]he Fourth Amendment today is an embarrassment. . . . The result is a vast jumble of judicial pronouncements that is not merely complex and contradictory, but often perverse. Criminals go free, while honest citizens are intruded upon in outrageous ways with little or no real remedy.”367

1. A Government of Limited Powers

The Constitution, the instrument that the early citizens of America created in 1787 to organize its new government, created a government

363. See id. at 63.
364. Thomas & Pollack, supra note 354, at 163; see also id. at 149 (“We also argue that the best way to determine the nature of the relevant convention is to involve society in the inquiry.”).
365. See, e.g., Amar, supra note 142, at 759 (“Fourth Amendment case law is a sinking ocean liner—rudderless and badly off course—yet most scholarship contents itself with rearranging the deck chairs.”), 761-800 (stating the substance of the critique); Amsterdam, supra note 290, at 349 (commenting that “[f]or clarity and consistency, the law of the fourth amendment is not the Supreme Court’s most successful product” and noting similar pronouncements by other commentators); Katz, supra note 286, at 549 (“[T]he Court has permitted police surveillance powers to grow almost unchecked to their present epic proportions. Today in America, the police may target any individual for scrutiny—for good reason, for bad reason or for no reason at all. They may use any number of sophisticated surveillance techniques without judicial authorization or review.”); cf. Saltzburg, supra note 328, at 1028-29.
366. See Amsterdam, supra note 290, at 349 (discussing Supreme Court’s own criticism of its Fourth Amendment jurisprudence); see, e.g., Coolidge v. New Hampshire, 403 U.S. 443, 483 (1971) (“[I]t would be nonsense to pretend that our decision today reduces Fourth Amendment law to complete order and harmony.”).
of limited powers.\footnote{368} However, nowhere in the text of the original Constitution is this axiom explicitly stated.\footnote{369} Instead, it is largely supplied by the context in which the United States of America and the Constitution arose and the writings of its principal authors, and by the Ninth and Tenth Amendments.\footnote{370}

The U.S. Constitution that we have today is the Founders' second attempt at a government. Since it was generally clear to all that the central government created by the first instrument, the Articles of Confederation, lacked sufficient power in key areas, the delegates to the Constitutional Convention emerged with a whole new document rather than amendments to the Articles.\footnote{371} Though seeking a stronger central government, they were nevertheless still wary of tyranny.\footnote{372} Moreover, they recognized the need to structure a government that would minimize the inevitable vices of faction and of oppression of the minority at the hands of the majority.\footnote{373} Accordingly, they devised

\footnote{368. As stated by Professor Amsterdam, “The Bill of Rights in general and the fourth amendment in particular are profoundly anti-government documents. They deny to government... desired means, efficient means, and means that must inevitably appear... to be the absolutely necessary means, for government to obtain legitimate and laudable objectives.” Amsterdam, \textit{supra} note 290, at 353. According to another commentator, “The objects sought by the American people in their aspirations for the preservation of their liberties are well stated in the Preamble to the Constitution. But while the scope of these objectives recognizes the unlimited power of the people, the Constitution itself imposes severe limitations upon the government.” Sol Bloom, United States Sesquicentennial Commission, \textit{The Story of the Constitution} 33 (1937). Professor Erwin Chemerinsky has stated that “[a] basic principle of American government is that Congress may act only if there is express or implied authority to act in the Constitution.” See \textit{Erwin Chemerinsky, Constitutional Law: Principles and Policies} 166 (1997). Professor Chemerinsky then notes that states, unlike the federal government, have police powers—that is, “state and local governments [can] adopt any law that is not prohibited by the Constitution.” \textit{Id.} Professor Katz has argued that the Supreme Court's current approach—namely, “using the privacy test in a way that favors the exercise of unreviewable government power”—“runs counter to the other great theme of the fourth amendment: \textit{that ours is a system of limited government}.” Katz, \textit{supra} note 286, at 554 (emphasis added).

369. Chemerinsky, Constitutional Law, \textit{supra} note 368, at 3. Professor Chemerinsky notes, “The implication [of vesting legislative power in Congress] is that Congress can act only if there is clear authority, with all other governance left to the states. But this is not made explicit in the text. Indeed, it was probably this lack of clarity that inspired the Tenth Amendment....” \textit{Id.}

370. \textit{Cf.} Bloom, \textit{supra} note 368, at 34 (“But as a further precaution the people reserved to the States and to themselves all powers that were not entrusted to the national government...”).

371. \textit{See} Chemerinsky, Constitutional Law, \textit{supra} note 368, at 9-10; CRS, Constitution of the United States, \textit{supra} note 147, at XX (“The convention [in Philadelphia in 1787] had been called to revise the Articles of Confederation. Instead, it reported to the Continental Congress a new Constitution.”).


373. \textit{See} Robert W. Scheef, Note, “Public Citizens” and the Constitution: Bridging the Gap Between Popular Sovereignty and Original Intent, 69 Fordham L. Rev. 2201, 2223 (2001) (“The Constitution controls faction in order to prevent a recurrence of the majoritarian tyrannies of the Critical Period [i.e., from the late 1770s through the
a government structure that, though able to effectively govern, would still "protect individual liberties." Further, the Founders relied on the interplay between the states and the federal government to protect citizens' liberties.

Although there was consensus that the federal government required more power, there was sharp disagreement about how much power to give and how to demarcate the boundary of this authority. Specifically, those generally opposed to a strong central government, the anti-federalists, sought the inclusion of a Bill of Rights "to prevent the new federal government from taking away individual rights." States dominated by anti-federalists signed the Constitution on the condition of a Bill of Rights. The federalists, by contrast, disfavored a Bill of Rights, claiming in Alexander Hamilton's words that they "are not only unnecessary in the proposed Constitution but would even be dangerous." To the federalists, individuals' liberties were sufficiently protected by the Constitution, which was by its very nature a powers-limiting instrument; the enumeration of rights, however, was an implicit invitation for government to go where it had not been explicitly prohibited. James Madison eventually prevailed on other federalists to accept the Bill of Rights and formulated the Ninth and Tenth Amendments to clarify the significance of the other amendments in light of the Federalists' prediction that it would invite the government to intrude on citizens' liberties and rights.

The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." After it was inserted, the Ninth Amendment sunk into obscurity and for nearly 160 years was

1780s.

374. See Chemerinsky, Constitutional Law, supra note 368, at 4; see also Laurence H. Tribe, American Constitutional Law § 15-3, at 1308 (2d ed. 1988) ("Human beings are of course the intended beneficiaries of our constitutional scheme.").

375. See Tribe, supra note 374, at 18-22.

376. See Wood, supra note 372, at 536-47 (discussing the disagreements between the federalists and the anti-federalists over the new constitution).


379. The Federalist No. 84 (Alexander Hamilton). See generally Wachtler, supra note 378, at 602 ("Like [James] Wilson, Hamilton argued that a bill of rights was not only unnecessary to secure fundamental rights, but also potentially dangerous.").

380. See Herberg, supra note 377, at 205 ("Since the Constitution gave no authority to the federal government to take away individual liberties, it stood to reason that the federal government could do no such thing.").

381. See Ely, supra note 13, at 34-36 (describing James Madison's view of a Bill of Rights); Herberg, supra note 377, at 205; Wachtler, supra note 379, at 600.

382. See infra note 385.

383. See infra note 395.

384. See Tribe, supra note 374, § 11-3, at 774-75.

385. U.S. Const. amend. IX.
rarely invoked.” Although the Ninth Amendment regained some notoriety in 1965 when Justice Douglas, writing for the majority, invoked it—albeit cautiously—in striking down a Connecticut law that forbade the use of contraceptives by married couples in Griswold v. Connecticut. more recently it has become mired in controversy over the proper role of judges in deciding such politically divisive issues as the rights to abortion and to sexual freedom. This debate centers on whether the Ninth Amendment permits the creation of other rights that are not included in the Constitution or its first eight amendments or whether it merely “mak[es] clear that a Bill of Rights might not by implication be taken to increase the powers of the national government in areas not enumerated.” Although arguing that the language of the Amendment supports the former view, Professor John Hart Ely states that the latter view is the “received account.” Even as a “rule of construction,” the Ninth Amendment states an important constitutional principle—namely that the powers conferred on the federal government by the Constitution must accede to certain liberties of the people—which is largely unrealized.

Like the Ninth Amendment and to some extent in conjunction, the Tenth Amendment also has aspects of a rule of construction—
i.e., it serves to give meaning to other portions of the text. The Tenth Amendment provides: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." The Tenth Amendment is also susceptible to two interpretations. According to Professor Chemerinsky, until the late eighteenth century and again from 1937 until 1990, the Court "viewed the Tenth Amendment simply as a reminder that Congress must have authority under the Constitution in order to legislate, not as a judicially enforceable limit on the legislative power." Thus, so long as Congress had the power in a given area, it could essentially do what it wanted, constrained only by political processes and pressures. However, in the last decade the Supreme Court appears to have revived an interpretation of the Tenth Amendment that was also prevalent from the late-eighteenth century until 1937—namely, that "the Tenth Amendment reserves a zone of activity to the states for their exclusive control."

