Volume 41
Number 4 *Symposium on Electronic Privacy in the Information Age*
*pp.*1383-1412

Symposium on Electronic Privacy in the Information Age

Post-9/11 Electronic Surveillance Severely Undermining Freedom

Bob Barr

SYMPOSIUM ON ELECTRONIC PRIVACY IN THE INFORMATION AGE

POST–9/11 ELECTRONIC SURVEILLANCE SEVERELY UNDERMINING FREEDOM

Bob Barr*

I. INTRODUCTION

Any article concerning surveillance must begin with these words:

> 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.[1]

Unfortunately those words appear to be in disrepute, their meaning denigrated, their import in disrepair. America, in the twenty-first century, appears to have become afraid of—or disinterested in—the "Grand Experiment in Freedom" begun almost 250 years ago by a group of patriots determined to govern themselves free from the control of an over-weaning and powerful government. Today, virtually the entire range of policy decisions within the purview of our federal government appear to be governed by fear, deception, or mistake—not by the courage exemplified by our forefathers. We went to war in Iraq ostensibly over the fear of "weapons of mass destruction." President

* Bob Barr represented the 7th District of Georgia in the U.S. House of Representatives from 1995 to 2003, serving as a senior member of the Judiciary Committee, Vice-Chairman of the Government Reform Committee, and member of the Committee on Financial Services. Bob is President and CEO of Liberty Strategies, L.L.C., a public policy consulting firm headquartered in Atlanta, Georgia. Bob was appointed by President Reagan to serve as the United States Attorney for the Northern District of Georgia (1986-90), and served as President of Southeastern Legal Foundation (1990-91). He was an official with the CIA (1971-78), and practiced law for many years. He currently serves *Of Counsel* with the Law Offices of Edwin Marger, with a national and international practice in both civil and criminal law.

1 U.S. CONST. amend. IV.

Bush authorized a program of electronic surveillance of Americans because he said it was necessary to "protect ourselves" from acts of terrorism.[2] The National Security Agency ("NSA"), or some other agency, maintains that we can only be "protected" by listening to our conversations without benefit of probable cause to believe that we are actually a threat, nevermind that the program is illegal.[3] Senators such as Senator Specter of Pennsylvania and former Senator DeWine of Ohio proposed to either legitimize that program ex post facto, or extend to the executive ever increasing elasticity in shadowing American citizens.[4]

These are dark clouds obstructing freedom in American life today. Some are covert; some are overt. Without the First Amendment, and a relatively free press, there would have been no discovery of this or other programs that are claimed by our benevolent government to have been devised for our protection. What might we do without this overly protective father figure looking after us? These new powers asserted by the federal government—powers that the president claims are necessary to protect us—were never intended to be part of the fabric of our society. But through an assertive executive branch, a pliant Congress, and a deferential judiciary, they have been sewn and stitched progressively into our lives, just as surely as Betsy Ross stitched our first flag.

II. THE FOURTH AMENDMENT TODAY

The Republic's founders intended flexibility and the concomitant ability of the people and their government to be able to respond in a fluid manner given the changing of the times. The Fourth Amendment was meant to meet the needs of all Americans, and designated power to their appointed temporary governing bodies only on those occasions when it became necessary to intrude into the lives of its citizens and violate their privacy in order to serve the greater good.

What lawyers in the Administration of George W. Bush apparently fail to grasp in the government's zeal to intrude into the private lives of Americans by, among other things, the NSA electronic spying program in the "War on Terror," is that the law, and its attendant lawful behavior, provide all the weapons needed to fight terrorism; no "sacrifices" are necessary. No one disputes that there is a need to battle acts of

---

2 *See* Bruce Fein, *Trusting the White House*, WASH. TIMES, Jan. 9, 2007, at A13.

3 *See id.*

4 Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, S. 3001, 109th Cong. (2006); Terrorist Surveillance Act of 2006, S. 2455, 109th Cong. (2006).

terrorism, but the methods that the Bush Administration has chosen are misdirected.