2. The Fourth Amendment

The Fourth Amendment was added, along with the rest of the Bill of Rights and the Ninth and Tenth Amendments, four years after the Constitution was enacted. It is generally acknowledged that the Fourth Amendment reflects the Founders' reaction to certain practices by the English that the colonists found particularly reprehensible. Specifically, the Fourth Amendment reflects the colonists' reaction against several laws Parliament enacted that authorized English agents to enter and search private homes and offices with few constraints on the officers' discretion. In addition, the Secretary of State was authorized to issue general warrants for search and seizure of contraband and evidence of seditious libel.

Although the longstanding English practice of authorizing general writs was increasingly disfavored both in America and England, it continued largely unabated until the famous case of John Wilkes

395. U.S. Const. amend. X.
396. Chemerinsky, Constitutional Law, supra note 368, at 226.
397. See id. at 226-27, 231. Professor Chemerinsky quotes Justice Stevens in Garcia v. San Antonio Metropolitan Transit Authority, 469 U.S. 528, 551 (1985), as stating "[t]he political process ensures that the laws that unduly burden the States will not be promulgated." Chemerinsky, Constitutional Law, supra note 368, at 231.
399. See American Criminal Procedure: Cases and Commentary 26 (Stephen A. Saltzburg & Daniel J. Capra eds., 4th ed. 1992) (noting that the Fourth Amendment is an expression of a philosophy against intrusions by the British in colonial America).
401. See id. at 42.
galvanized the consensus against these repressive actions. In 1792, Secretary of State Lord Halifax issued a general warrant to search for the source of a pamphlet harshly critical of the government. Under this warrant, forty-nine people—publishers, printers, and authors who might have been responsible—were arrested before Wilkes, a member of Parliament and the author of the pamphlet, *The North Briton, Number 45*, was found. Wilkes sued and won £4000, a “princely” amount of money.

Several scholars have argued that the current interpretation of the Fourth Amendment differs significantly from the original intent in several critical respects. Generally, as Professor Amar notes, the Fourth Amendment was enacted at a time when centralized government was viewed with considerable skepticism. More substantively, Professors Amar and Taylor have argued that the Founders, generally distrusting warrants, intended the Warrant and Reasonableness Clauses of the amendment to be read disjunctively—in direct contrast to the modern interpretation, in

---

402. See id. at 43. As Professor Amar explained:

> We need only recall the facts of the 1763 English case, *Wilkes v. Wood*, whose plot and cast of characters were familiar to every schoolboy in America, and whose lessons the Fourth Amendment was undeniably designed to embody. *Wilkes*—and not the 1761 Boston writs of assistance controversy, which went almost unnoticed in debates over the federal Constitution and Bill of Rights—was the paradigm search and seizure case for Americans. Indeed, it was probably the most famous case in late eighteenth-century America, period.

Amar, supra note 142, at 772 (footnotes omitted).

403. See Lasson, supra note 400, at 43.

404. See id. at 43-44.

405. See id. at 45; Amar, supra note 142, at 781.

406. See Amar, supra note 142, at 771-73. According to a recent survey, fifty-four percent of Americans favor enabling federal law enforcement to monitor email messages out of concern for Internet-related child pornography, terrorism, fraud, credit card theft, and hacking into government computers. See Kornblum, supra note 44. However, the survey’s respondents also found a concomitant skepticism about government and a desire for privacy laws to protect against “government snooping.” According to this study, which was conducted by the Pew Internet & American Life Project, “[t]rust in government to do the right thing most of the time sank to 31%, from 39% in 1997, 41% in 1988. Of all Americans, 62% want new privacy laws and protections from government snooping.” Id.

407. According to Professor Taylor, several states created their own constitutions after gaining independence in which “the warrant is treated as an enemy not a friend.” Taylor, supra note 139, at 41; see also Amar, supra note 142, at 774 (“In every state constitution prior to the federal Bill [of Rights], the warrant is treated as an enemy, not a friend.” (quoting Taylor)).

408. See Taylor, supra note 139, at 23-24 (stating that the widely-held view, in which “the warrant [is] the touchstone of ‘reasonableness’”—i.e., the two clauses of the Fourth Amendment are read conjunctively—stands “the fourth amendment on its head”); id. at 38-46 (discussing the original intent of the Fourth Amendment); Amar, supra note 142, at 762-63 (arguing that the Amendment’s first “command”—that searches and seizures not be unreasonable—does not “require” the second—that warrants be based on probable cause and narrowly tailored).
which warrants issued by judges are seen as a hallmark of reasonableness.\textsuperscript{409} According to Professor Amar, juries rather than judges and magistrates were ultimately the main arbiters of the reasonableness of searches and seizures; government agents conducted an unreasonable search at peril of a civil suit for damages and early post-colonial juries were highly suspicious of government agents.\textsuperscript{410} Because warrants largely (though not entirely) immunized an agent conducting a search from a subsequent civil suit for damages, warrants were to be granted in rare instances.\textsuperscript{411}

This part of the Note has attempted to show that as Fourth Amendment doctrine has evolved the governmental/law enforcement component has grown steadily more robust and expansive, while the rights component has remained static or has weakened.\textsuperscript{412}

\textsuperscript{409} See supra notes 142-46 and accompanying text.

\textsuperscript{410} See Amar, supra note 142, at 771 ("[J]uries, not judges, are the heroes of the Founders' Fourth Amendment story. Indeed, at times, the Founders viewed judges and certain judicial proceedings with suspicion . . ."). Professor Amar further explained:

Even when a judge issued a warrant, revolutionary Americans greeted the event with foreboding. Prior to the Revolution, American judges lacked the independence from the Crown that their British brothers had won after the Glorious Revolution. Sitting at the pleasure of the monarch, the King's judicial magistrates in America were at times hard to distinguish from His executive magistrates—especially when a single Crown lackey wore several hats, as often occurred. Nor did the foreboding disappear after the Revolution, when American judges won a measure of institutional independence from the executive branch. Even an Article III judge, after all, had been appointed by the President, looked to the President for possible promotion to a higher court, and drew his salary from the government payroll. What's more, such a judge was an official of the central government—perhaps not so imperial as his Crown-directed colonial predecessors, but suspicious nonetheless. Would the handful of elite federal judges truly be able to empathize with the concerns of ordinary folk? And a single bad apple could spoil the bunch; if even one federal judge was a lord or a lackey, executive officials shopping for easy warrants would know where to go. Far more trustworthy were twelve men, good and true, on a local jury, independent of the government, sympathetic to the legitimate concerns of fellow citizens, too numerous to be corrupted, and whose vigilance could not easily be evaded by governmental judge-shopping.

\textit{Id.} at 773 (footnotes omitted).

\textsuperscript{411} See id. at 771-72 ("The Framers did not exalt warrants, for a warrant was issued ex parte by a government official on the imperial payroll and had the purpose and effect of precluding any common law trespass suit the aggrieved target might try to bring before a local jury after the search or seizure occurred.").

\textsuperscript{412} As Justice Brandeis stated in his dissenting opinion in \textit{Olmstead}:

We have... held that general limitations on the powers of Government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the States from meeting modern conditions by regulations which a century ago, or even half a century ago, probably would have been rejected as arbitrary and oppressive. \textit{Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world.} Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting) (emphasis added) (quotations and citations omitted).
Accordingly, the following Part recommends a regime where the government bears more onus for ensuring that all covert, high-technologically-assisted searches and seizures are reasonable.

III._argument_and_proposal

The substance of the Fourth Amendment essentially boils down to this: Law enforcement has virtually unlimited discretion to peer, poke, and prod into the lives of U.S. citizens—even those not suspected of criminal activity—until the public and the courts become aware of and disquieted by a particular technology-assisted law-enforcement practice; if the technology or the practice reaches the Supreme Court and it decrees that technology or practice a search, the law-enforcement officer must then get a warrant if he intends to use the information or evidence in court in a prosecution—otherwise the disincentive for misuse is weak.\textsuperscript{413} Of course, Congress can and has constructed protections which the Court has deemed are not required by the Constitution. Yet, with the costs of the Fourth Amendment in this technological age falling almost entirely on the shoulders of citizens,\textsuperscript{414} and commonly on the criminals and convicts against whom these technologies are most often and most overtly used,\textsuperscript{415} the

\begin{flushright}
413. See Amsterdam, supra note 290, at 388 ("[l]f [a police activity] is not labeled a "search" or "seizure," it is subject to no significant restrictions of any kind. . . . [P]olice activities of any other sort may be as unreasonable as the police please to make them." (endnotes omitted)). Professor Amsterdam further explains:

The question of what constitutes a covered "search" or "seizure" would and should be viewed with an appreciation that to exclude any particular police activity from coverage is essentially to exclude it from judicial control and from the command of reasonableness, whereas to include it is to do no more than say that it must be conducted in a reasonable manner. With the question put in this fashion the answer should seldom be delivered against coverage.

\textit{Id.} at 393 (endnote omitted).