Of course, this process of government over-reaching did not start the day after 9-11. In fact, since at least the 1960s, the Fourth Amendment has been systematically whittled in favor of the government in a variety of ways.[5] In 1967, for example, in *Katz v. United States*,[6] the Supreme Court definitively defined, for the first time, the formula for a tightening of access to the Fourth Amendment power of evidence-suppression. In that landmark beginning, the Court intoned both a subjective and objective "reasonable expectation of privacy" and, in doing so, mandated that the privacy "expectation be one that society is prepared to recognize as 'reasonable.'"[7]

Less than a generation later, in a trilogy of cases—*Rakas v. Illinois*,[8] *Rawlings v. Kentucky*,[9] and *United States v. Salvucci*[10]—the U.S. Supreme Court set in motion a true loosening of the strictures of the Fourth Amendment with the advent of the focus on "reasonable expectation of privacy," and created a seminal event in the history of the Amendment.[11] What those decisions did, in practical terms, was to limit the "persons and places searched" provision to an ever-shrinking number of people and circumstances. In other words, if I put my drugs (or bomb-making materials) in your briefcase, I could not complain about the search no matter how constitutionally problematic, because I had given up my "expectation of privacy." This analysis based on the judicially-created "expectation of privacy" test for Fourth Amendment protection, however, makes little sense in many situations in which our citizens necessarily find themselves involved in the modern world.

---

5 *See, e.g.*, Rawlings v. Kentucky, 448 U.S. 98 (1980); United States v. Salvucci, 448 U.S. 83 (1980); Rakas v. Illinois, 439 U.S. 128 (1978); Katz v. United States, 389 U.S. 347 (1967).

6 389 U.S. 347.

7 *Id.* at 361 (Harlan, J., concurring).

8 439 U.S. 128 (1978).

9 448 U.S. 98 (1980).

10 448 U.S. 83 (1980).

11 *Rawlings*, 448 U.S. at 104 (holding that considering petitioner's admission at suppression hearing that he did not believe acquaintance's purse would be free from search, there was not sufficient showing that his reasonable expectations of privacy were violated); *Salvucci*, 447 U.S. at 93 (holding that Fourth Amendment rights should be analyzed by asking not merely whether defendant had a possessory interest in the items seized, but whether he had an expectation of privacy in the area searched); *Rakas*, 439 U.S. at 148 (holding that there was no showing that mere passengers in a car had any legitimate expectation of privacy in the glove compartment or area under the seat of the car).

Is one private phone call more worthy of protection than another, simply because of the particular phone we use? Do we have a lesser "expectation of privacy" if we communicate by e-mail as opposed to phone, simply because e-mail transmissions travel through an ISP over which we have no control? Are our private medical records considered by us to be less private simply because they are kept at our doctor's office where they necessarily must stay? Or are our private financial records not considered to be private? Common sense tells us that such situations are quite reasonably considered by Americans to be just as "private" as the letters that were the more common mode of communication in the late eighteenth century when the Fourth Amendment was crafted. Yet, because of the artificial, "expectation of privacy" test, through which the federal government has driven a Mack truck, this common sense violation of privacy, which was the basis for the Amendment, has been rent asunder.

Restrictions on the Fourth Amendment's protections have not ended. The federal courts, in their zeal to find reasons to justify expanded government law enforcement powers, have found ever more imaginative ways to limit personal freedom, especially those freedoms guaranteed by the Fourth Amendment. The "good faith exception" of *United States v. Leon*[12] allowed searches even if the warrant subsequently was shown to be unsupported by probable cause.[13] Garbage is no longer protected.[14]

---

[12] 468 U.S. 897 (1984). In *Leon*, on the basis of information from a confidential informant of unproven reliability, the Burbank, California, police department set up surveillance of a pair of individuals suspected to be involved in the sale of illegal drugs. *Id.* at 901. From their investigation, the officers were led to Alberto Leon, who had been previously arrested for a drug offense and about whom a different tip was received regarding storage of illegal drugs. *Id.* at 901-02. Upon the arrest of two other suspects, the officers retrieved items that they believed were utilized in Leon's drug business. *Id.* Subsequently, a search warrant was issued for Leon's residence where drugs were found. *Id.* at 902. Leon challenged the use of the evidence citing a lack of probable cause for issuance of the warrant, and the government responded with the notion that the "exclusionary rule should not apply where evidence is seized in reasonable, good-faith reliance on a search warrant." *Id.* at 903.