414. See infra text accompanying note 467; \textit{see also} McKnight, supra note 83, at 1264 (proposing the Court re-adopt a rule that the use of thermal imagers is presumptively unreasonable and thereby shift the burden to the government to prove the reasonableness of its actions). The author reasons that:

The Fourth Amendment protects against "unreasonable searches and seizures." Thus, the question to be asked is whether the government activity—the search or seizure—is reasonable. However, the second prong of Justice Harlan's test [concurring in \textit{Katz v. United States}, 389 U.S. 347 (1967)] reverses the focus from whether the government's action is reasonable to whether the citizen's expectation of privacy is reasonable. In effect, this shifts the burden of proof from the government to the citizen to prove "reasonableness." Now, instead of the government having to justify its actions, the citizen is forced to prove that his expectation is one society recognizes as reasonable.

\textit{Id.} at 1262. The author proposes that the Court re-adopt a rule whereby the government bears the burden of proving the reasonableness of its actions. \textit{Id.} at 1262, 1264. He suggests that the court do this by "declar[ing] such warrantless searches presumptively unreasonable." \textit{Id.} at 1264.

415. Criticizing the exclusionary rule as the device for deterring the government
protections of this important piece of the Constitution are extremely fragile.

During the media's coverage of the controversy over the clandestine surveillance at the Super Bowl, a police spokesman said that it is not uncommon for police to experiment with new devices that become available. The officer also noted that people would appreciate the protection that this surveillance provided. Even if this officer's perception accurately reflects the prevailing communal attitude toward privacy, it begs the question whether local law-enforcement agents experimenting with technologies and unilaterally deciding that it does not invade citizens' privacy comports with our larger notions of liberty and with the Constitution. Furthermore, in this high-technology age, linking the protections of the Fourth Amendment to a person's reasonable expectation of privacy is a

from violating citizens' rights, Professor Amar explained:
The criminal defendant is a kind of private attorney general.

But the worst kind. He is self-selected and self-serving. He is often unrepresentative of the larger class of law-abiding citizens, and his interests regularly conflict with theirs. Indeed, he is often despised by the public, the class he implicitly is supposed to represent. He will litigate on the worst set of facts, heedless that the result will be a bad precedent for the Fourth Amendment generally. He cares only about the case at hand—his case—and has no long view. He is not a sophisticated repeat player. He rarely hires the best lawyer. He cares only about exclusion—and can get only exclusion—even if other remedies (damages or injunctions) would better prevent future violations.... He is, in short, an awkward champion of the Fourth Amendment.

Amar, supra note 142, at 796; see also CRS, Constitution of the United States, supra note 147, at 1258 (“[O]n the practical side, persons subjected to illegal arrests and searches and seizures are often disreputable persons toward whom juries are unsympathetic . . . .”); Taylor, supra note 139, at 65 (“[A]s Learned Hand reminded us in Prohibition times: ‘. . . What seems fair enough against a squalid huckster of bad liquor may take on a very different face, if used by a government determined to suppress political opposition under the guise of sedition.’” (endnote omitted)); Katz, supra note 286, at 550 (“The court's answer to [the criminal defendant's] plea [for improperly obtained evidence] will set the level of privacy and freedom for the whole community. Suppression of illegally obtained evidence protects us all, not just those suspected of criminal activity.”).

416. See supra notes 2 and accompanying text.

417. Jack Carey, ACLU Decries Super Bowl Surveillance: Fans, Workers Secretly Taped in High-tech Security Effort, USA Today, Feb. 2, 2001, at 1C (“‘After we saw [the technology offered as an experiment], we thought it would be an asset,’ [Maj. K.C.] Newcomb said. ‘I was fully comfortable that we were not infringing on anybody's rights.’”); cf supra note 290 and accompanying text.

418. Jim Loney, Super Bowl Surveillance Draws Protest from ACLU, The San Diego Union-Tribune, Feb. 2, 2001, at A-15 (“‘If this tool could prevent a terrorist act or something else, I think the tool will be priceless,’ Durkin said. ‘The vast majority of visitors to Raymond James (Stadium) would applaud our efforts to keep it safe for everyone.’”).

419. Cf. Rosen, A Watchful State, supra note 122, at 42 (describing how the head of company developing face-recognition technology said he would not let the technology be used improperly and noting “it seems odd to put the liberties of a democracy in the hands of one unelected scientist”).
prescription for the inexorable and continued erosion of the right protected by the Fourth Amendment. The government's present capabilities for monitoring its citizens are very broad; it seems certain that these capabilities will continue to evolve—so that its surveillance will become faster, more precise, cheaper, more covert, and more intrusive.420

Recognizing that Americans in later ages and in different circumstances might prefer a different balance between governmental power and governmental restraint, the Founders arrived at language that on its face indicates flexibility: searches and seizures cannot be unreasonable.421 The tension between the two important but competing interests balanced in the Fourth Amendment—protection of citizens' liberties and effective governmental authority to maintain peace—must be continually resolved as society faces new challenges and threats.422 In an age of powerful and fast-evolving science and

420. See, e.g., Kenneth Chang, Clever Wiring Harnesses Tiny Switches, N.Y. Times, July 17, 2001, at F1 (discussing a patent issued to Hewlett-Packard for a molecule-based switch for eventual use in memory chips and computer processors); John Markoff, Researchers Make an Ultra-Tiny Chip, N.Y. Times, June 10, 2001, at 42 (discussing the development of "silicon transistors no more than 70 to 80 atoms wide and 3 atoms thick . . . [which] are capable of switching on and off 1.5 trillion times a second") [hereinafter Markoff, Ultra-Tiny Chip]. According to this news report:
The research will make possible computer processor chips with as many as one billion transistors and 20 gigahertz speeds. That is more than 23 times the number of transistors used in Intel's current state-of-the-art Pentium 4 microprocessor, which has 42 million transistors and is capable of executing 1.7 billion instructions a second.

Markoff, Ultra-Tiny Chip, supra. In addition, this new chip will consume significantly less electricity than current microprocessors. Id. The article also describes Moore's Law, which states that "the number of transistors that can be etched on a single chip of silicon doubles on average every 18 months." Id.

421. See Carol S. Steiker, Second Thoughts About First Principles, 107 Harv. L. Rev. 820, 824 (1994) ("[T]he Fourth Amendment, more than many other parts of the Constitution, appears to require a fairly high level of abstraction of purpose; its use of the term 'reasonable' (actually, 'unreasonable') positively invites constructions that change with changing circumstances.").

422. See United States v. United States District Court (Keith), 407 U.S. 297, 314-15 (1972) ("As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."). Justice Powell further explains in Keith:
The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens. . . .

But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development—even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and
technology, the challenge of the Fourth Amendment is to derive maximum benefits from these technologies while keeping their use properly and fully within our norms of liberty. As one hornbook on criminal procedure states, "[e]avesdropping techniques, many of which were probably unforeseen by the framers, raise special problems [about the meaning of searches and seizures]. . . . Courts have used the [Fourth] Amendment to limit some new forms of surveillance, but they have struggled to make the Amendment meaningful in a technological society." To be sure, these technologies can and should be exploited for many important governmental functions; however, equally paramount is the need to properly regulate their use, especially given the sophistication of these technologies and the inevitability of further technological advances. The regime proposed here attempts to fully accommodate these two competing ideals.

The desire to equip local, state, and federal law-enforcement agents with effective tools to maintain peace and order seems to derive its sense of urgency from the highly-publicized campaign to battle drug-trafficking and to rid communities of the social upheaval and violence attendant on the use of narcotics, as well as the threat of terrorism by domestic and international enemies. After the devastating attack on the World Trade Center and the Pentagon, there were renewed calls for broader and stronger surveillance capabilities. Further, apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. Id. at 312.

The attacks on the World Trade Center and the Pentagon on September 11, 2001, and the rash of anthrax contaminations which occurred shortly thereafter appeared to profoundly alter Americans' perceptions about the interplay of civil rights and security. See supra note 6 and accompanying text. Congress quickly took steps to significantly increase the authority of law-enforcement agencies such as the FBI and CIA. See supra notes 271-84 and accompanying text. However, several commentators urged caution, lest "security measures start to corrode the very society they are designed to protect." See The National Defense, Editorial, N.Y. Times, Sept. 12, 2001, at A26 ("Americans must rethink how to safeguard the country without bartering away the rights and privileges of the free society that we are defending. . . . President Bush and Congress must carefully balance the need for heightened security with the need to protect the constitutional rights of Americans.").