[13] *Id.* at 925.

[14] *See* California v. Greenwood, 486 U.S. 35 (1988). In *Greenwood*, a Laguna Beach, California police officer received information from both federal agents and a neighbor that Greenwood may be involved in drug trafficking. *Id.* at 37. The officer attempted to verify this information by setting up surveillance on Greenwood's home. *Id.* She observed vehicles making short stops late in the evening and followed one of these vehicles to another residence that was also under investigation. *Id.* The officer asked the regular trash collector to pick up and turn over Greenwood's trash bags to her without mixing them with the other collected trash, and when the garbage collector did so, the officer found evidence of narcotics use within the trash. *Id.* at 37-38. The fruits of this search were the basis for a warrant used to search the residence, which unearthed cocaine and hasish. *Id.* Greenwood challenged the searches of his trash, contending, *inter alia*, that it violated his

The mail, though protected generally, is now subject to a number of exceptions;[15] as a result, the protection of the mails is not absolute.[16] Additionally, there is no Fourth Amendment right of privacy in bank records despite the fact that in the modern world it is virtually impossible to conduct necessary affairs in one's own behalf without use of financial institutions, credit cards, doctors' offices, insurance companies, and the myriad of other institutions prevalent in our lives. [17]

Fourth Amendment rights. *Id.* The Supreme Court first explained that the search of the trash "would violate the Fourth Amendment only respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable." *Id.* at 39 (citations omitted). As a result, the Court found that the respondent had sufficiently exposed his trash to the public as to defeat any claim to Fourth Amendment protection. *Id.* at 40. "It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.* (citations omitted). Additionally, the Court noted that the material had been placed at the curb for transference to a third party, here, the trash collector. *Id.* Therefore, "having deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,' respondents could have had no reasonable expectation of privacy in the inculpatory items that they discarded." *Id.* at 40-41 (citations omitted).

15 United States v. Young, 350 F.3d 1302 (11th Cir. 2003). In *Young*, the defendant was convicted of various counts involving deception of IRS agents and making false statements on IRS forms to enable him to purchase gasoline and diesel without paying federal excise taxes. *Id.* at 1303-04. His scheme involved large and frequent cash transactions that were sent to him via Federal Express two to three times per month. *Id.* at 1304. As part of its investigation, an IRS agent requested that Federal Express allow the government to x-ray the packages, without a warrant. *Id.* The packages were found to contain large amounts of currency and based on this finding, four warrants were issued for searches of Young's residence and place of business. *Id.* at 1304-05. The Eleventh Circuit found that Young "certainly had a subjective expectation (or hope) of privacy" but that "[n]o reasonable person would expect to retain his . . . privacy interest in a packaged shipment after signing an airbill containing a explicit, written warning that the carrier is authorized to act in direct contravention to that interest." *Id.* at 1307-08. Similarly, in *United States v. Smith,* after receiving information that Smith was receiving illegal drugs, specifically LSD, in the mail, using a third party to actually receive the material, the postal inspector intercepted a letter that bore another person's name and address, but had Smith's name and address crossed out on the envelope. 39 F.3d 1143, 1144 (11th Cir. 1994). When the other party allowed the inspector and a police officer to open the letter in her presence, they discovered LSD. *Id.* The letter was taped to Smith's door, and the officer obtained a search warrant for the residence. *Id.* At trial, Smith moved to suppress the letter, claiming that the third party had agreed to accept the letter, which allegedly was supposed to contain cash from the sender, but that she had no authority to open the letter. *Id.* The Eleventh Circuit Court of Appeals found the arrangement that Smith had with the third party was insufficient to preserve his legitimate expectation of privacy in the letter as he was neither the sender nor the addressed recipient, even though he had not given permission for the third party to open and examine the contents of the letter. *Id.* at 1145.