425. Such extraordinary events as the bombing of the Alfred P. Murrah Federal Building in Oklahoma City, OK, in April 1995, which killed 168 people and injured more than 700, and of the World Trade Center in New York City in 1993 have clearly had a substantial impact on the nation's sense of its peril and its vulnerability. Several high-profile airplane disasters seem to further galvanize this perception. Louis J. Freeh, FBI, Ensuring Public Safety and National Security Under the Rule of Law: A Report to the American People on the Work of the FBI 1993-1998, at 3-4 (undated).
426. See supra notes 6-7 and 271-84 and accompanying text.
given the potentially disastrous effects of an attack on portions of the
nation’s critical infrastructure, extreme protective measures seem
clearly warranted to protect the nation’s power grid, banking system,
and air-traffic control from either physical or electronic sabotage.\footnote{427}

To be sure, a critical aspect of liberty involves freedom from crime
and personal violence and protection of property, for which effective
and efficient law enforcement is arguably \textit{sine qua non}.\footnote{428} It is
important that law enforcement agencies are sufficiently well
equipped to counter the use by criminals of new tools as they are
developed.\footnote{429} Accordingly, under the broad powers the Constitution
grants to the states to maintain social order\footnote{430} and to the federal

\footnote{427. In 1996, President Clinton signed an Executive Order (“E.O.”) creating a
Fed. Reg. 37,347} (July 17, 1996). Executive Order 13,010 identified as critical
infrastructure the following: “telecommunications, electrical power systems, gas and
oil storage and transportation, banking and finance, transportation, water supply
systems, emergency services (including medical, police, fire, and rescue).” \textit{Id.} (The
E.O. also included “continuity of government” as a critical infrastructure. \textit{See id.})
The E.O. then delineated two types of threats—“physical threats to tangible
property” and “threats of electronic, radio-frequency, or computer-based attacks on
the information or communications components that control critical infrastructures
(“cyber threats”)”—and noted that “many of these critical infrastructures are owned
and operated by the private sector.” \textit{See id.; see also The Clinton Administration’s
Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, at 1
(May 22, 1998).}

In 1998, the FBI established a National Infrastructure Protection Center “to
prevent, deter, respond to, and investigate attacks on the nation’s critical
infrastructure.” \textit{Counterterrorism Threat Assessment and Warning Unit, U.S. Dep’t
http://www.fbi.gov/library/terror/terroris.htm.}

\footnote{428. Sir Robert Peel, who is largely credited with devising the model in 1882 in
London of the modern police force, countered his opponents’ suggestions that such an
organized police would infringe people’s liberty by “asking if liberty ‘... consists[s]
[sic] in having your house robbed by organized gangs of thieves?’” \textit{Christopher
Slobogin, Criminal Procedure: Regulation of Police Investigation 3} (2d ed. 1998)
(quoting George L. Kirkham & Laurin A. Wollan, Jr., \textit{Introduction to Law
Enforcement} (1980)); \textit{see also Saltzburg, supra note 328, at 1001 (“Only in a secure
nation can the rights and liberties guaranteed by the Constitution themselves be
secure.”); Chiarella & Newton, supra note 131, at 25-26 (“No governmental interest is
more fundamental than guaranteeing the security of the nation. Only in a secure
nation can the rights and liberties guaranteed by the Constitution be secure. United
States intelligence activities play a vital role in the protection of national security . . . .
”)}

Similarly, a person wrongfully accused and convicted is most poignantly and
pointedly denied his liberty—so technologies such as DNA analysis, which exculpate
the innocent as much as they inculpate the guilty, have potentially great value in
ensuring our liberty.

\footnote{429. \textit{See supra} note 422.}

\footnote{430. \textit{See generally Philip A. Talmadge, The Myth of Property Absolutism and
L. Rev. 857} (2000). Quoting Madison in \textit{Federalist 45} as stating that “[t]he powers
reserved to the several States will extend to all the objects which, in the ordinary
course of affairs, concern the lives, liberties, and properties of the people, and the
internal order, improvement, and prosperity of the State,” Judge Talmadge noted that}
government to preserve national security, our country has built law-enforcement agencies far beyond what was present when the Constitution was crafted. We also have witnessed the proliferation of federal crimes.

There are also reasons outside of law-enforcement for which increasing control over the populace is sought. The size, diversity, and mobility of the nation's population require means to count, account for, differentiate, and keep track of people for the proper delivery of governmental services with a minimum of waste and fraud. Given these internal and external threats to the nation's security and peace and given the demand for greater governmental services delivered more efficiently and accurately, our society and government should capitalize on these technologies. The regime proposed in this Note assumes that surveillance technologies can and should effectively be used to serve these goals.

“[e]ven the advocates of a smaller federal governmental presence, such as Madison, conceded the need for vigorous exercise of government power by the states.” Id. at 867.

431. See id. at 868. Judge Talmadge noted, “Although the U.S. Constitution does not specifically reference the police power, the Founders envisioned a federal government actively exercising police powers within the sphere of its enumerated powers. The Framers considered the police power an essential attribute of government sovereignty.” Id. (footnotes omitted).

432. See Steiker, supra note 421, at 824 (responding to and criticizing Professor Amar's “intentionalist” reading of the Fourth Amendment). Professor Steiker notes: "At the time of the drafting and ratifying of the Fourth Amendment, nothing even remotely resembling modern law enforcement existed. The invention in the nineteenth century of armed, quasi-military, professional police forces, whose form, function, and daily presence differ dramatically from that of the colonial constabulary...." Id.


Professor Baker cites “the Supreme Court's statement in United States v. Lopez that the Commerce Clause power does not include a general police power to define and punish all crimes,” and notes that “Congress and the Justice Department, however, continue to act as if the federal government has virtually unlimited police powers.” Id. at 674 (footnotes omitted). A report from a commission Congress created in 1997 as part of the Antiterrorism and Effective Death Penalty Act described the proliferation of federal crimes as “startling.” Commission on the Advancement of Federal Law Enforcement, Law Enforcement in a New Century and A Changing World: Improving the Administration of Federal Law Enforcement 2 (2000). The report continued:

In 1789, perhaps a dozen crimes were considered sufficiently serious to warrant Federal attention; today that total exceeds 3,000. Federalizing common crimes—crimes that historically were the responsibility of State and local law enforcement agencies—has placed U.S. society in danger of having Federal law enforcement resources spread much too thinly. If the trend continues, the United States will develop the type of national police force that we have traditionally avoided.

Id.

434. See supra note 126-27 and accompanying text.
Though broad, government's power under the theory of our
government is also limited. While the Constitution affords the states
and the federal government considerable power, the Constitution was
primarily a powers-limiting document, painting with a broad brush
what and how the federal government was to operate.\textsuperscript{435} The Bill of
Rights specifically enumerated those fundamental rights that, in
Justice Cardozo's words, are "the very essence of a scheme of ordered
liberty,"\textsuperscript{436} where the government had to tread lightly, if at all.\textsuperscript{437} As
Chief Justice Burger remarked in \textit{INS v. Chadha},\textsuperscript{438} "[c]onvenience
and efficiency are not the primary objectives—or the hallmarks—of
democratic government."\textsuperscript{439} While society has a justified need for
effective public safety through vigorous prosecution of criminals,\textsuperscript{440} it
is critical that those crafting the policy of surveillance bear in mind
Professor Amar's observation that the citizenry's security is
threatened as much by the government as by criminals.\textsuperscript{441}

\textbf{A. Proposal}

This Note argues that the current regime for surveillance
technologies should be changed in several fundamental ways in order
to keep the spirit of the Constitution and the Fourth Amendment
meaningful in a technological age. Though substantial, the changes
proposed here need not and should not constrict the \textit{lawful}
use of these powerful and promising technologies for legitimate
governmental purposes. Unlawful surveillance, on the other hand,
deserves little quarter. If the unreasonable use of the technologies
cannot be adequately prevented or if no reasonable use can be
articulated, necessarily a technology offends the principle contained in
the Fourth Amendment that the right to be secure from unreasonable
searches and seizures \textit{shall not be violated}. The changes advocated
here are aimed primarily at preventing abuse and misuse of the
technologies, by reckoning fully with several problematic
characteristics of modern surveillance technologies in the current
regime: that many of these technologies are unknown to the general
public because they are inherently intended to be used without

\textsuperscript{435} See Baker, \textit{supra} note 243, at 674; Talmadge, \textit{supra} note 430, at 868 ("The
powers delegated by the proposed Constitution to the federal government are few
and defined.")(quoting The Federalist No. 45).


\textsuperscript{437} See, \textit{e.g.}, \textit{United States v. Playboy Entm't Group, Inc.}, 529 U.S. 803, 813 (2000)
describing how the Court strictly scrutinizes legislation regulating speech by
requiring the regulation to be "narrowly tailored to promote a compelling
Government interest").


\textsuperscript{439} \textit{Id.} at 944.

\textsuperscript{440} See, \textit{e.g.}, \textit{Davis v. United States}, 512 U.S. 452, 461 (1994) (noting law
enforcement is the other side of "the Miranda equation").

\textsuperscript{441} See supra note 342.
detection by citizen-subjects; that they are characterized by rapid
development and are growing increasingly sophisticated; that the
laws in place to regulate the more commonplace forms of
surveillance—such as wiretaps and bugs—fail to reach other
important and powerful ways that government monitors and controls
citizens—such as the many and increasingly interconnected databases
of the federal government; and that there is a substantial
opportunity for and long history of misuse of covert surveillance
technologies. Ultimately, this proposal seeks to shift the
jurisprudence of surveillance from a normative orientation to a
process orientation. One set of important aims of the proposal is to
create broader public recognition of the true extent of the
government's surveillance capability, to create mechanisms for more
open and fuller public discourse about central normative issues (such
as what surveillance is reasonable and what is not), and to integrate
the perspectives of the general public into the decisions about these
normative judgments. A second set of aims is to require the
government to take into account the full and future capabilities of the
technologies and to implement realistic and viable measures to
prevent misuse.

1. Legislative or Administrative Rulemaking

At the heart of this proposal is the adoption by the court of a rule
that the use of technology is per se unreasonable unless the executive
agency or the Congress (or both) have clearly and overtly disclosed its
intended usage and established the rules and regulations governing its
use, especially measures to effectively prevent abuse or misuse.
Building on proposals by several academics, such as Professor
Amsterdam, and recently the American Bar Association, the

442. See supra Part I.A & notes 305-08 and accompanying text.
443. See supra Part I.A.
444. See supra notes 287-303 and accompanying text.
445. See supra note 135 and accompanying text.
446. The centerpiece of Professor Amsterdam's proposal for reform was "that
police discretion to conduct search and seizure activity be tolerably confined by either
legislation or police-made rules and regulations, subject to judicial review for
reasonableness." See Amsterdam, supra note 290, at 409. Professor Amsterdam
explained:
I think that the Court should hold that the fourth amendment requires all
police search and seizure activity to be regulated by legal directives that
confine police discretion within reasonable bounds.... Unless a search or
seizure is conducted pursuant to and in conformity with either legislation or
police departmental rules and regulations, it is an unreasonable search and
seizure prohibited by the fourth amendment.
Id. at 416. Professor Amsterdam indicated a preference for rulemaking, skeptical as
he was about the ability of the legislature to meet this challenge. See id. at 378-79
("The long-time, wholesale 'legislative default' in regulating police practices is no
accident. Legislatures have not been, are not now, and are not likely to become
sensitive to concerns of protecting persons under investigation by the police.").
function and purpose of such a rule would be to force the government—either the executive governmental agencies seeking to use these technologies or the Congress—to be accountable in their use of increasingly sophisticated and unobtrusive technologies; the government would bear the burden in the first instance of defining their reasonable use and implementing measures to prevent misuse. The present jurisprudence of electronic searches and seizures places the burden on the citizen to detect and prove the unreasonable ness of an intrusion. As has been discussed, this arrangement renders the Fourth Amendment almost meaningless in this context, since citizens are rarely able to detect (let alone prove) the use (reasonable or not) of a technology whose success by its nature depends on the unwittingness of its subject.

The contents of these legislative or administrative rules created for these covert surveillance technologies should include at least the following basic elements: First, the rules should clearly and comprehensively describe the technology so that law-enforcement agents, citizens, and judges understand what is at issue. Second, the rules should explain, with meaningful specificity, the reason for the technology's deployment—the goals that justify its use. Third, the rules should explain (in general terms but again with meaningful specificity) how the technology will be used; the rules should not unduly constrict the discretion necessary for law enforcement to effectively carry out the difficult job entrusted to it. Fourth, the rules

Similarly, Professor Amar has suggested that a meaningful Fourth Amendment should be prospectively rather than retroactively regulatory. See Amar, supra note 142, at 815 (“Early prevention is often better than after-the-fact remedy.”). Further, he has suggested greater input by citizenry, such as through citizen review panels and “public promulgation of agency guidelines [that] will enable the citizenry to better assess the things done in their name.” See id. at 817. Richard Morgan, seeking a middle ground, has stated: “What is needed is a flexible combination of statutory and administrative rules with oversight mechanisms adjusted so that compliance is strongly encouraged, but without paralyzing law enforcement agencies when crime is suspected in political contexts.” See Morgan supra note 135, at 13. Professor Gerard Bradley also criticizes the present “judicialized” regime of search and seizure and argues that “the reasonableness clause, properly understood… exists to affirm legislative supremacy over the law of search and seizure.” See Gerard V. Bradley, The Constitutional Theory of the Fourth Amendment, 38 DePaul L. Rev. 817, 817 (1989). He therefore advocates placing (or rather replacing) the power to “shape our ‘living’ law of search and seizure” into the hands of legislators rather than judges, see id. at 856-57, and suggests Title III as paradigmatic: “Having decided that society deems electronic surveillance to be fourth amendment activity, the Court in effect said to Congress: put together a regulatory scheme along the lines which we have sketched here.” Id. at 869 (footnote omitted).

447. One of the reasons the American Bar Association promulgated standards related to electronic surveillance was to “encourage the development—both by legislatures and administrative bodies—of even more specific written rules governing technologically-assisted physical surveillance.” ABA Standards for Electronic Surveillance, supra note 67, at 7.

448. See supra notes 305-08 and accompanying text.

449. See id.
should explain how the technology's use will meet the stated goals. Finally, the rules should detail how the individual governmental agents will be accountable to the governmental agency and the governmental agency to the public in the use of their discretion; the rules should contain reasonable and realistic mechanisms to ensure that the governmental agents and agencies conform with parameters and procedures that are established.

This burden must also be meaningful. The case of Carnivore can be used to illustrate how such a rule would operate: In the legislation or administrative rulemaking, the FBI would describe what Carnivore is (a suite of software which, when attached to the computers of an Internet service-provider, would permit the FBI to intercept electronic communications) and what purpose it serves. The purpose served seems self-apparent—given the quickly growing use of this medium for general communication, law enforcement needs the power to intercept electronic communications in the proper circumstances, lest the Internet foster rampant criminal activity. Nevertheless, the description of the purposes should be thorough and specific.

In addition, the FBI would be obliged to show how Carnivore would work and to clearly demonstrate that there are effective mechanisms to ensure compliance with proposed norms. If the FBI sought to stretch Title III to cover the use of Carnivore, the FBI would have to prove that the interception of electronic communication is in nature and practice sufficiently identical to interception of telephonic or wire communication to allow identical treatment under the law. As discussed above, Carnivore differs substantially in key ways from traditional telephonic wiretapping—particularly the ease with which it can be configured to comb very broadly the traffic search traversing an Internet service-provider's network. More fateful still, Carnivore as configured in late 2000 consisted of technical features that too-easily thwarted oversight; agents could use it totally unaccountably. As long as Carnivore's configuration lacks reliable and realistic mechanisms for oversight, it would fail to meet the standards proposed here.

Giving the executive-branch law-enforcement agencies such a prominent role in promulgating these rules itself creates the potential for abuse, if the rulemaking is not diligent and if mere lip-service is

450. See supra notes 44-46, 316-23 and accompanying text for a description and discussion of Carnivore.
451. See supra note 274 for a discussion of recent legislation whose measures were out of proportion, if not entirely unrelated, to the problem purportedly addressed.
452. See Independent Review of Carnivore, supra note 43, at 3-4 to 3-5.
453. See supra notes 317-23 and accompanying text.
454. See supra note 135 and accompanying text for discussion of abuses by law enforcement, and supra notes 345-48 and accompanying text for discussion of how officials in intelligence agencies bristle under the current rules.
paid to the tall burdens imposed on the government. One important means of ensuring a level of diligence is the public exposure of these technologies and their governing rules to public discourse and scrutiny. This public airing of the proposal would permit lawmakers and public advocacy groups to test the legitimacy of the proposal and its underlying elements. The other important lever for ensuring diligence is the oversight of the judiciary.

2. Judicial Role

In effect, the courts would be a primary bulwark against the foxes taking over the henhouse. Thus, the role of the courts in this proposed regime would be critical.\textsuperscript{455} The judiciary's primary role would be to require that executive-branch law-enforcement agencies fully disclose and be accountable for their use of these technologies. Courts would oversee the development of proper rules and regulations, viable and effective measures to prevent misuse, and compliance with these rules and regulations. For example, the courts could prevent Congress from enacting with little public discourse laws that made subtle but significant changes in the government's powers of surveillance, as it has done on several occasions in amending Title III.\textsuperscript{456} and as occurred with legislation hastily enacted after the events of September 11, 2001.\textsuperscript{457}

The courts' role would entail oversight of both the procedure and substance of the rulemaking. Procedurally, courts would make sure that the legislature or the executive-branch agency crafting administrative rulemaking describe the technology, its use, and its purpose with sufficient clarity and specificity. The courts must ensure that penalties effectively deter governmental agents or agencies from circumventing the rulemaking or legislative sanction recommended

\textsuperscript{455} See Amsterdam, supra note 290, at 429 ("Judicial review both of the substance of the rules and of police compliance with them in particular cases remains essential.").

\textsuperscript{456} See Barr, supra note 109, at 75 (discussing the surreptitious enactment of a provision broadening the use of "roving wiretaps"). If, as seems likely, neither the courts nor the populace would permit Congress to quietly and surreptitiously pass a law affecting a First Amendment right, it seems worth asking why the courts would treat a law affecting Fourth Amendment rights any differently.