16 *Young*, 350 F.3d at 1309; *Smith,* 39 F.3d at 1145; *see also supra* note 15 (discussing Smith and Young).

17 United States v. Miller, 425 U.S. 425 (1976).

The courts have also upheld the substitution of the *Aquilar-Spinelli* standard as it relates to the test of informant reliability.[18] Similarly, in *Illinois v. Gates*, the Supreme Court held that a purely anonymous tip supported to some degree by corroboration (based on surveillance) of some otherwise innocent data, could establish the legality of the search.[19] In *Gates*, the Court concluded that a totality of the circumstances test must be utilized to determine probable cause.[20] Even *stale* information can be updated and/or corroborated to form the basis for probable cause.[21]

Recently, the Court has even found an *anticipatory* search warrant lawful; that is, a search warrant that is granted but then can be simply stuck in a police officer's pocket or file to await a triggering event before it is executed.[22] In fact, even falsely sworn statements in a search

---

[18] Spinelli v. United States, 393 U.S. 410 (1969) (holding that informant's basis of knowledge and facts establishing informant's reliability and credibility should be considered in determining probable cause from this information); Aquilar v. Texas, 378 U.S. 108 (1964) (holding that affidavit for search warrant may be based on hearsay information so long as informant is "credible").

[19] 462 U.S. 213, 238 (1983).

[20] *Id.* The court concluded

> [T]hat it is wiser to abandon the "two-pronged test" established by our decisions in *Aguilar* and *Spinelli*. In its place, we reaffirm the totality-of-the-circumstances analysis that traditionally has informed probable-cause determinations. . . . The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a "substantial basis for . . . [concluding]" that probable cause existed. We are convinced that this flexible, easily applied standard will better achieve the accommodation of public and private interests that the Fourth Amendment requires than does the approach that has developed from *Aguilar* and *Spinelli*.

Id. at 238-39 (citations omitted).

[21] United States v. Magluta, 198 F.3d 1265, 1272 (11th Cir. 1999).

[22] United States v. Grubbs, 126 S. Ct. 1494, 1500 (2006). In *Grubbs*, Mr. Grubbs purchased child pornography from a website that was operated by a postal inspector acting undercover. *Id.* at 1497. The delivery was arranged, and the postal inspector submitted a warrant application to a federal magistrate detailing the operation. *Id.* There was a caveat in the application, stating that

> [e]xecution of this search warrant will not occur unless and until the parcel has been received by a person(s) and has been physically taken into the residence. . . . At that time, and not before, this search warrant will be executed by me and other United States postal inspectors, with

warrant are no longer grounds to discard the warrant.[23] This is true even if the misrepresentations are knowingly made, but given the allowed inclusion of other circumstances, even innocent ones, while discounting the untruths, another justification is found for the search.[24]

> appropriate assistance from other law enforcement officers in accordance with this warrant's command.

Id. (citations omitted). In addition, to this statement, the application relied on two attachments that were not in the body of the warrant request that described both the residence and items sought. *Id.* The warrant was issued as requested and the package delivered two days later. *Id.* at 1497-98. Grubbs' wife signed for the package, took it inside, and moments later, inspectors and officers detained Grubbs as he attempted to leave his home. *Id.* Grubbs was supplied with a copy of the warrant approximately thirty minutes into the search, but the items supplied to Grubbs did not include the affidavit which described the triggering condition of the search warrant. *Id.* Grubbs consented to interrogation, admitted to ordering the tape, was placed under arrest and items seized. *Id.* The Supreme Court upheld the validity of these so-called "anticipatory" search warrants, stating that "they are no different in principle from ordinary warrants." *Id.*