\textsuperscript{457} See supra note 272 and accompanying text for discussion of pressure exerted by the Bush administration on Congress to quickly enact wide-reaching legislation. Although legislation strengthening the government's surveillance powers passed by overwhelming majorities in the House (337-79) and Senate (96-1), it was enacted with little debate in the House and Senate. See Toner & Lewis, House Passes Terrorism Bill, supra note 273; Robin Toner & Neil A. Lewis, Bill Greatly Expanding Surveillance Power in Terrorism Fight Clears the Senate, N.Y. Times, Oct 12, at B11. However, the version of the bill passed by the House was different from the version negotiated and unanimously adopted by the House Judiciary Committee; the version passed was one agreed on by "top House Republicans and the Bush administration" and inserted at the last minute, so that there was little opportunity to read and debate the bill. See Toner & Lewis, House Passes Terrorism Bill, supra note 273.
ELECTRONIC SURVEILLANCE

here—creating strong rules on the surface but then permitting governmental agents or agencies to easily hide dubious practices is no solution. Further, the courts should ensure that the mechanism touches the many facets of governmental surveillance, especially those activities that yield information that will not be exposed in court (where defendants are motivated to expose and challenge the legality of the search), such as the creation of powerful but largely invisible databases. In this sense, the judiciary's role in the regime proposed here closely resembles the “participation-oriented, representation-reinforcing approach to judicial review” advocated by Professor Ely.\(^4\)\(^5\) As Professor Ely explained:

\[
\text{[U]nlike an approach geared to the judicial imposition of }
\text{“fundamental values,” the representation-reinforcing orientation . . .}
\text{is entirely supportive of] the American system of representative democracy. It recognizes the unacceptability of the claim that appointed and life-tenured judges are better reflectors of conventional values than elected representatives, devoting itself instead to policing the mechanisms by which the system seeks to ensure that our elected representatives actually represent.}\(^6\)
\]

Substantively, the courts’ first responsibility would be to scrutinize the agency’s articulated purpose and the extent to which the government’s stated purposes dovetail with the stated capabilities of the technology. In the context of administrative rulemaking, the ordinarily high level of deference that courts afford executive-branch agencies would have to be lowered,\(^7\) since the issues involved here are potentially, if not actually, of a constitutional dimension.\(^8\) Indeed, the standard of judicial review for both legislative and administrative rulemaking should be consistent with the standard of review for other constitutional rights; the Supreme Court’s jurisprudence of the Equal Protection Clause and the First Amendment, for example, requires the government (usually Congress) to articulate either an important or compelling governmental interest and to demonstrate that the measure is either substantially related or narrowly tailored to meet that interest.\(^9\)

\(^4\) Ely, supra note 13, at 87.
\(^5\) See id. at 73-104.
\(^6\) Id. at 101-02.
\(^7\) See Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 842-44 (1984) (establishing rule that courts should defer to an agency if the agency’s interpretation of a statute is reasonable); SEC v. Chenery Corp. (Chenery II), 332 U.S. 194, 202-03 (1947) (holding that administrative agencies may flesh out vague and ambiguous statutes through retroactive adjudication); see e.g., U.S. Telecom Ass’n v. FCC, 227 F.3d 450, 457-58 (D.C. Cir. 2000) (stating the Chevron doctrine).
\(^8\) Cf. INS v. Cardoza-Fonseca, 480 U.S. 421, 446 (1986) (stating as a reason for not deferring to an administrative agency’s construction of a statute that “a pure question of statutory construction [is] for the courts to decide”).
\(^9\) See, e.g., United States v. Virginia, 518 U.S. 515, 524 (1996) (holding that Virginia failed to show “an exceedingly persuasive justification” for its all-male state-
A second important substantive oversight responsibility of the courts would be to scrutinize the mechanisms proposed by the agency to ensure compliance with the stated standards. Courts would be tasked with evaluating whether there was adequate accountability of the agents and the agencies to ensure that the discretion remains properly moderated. In addition, courts would scrutinize whether the enforcement mechanisms proposed by the agency or legislature would sufficiently guard against wayward conduct. However, since the jurisdiction of federal courts requires that there be a case or controversy, one important open question would be how to ensure that a legislative or administrative law could be reviewed by the courts— in other words, how to ensure that citizens or groups have standing to challenge a surveillance-sanctioning law or the executive-branch agency’s adherence to such a law even when the citizen or group is not directly effected.

3. Limiting Governmental Immunity

The present system of law enforcement affords agents with broad immunity. In large part, this is a function of the heavy reliance on warrants, which serve to immunize governmental agents. This immunity greatly erodes the accountability of governmental agents. Following a proposal by Professor Amar, the regime advocated here would seek to increase the accountability of governmental agents and agencies’ use of covert surveillance technologies by limiting this immunity and permitting juries to decide whether conduct is supported military academy); Adarand Constructors, Inc. v. Pena, 515 U.S. 200, 227 (1995) ("[W]e hold today that all racial classifications, imposed by whatever federal, state, or local governmental actor, must be analyzed by a reviewing court under strict scrutiny. In other words, such classifications are constitutional only if they are narrowly tailored measures that further compelling governmental interests."); Craig v. Boren, 429 U.S. 190, 204 (1976) (holding that Oklahoma in enacting a statute that treated men and women differently failed to show that the gender-based distinction served an important governmental interest and was substantially related to its objective); see also supra note 437 and accompanying text.


No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.


466. See Amar, supra note 142, passim.
reasonable, and, if not, the appropriate measure of punishment. Professor Amar has recommended strict governmental liability for unreasonable searches and seizures:

In our century, however, judges for the first time have created wide zones of individual officer immunity for constitutional torts. Within these zones, the innocent citizen victim is in effect “held liable” and left to pay for the government’s constitutional wrong. The best way to close this shocking remedial gap today would be to recognize direct liability of the government entity. If the search or seizure is ultimately deemed unreasonable, the government entity should pay. And the damages assessed will be a visible sign to legislators and the general public of the true costs of unreasonable government conduct.467

Thus, under Professor Amar’s rubric, not only should this compel proper exercise of discretion, but the costs of unreasonable searches or seizures are borne by the tortfeasor—the government.

4. Citizen Involvement

These normative decisions about reasonableness of searches and seizures and about the government’s power versus citizens’ rights would be returned to the citizens. Rather than having law-enforcement officers and agencies unilaterally deciding and judges periodically decreeing what intrusions are reasonable and what privacy is appropriate, citizens should have meaningful input on these important normative decisions. Citizens should be far more involved than they presently are in making normative decisions about the relevance and substance of their own privacy interest and their own tolerance for governmental intrusions in the name of maintaining public order.

Ensuring or increasing citizens’ involvement can take several forms. First, this proposed regime envisions greater use of the various political measures available, especially through legislative or administrative deliberation, discourse, and debate.468 In addition, increased citizen involvement can take the form of public hearings or citizens’ advisory committees, where law enforcement would present a technology and its intended use to the public. Citizens would provide feedback and guidance about how they value their liberties vis-à-vis security and what they deem unreasonable;469 to be meaningful, the government’s disclosures about the technology and the intended uses should be thorough and comprehensive, and citizens’ input should be able to influence outcomes.

467. Id. at 812-13.
468. See supra notes 446-54 and accompanying text.
469. See Amar, supra note 142, at 816-17 (discussing the benefits of citizen review or advisory panels).
The second mechanism for increasing citizens’ involvement in defining Fourth Amendment reasonableness is through the jury system. Following a proposal by Professor Amar, this regime would seek to reintroduce civil and criminal penalties against governmental agents conducting unreasonable searches and seizures as a key means for policing the police’s conduct. As Professor Amar noted, such a system, which comports with the practice in the late eighteenth century, would be a very effective method for preserving the meaning of the Fourth Amendment. However, this development would require a fundamental rethinking of warrants, which are currently the centerpiece of Fourth Amendment jurisprudence.

B. Advantages

As mentioned above, the regime proposed here is principally concerned with redressing several problematic characteristics of modern surveillance technologies. The first section of Part III has sketched the operation of this proposed regime and has attempted to show how the proposal accomplishes its intended goals. This section suggests several additional operational and doctrinal advantages that are gained by making legislative or administrative pre-clearance bear the brunt of the regulation of surveillance technologies.

First, although courts possess considerable institutional competencies and resources, the executive-branch law-enforcement agencies that seek to deploy the technology will know more about the technology and the purposes for which it is being developed. In addition, since courts decide specific cases and controversies, they may not be presented the full scope of a technology when deciding its constitutionality, as *Kyllo* illustrates. Thus, by placing this onus of declaring an intended use and proposing the parameters for such use, this regime has the advantage of drawing on the expertise of those who will actually use the technologies.

Second, given their greater technological expertise, these agencies, can, with appropriate oversight, develop parameters and rules that are customized to the technology. As the ABA has suggested, what is reasonable will vary depending on the particular technology and the particular usage. Further, a single technology may have multiple applications, with each application creating different benefits and posing different risks and thus requiring different constraints and protections. However, the Supreme Court’s conjunctive reading of

470. See Amar, supra note 142, passim.
471. See supra notes 407-11 and accompanying text.
472. See supra notes 142-56 and accompanying text.
473. See supra Part II and text accompanying notes 442-45.
474. See supra notes 77-83 and accompanying text.
475. See supra notes 128-29 and accompanying text.
476. For example, rudimentary thermal imagers can be used to monitor unusual
the Fourth Amendment has yielded a simple binary jurisprudence—
conduct that is a search or seizure requires a warrant, which serves to
assure reasonableness, while conduct that is not requires nothing—
which fails to adequately address the many possible gradations of the
invasiveness of a particular technology or application and the
importance and value of the information gleaned. Further, since
warrants require a showing of probable cause and particularity of
description, the Court currently seems disinclined to find that
technologies which intrude relatively minimally on each person’s
privacy but which improve safety and security are searches or
seizures. And just as there are technological applications where a
warrant is overly burdensome, there may also be technologies and
applications where a warrant is not sufficiently rigorous and more
precautions are required. In short, the present regime lacks the
suppleness necessary to properly regulate the many surveillance
technologies in use and in development.

A third operational advantage is that this regime would eliminate
the interval during which a highly intrusive technology is being used
without public or judicial scrutiny. For example, the FBI first
implemented its Carnivore system secretly; though the FBI apparently
hews closely to Title III for the use of Carnivore, there may yet be
different or additional risks posed by this new technology that require
different treatment. Under the current regime, the constitutionality of
a particular technology’s usage percolates slowly to the Supreme
Court, during which time there may be no constraints on its usage and
thus no ability to attempt to ensure its use is reasonable. Some
technologies, such as large-scale federal databases, are never judicially
scrutinized at all. The regime proposed here would attempt to close
this gap by placing the evaluation of the technology upfront.

Fourth, Professor Amsterdam delineated several ways that his
regime would improve the performance of the police in upholding the
Fourth Amendment. First, requiring the police to make prior rules

heat patterns emanating from houses, while more sophisticated versions can detect
weapons, drugs, and other contraband on people. See supra notes 77-83 and
accompanying text.

477. See supra note 413 and accompanying text.

478. Since it would be impractical to require law enforcement to secure warrants
for broad but minimally invasive surveillance such as face-recognition cameras or
airport metal detectors, the Court has crafted an administrative or special-needs
exception to the warrant requirement. See Buffaloe, supra note 142, at 533-42.
However, once a technology has been deemed not to implicate the Fourth
Amendment, there are effectively no other controls over its use.

479. The prime example of this is surveillance orders for wiretaps. See Taylor,
supra note 139, at 79-85 (discussing differences between search warrants and
surveillance orders). Though often treated as synonymous with regular search
warrants, surveillance orders were designed initially to be more cumbersome. See
supra note 237-42 and accompanying text.

480. See supra Part II.A.1.
about certain practices would improve "the quality of police decisions" by 1) making police aware that there are policies to be made—rather than making decisions haphazardly, 2) by forcing "someone with responsibility and proven judgment" to make these decisions, and 3) by increasing the awareness of the seriousness of their practices. Second, such rulemaking would ensure fairness and consistency in the treatment of citizens. Third, in contrast to the current practice which "remains necessarily unresponsive and irresponsible," his proposal would "increase[] the visibility of police policy decisions." Such a system would force the police to confront its own practices and to make them known to other government agencies and to the general public. In Professor Amsterdam's view, "[r]ulemaking offers the best hope we have for getting policemen consistently to obey and enforce constitutional norms that guarantee the liberty of the citizen."

The increasing reliance by the police and federal law enforcement on surveillance also represents a decision on how to allocate financial and personnel resources. Although there was a rush to change wiretap laws after September 11, there was also considerable evidence that the failure was not due to lack of technology or to

481. Amsterdam, supra note 290, at 423-24; supra Part II.A.1.
482. Amsterdam, supra note 290, at 425.
483. Id. at 426.
484. Id. at 426-27.
485. Id. at 428 (emphasis in original omitted).
486. The financial costs of surveillance are substantial. In 1999, courts authorized federal and state law-enforcement to conduct 1350 wiretaps. See Wiretap Report 1999, supra note 26, at 7. The total cost of these wiretaps was in excess of $70 million, and the average wiretap cost $57,511, of which the cost in manpower constitutes the vast majority of this expense. See Wiretap Report 1999, supra note 26, at 10. Dwarfting this sum, however, is the $500 million that taxpayers will pay to retrofit existing telecommunications facilities so that law enforcement has a guaranteed right of access to any and all electronic communications, pursuant to CALEA. See OTA, Surveillance in a Digital Age, supra note 21, at 6. One recent estimate placed the cost of electronic surveillance and spy satellites at $10 billion a year. See Tim Weiner, To Fight in the Shadows, Get Better Eyes, N.Y. Times, Oct. 7, 2001, § 4 (Week in Review), at 1.

There is also reason to question the value of these large investments. Recently, the government disclosed that a U.S. federal agent spying for the Soviet and Russian governments compromised a surveillance operation under the Russian Embassy in Washington, D.C. costing "several hundred million dollars." James Risen & Lowell Bergman, U.S. Thinks Agent Revealed Tunnel at Soviet Embassy: Costly Effort to Spy in Washington Was Ruined, Officials Say, N.Y. Times, Mar. 4, 2001, at 1. The journalists also note that this was not atypical. Id. ("The tunnel operation against the Soviet complex... is just one of many similar clandestine technical operations run by the United States intelligence community.... And, like the embassy operation, many of those other operations were eventually compromised by spies.").

Critics also question whether the track record of databases are any better. For example, in his evaluation of the Treasury Department's FinCEN, Steven Bercu asserts that the benefits of FinCEN have never been adequately shown. See Bercu, supra note 96, at 447-48.
487. See supra notes 271-76 and accompanying text.
overly restrictive laws. Instead, there were other indications that the "failure" to prevent the attack on the Pentagon and the World Trade Center—to the extent that the attacks actually could have been interdicted—was a failure in other aspects of the United States' law enforcement and intelligence. Indeed, it may be the case that our security lies in devoting fewer resources to high-technology clandestine surveillance and more resources on time-tested

488. See infra note 489.
489. The hijackings exposed how the security measures in place at American airports are poorly enforced. See Kate Zernike, Change Ahead for Troubled Boston Airport Agency, N.Y. Times, Sept. 21, 2001, at A14 (describing Logan Airport's history of security lapses and how insecure is rife at the authority that runs the airport); see also Carey Goldberg, Boston's Airport Security Is Described as Standard, N.Y. Times, Sept. 12, 2001, at A16 (stating that the type and frequency of security lapses at Logan was comparable to other U.S. airports). A second frequently-cited reason for the "failure" was problems within and among the law-enforcement and intelligence communities, such as internecine battles within the agencies and turf wars without, incompetence, and lack of agents able to translate intercepts of Arabic and Farsi communications. See Seymour M. Hersh, What Went Wrong: The C.I.A. and the Failure of American Intelligence, The New Yorker, Oct. 8, 2001, at 34 (describing problems within the C.I.A., particularly the small and decreasing number of intelligence operatives in the field, that prevented it from detecting and preventing the attacks of September 11); Walter Pincus, Committee: Terrorism Threat Is Long-Term; Agencies Advised To Collaborate More, Wash. Post, Sept. 20, 2001, at A33 (noting the "concern" in Washington, D.C., that "neither the FBI nor CIA has enough Arabic and Farsi translators for the enormous amounts of intelligence intercepts occurring around the world"); Peter Slevin, FBI Courts Arab, Muslim Communities: Agency Seeks Information, Easing of Old Tensions, Wash. Post, Sept. 19, 2001, at A14 (discussing the FBI's difficulty in gaining contacts within the Muslim and Arab-American communities and stating that "the infiltration of terror networks has proven far more difficult than even the puncturing of Soviet intelligence or Mafia families, particularly given a shortage of Arab American agents"); Tim Weiner & David Cay Johnston, Roadblocks Cited in Efforts to Trace Bin Laden's Money, N.Y. Times, Sept. 20, 2001, at A1 (citing as one reason the U.S. government failed to track and stop the flow of money between the terrorists was that the people within the U.S. intelligence agencies assigned the task were "generally incompetent" to handle it).

In addition, there are commentators who credit the perpetrators as much as criticize U.S. intelligence and law enforcement. See Hersh, supra; see also Stephen J. Hedges et al., FBI Probes 5th Flight for Hijackers: Plane Grounded on Day of Attack, Chi. Trib., Sept. 18, 2001, at 1 (describing evidence that the hijackers used computers at public libraries to avoid detection while communicating); Weiner, supra note 486 ("[American surveillance's] targets are hard men hiding in shadows and speaking in codes, against whom spy satellites, surveillance systems and smart bombs count for little.").

Amid the news about the government's attempt to expand its wiretapping capabilities was the not-very-prominent disclosure of a highly classified internal investigation into alleged improprieties by the FBI in the investigations of the bombings of two United States' embassies in Tanzania and Saudi Arabia in 1998. See David Johnston & James Risen, Officials Say 2 More Jets May Have Been in the Plot, N.Y. Times, Sept. 19, 2001, at B1. According to a report appearing in the New York Times, the investigation was instigated by the chief judge of the Foreign Intelligence Surveillance Court (the court that administers warrants for surveillance orders under FISA), "apparently related to whether the [FBI] was seeking wiretaps under the [Foreign Intelligence Surveillance Act] on individuals without informing the court of a subject's status pending criminal investigations." Id.
intelligence-gathering and crime-fighting methods—\textsuperscript{490} for example, by deploying more officers on the street and focusing on improving the techniques and technologies currently in place.

Finally, Professor Amsterdam identified four doctrinal advantages of shifting a substantial part of the responsibility for making Fourth Amendment law from the judiciary to administrative bodies or to the legislature.\textsuperscript{491} First, "it provides a pervasive safeguard against arbitrary searches and seizures that runs the length and breadth of the amendment and does not require the creation of any new categories . . . ."\textsuperscript{492} Second, the rules would be clear, flexible, and intelligible (without being "amorphous") to law-enforcement agents, since law-enforcement agents who are presumptively more knowledgeable than the courts about the technologies and the purposes (legitimate and otherwise) for deploying the technologies, would have created the rules.\textsuperscript{493} Third, forcing the police to secure authorization for certain practices through administrative rulemaking "would operate to tame the wild proliferation of police practices that has presented one of the Supreme Court's greatest problems in developing a coherent body of fourth amendment law."\textsuperscript{494} Finally, rulemaking "would permit the Court to extend the coverage of the fourth amendment over police activities that demand some control against abuse but do not appear to lend themselves to regulation by warrants or the probable cause standard of justification."\textsuperscript{495}

\textsuperscript{490} See Weiner, supra note 486 (citing an intelligence expert as recently saying that "American intelligence was in disarray, drowning under a tidal wave of technology, harried by short-term military tasks, [and] short on brain power").

\textsuperscript{491} Professor Amsterdam placed greater faith in administrative rulemaking to correct the ills of the Fourth Amendment practice than in legislation by the Congress. See Amsterdam, supra note 290, at 378-79. As Professor Amsterdam stated, Nor do I ignore the possibility of controlling that ["enormous range of police"] power [that "stands unrestrained"] and restraining its abuses by subconstitutional law. I only wish that the possibility might become a reality. But our fondest hopes must be tempered by a little common sense. The long-time, wholesale "legislative default" in regulating police practices is no accident. Legislatures have not been, are not now, and are not likely to become sensitive to the concern of protecting persons under investigation by the police.

\textsuperscript{492} Id. at 418.

\textsuperscript{493} Id. at 418-19.

\textsuperscript{494} Id. at 419. See supra notes 481-85 and accompanying text for discussion of how rulemaking would improve police practices.

\textsuperscript{495} Amsterdam, supra note 290, at 422. As discussed above, the Supreme Court's reliance on the warrant's probable-cause requirement to ensure the reasonableness of a search or seizure has led the Court to contort its Fourth Amendment jurisprudence and allow practices which are clearly searches or seizures, but which would never meet the probable-cause standard. See supra notes 477-78 and accompanying text.
CONCLUSION

There are numerous examples of misuse of surveillance technologies, confirming the Founders' suspicions about the often irresistible allure of power. Justice Scalia recently observed that "[o]nly someone who has worked in the field of law enforcement can fully appreciate the vast power and the immense discretion that are placed in the hands of a prosecutor with respect to the objects of his investigation." Americans take great pride and comfort in the belief that our democratic institutions largely serve to prevent abuses of

496. See supra notes 135, 341-44 and accompanying text.
497. As Senator Sam Ervin, chair of the Senate Subcommittee on Constitutional Rights, stated in 1974:
   The Founding Fathers knew well that with power comes the ability to do harm. The fundamentals of our constitutional system require us always to ensure that governmental power is sufficiently constrained by law so that as much as is humanly possible the power of government is used for good alone, and that our nation continues to have a government subject to the people, and not the reverse. We have slowly come to the realization that this is true no less for information practices as it is for other of Government's activities.
Sam J. Ervin, Jr., Preface to 1 Federal Data Banks and Constitutional Rights, supra note 23, at III.
499. The robust existence of the "administrative state," in which difficult or complex issues are delegated to expert and insulated agencies, raises concerns about the efficacy of political practice as an adequate assurance that law enforcement conduct clandestine surveillance within the confines of constitutional strictures. See Motor Vehicles Mfrs. Ass'n v. State Farm Mut. Auto Ins., 463 U.S. 29, 48 (1983) ("Expert discretion is the lifeblood of the administrative process, but unless we make the requirements for administrative action strict and demanding, expertise, the strength of modern government, can become a monster which rules with no practical limits on its discretion." (internal quotations omitted) (quoting Burlington Truck Lines, Inc., v. United States, 371 U.S. 156, 167 (1962))); E. Donald Elliot, INS v. Chadha: The Administrative Constitution, the Constitution, and the Legislative Veto, 1983 Sup. Ct. Rev. 125, 169-75 (describing how the rise of the administrative state has transformed the three-branch constitutional system originally established). As Professor Elliot states:
   The United States has at least one other "constitution (with a lower-case 'c')," which we might call the "constitution of the administrative state." Its functions are to provide structure and control over the enormous array of federal departments, independent commissions, agencies, government corporations, banks, boards, committees, and quasi-official agencies and authorities that now exercise power to make law in various forms....
   Together the constitution of the administrative state creates a system of law by which government instrumentalities are supposedly controlled and managed.
   Id. at 169-70.

Another commentator, discussing the Financial Crimes Enforcement Network ("FinCEN"), observed: "What dangers arise when an entrenched bureaucratic agency controls powerful, largely invisible technologies? The chief concern, perhaps, is that bureaucracies have little incentive to regulate themselves.... FinCEN is largely cabined off from the political process." See Bercu, supra note 96, at 403.
power. However, even Louis Freeh, the former Director of the FBI, acknowledges the very fine line between protection and repression:

Compliance with the highest ethical standards is essential for all law enforcement officers because one of history’s darkest lessons teaches us what happens when the law is subject to the most horrifying misuse by police. The place was Nazi Germany and the time was the 1930s. . . . Hitler persuaded the German president to invoke a section of the German constitution that in effect suspended all civil liberties, thus permitting warrantless searches and seizure of property without due process.

Thus, the need for some form of careful and thorough oversight and accountability is especially heightened in the area of clandestine surveillance because the political controls that may be useful in other areas are much less availing.

This Note argues that the powers of law enforcement—both legally and technologically—are already extremely broad. In essence, the modern Fourth Amendment permits governmental officials extremely broad discretion to peer into the lives of U.S. citizens—partly because the Court has ruled that several of these technologies are outside the Fourth Amendment and partly because the measures that have been established to ensure that the meaning of it is honored are notably unavailing in the context of modern surveillance. Further, the current regime for modern surveillance technologies contains several serious flaws and these flaws will only worsen as technologies continue to advance. Given the prospect of a protracted battle against terrorism following the calamitous hijackings and attacks of September 11, 2001, new law-enforcement techniques may be appropriate.

However, since the liberties that are central to American ideals are at issue, there needs to be extremely close analysis of the question whether the events of September 11 resulted from failures of

---

500. Cf. Talmadge, supra note 430. Judge Talmadge notes that “[t]he self-corrective feature of democratic government is a significant check on governmental abuse, and is often overlooked by advocates of greater constitutional limits on the police power.” Id. at 907. While Judge Talmadge’s notion has appeal in the context of the infringement of property rights by abuses of police powers, it is less clear that reliance on this “self-corrective feature of democratic government” is a sufficient safeguard against sophisticated modern electronic surveillance techniques and technologies, which by their very essence are hidden from view and therefore beyond the range of the public and therefore democratic self-correction. See supra note 499.

501. See Freeh, supra note 425, at 14; see also 1 Fishman & McKenna, supra note 24, § 1:1, at 1-3 (referencing Nazi Germany and the Soviet Union and noting that “[t]he Watergate scandal . . . should suffice to destroy any illusions that the United States is somehow inherently immune from the misuse of these techniques”); Diffie & Landau, supra note 20, at 4 (“Totalitarian regimes have given us abundant evidence that the use of wiretaps and even the fear of their use can stifle free speech. Nor is the political use of electronic surveillance a particularly remote problem—the Watergate scandal is only the most recent example in contemporary American history for its use by the party in power in its attempts to stay in power.”).
technology or overly restrictive laws. If not—if the failures resulted from institutional problems of the intelligence and law-enforcement agencies—then it seems entirely appropriate to demand that the agencies correct these malfunctions before the rights of citizens are further encroached and the agencies given even more power and discretion.

This Note has attempted to articulate how our fundamental liberty values can be revived and reconciled with equally important government interests to permit these technologies to be properly exploited. It has asserted these technologies be exploited to the extent of the citizenry's appetite for them and to the extent that their use can be duly confined within the bounds of the ideals of our society.