[23] Franks v. Delaware, 438 U.S. 154, 172-73 (1978). In *Franks*, Cynthia Bailey reported to police on March 5, 1976, that she had been sexually assaulted by a man in her home. *Id.* at 156. Bailey provided a description of her assailant, detailing that he wore a white thermal undershirt, black pants with a metallic buckle, a brown leather coat, and a dark knit cap. *Id.* She also described some of his physical characteristics, including age, weight, race, height, build and facial hair. *Id.* By coincidence, that same day, Franks was arrested in connection with a different assault of a fifteen year old identified as "Brenda B." *Id.* While awaiting a bail hearing, Franks made an incriminating statement before being read his *Miranda* rights, expressing confusion over who it was alleged that he assaulted. *Id.* On March 8, the officer who heard the incriminating statement mentioned it to a detective on the Bailey case. *Id.* at 157. Based in part on this information, the detective sought a search warrant, including in his application affidavits from those who worked with Franks that indicated that he often wore the type of clothing that Bailey indicated was worn by her assailant. *Id.* The judge issued the warrant and officers seized items matching the description Bailey provided. *Id.* Franks challenged the admissibility of the evidence, noting that the warrant was not truthful and that those allegedly interviewed by the applying officer were not and that any information they may have given to another officer differed from what was presented in the affidavit. *Id.* The Court ultimately held that to challenge a warrant based on veracity of the affidavit, the challenger must not present a conclusory statement that the warrant was based on untruths, but rather

> [t]here must be allegations of deliberate falsehood or reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant or affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons.

Id. at 171.

[24] *Id.*; *see, e.g.*, United States v. Karo, 468 U.S. 705, 719 (1984) (holding that a search warrant could have been procured without relying on a hidden beeper, but rather via the visual surveillance of the defendant's vehicle and residence); United States v. Levasseur, 816 F.2d 37, 43-44 (2d Cir. 1987) (asserting that thirty paragraphs in the Cross Affidavit supplied sufficient independent information to support a finding of probable cause).

There are numerous other examples of this continuing and profound lessening of prohibition against governmental intrusion. The courts continue, by and large, to be in lockstep with various administrations, including the current one. For example, even as it solidified the "reasonable expectation of privacy" standard, the Supreme Court held that the use of a pen register does not constitute a search under the Fourth Amendment.[25] And recently, courts have gone further when addressing computer privacy issues. In *United States v. Steiger*, the Eleventh Circuit held that a "Trojan Horse" virus that enables a hacker to discover and download files from another person's computer is not unlawful because interception is defined as containing a requirement that the electronic communication be obtained contemporaneously with its transmission.[26] Thus, a government hacker can lawfully search all of the files in existence on any citizen's computer and seize the same files on the sole basis that the files were electronically created at a time prior to the search and seizure.

All of these examples, which are not exhaustive, are weapons that are being utilized by the government, not only as part of its "War on Terror," but in other types of criminal investigations as well.

III. TECHNOLOGY DOES NOT SUPPLANT FREEDOM

A new era of science and technology envelopes us; technology has opened new vistas to snoop beyond any extent envisioned by those founding geniuses, Thomas Jefferson, Benjamin Franklin, and James Madison, among others.

To be sure, we as a nation have been attacked; we are at peril from a new kind of enemy—a shadowy, will o' the wisp enemy is at our shores. We should not shrink from this exacting truth. But, were not the threats to our shores, our very existence, in 1776 and in the first few decades thereafter, also serious? Were they any less dangerous to the infant

---

[25] Smith v. Maryland, 442 U.S. 735, 746-47 (1979). "Pen register" is defined as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." *Id.* at 736 n.1. The Court held that the pen register did not constitute a search for Fourth Amendment purposes because a person does not have a legitimate expectation of privacy in the numbers she may dial on a telephone. *Id.* at 742. Additionally, the Court noted that pen registers have no ability to record the contents of the communications, and that "all telephone users realize that they must 'convey' phone numbers to the telephone company. . . [and] moreover, that the phone company has facilities for making permanent records of the numbers they dial." *Id.*

[26] 318 F.3d 1039, 1050 (11th Cir. 2003).

nation than the threats facing us today? The fledgling country was at risk at every turn, but in the exercise of the kind of vision and courage that has been our trademark throughout our history, our Founding Fathers did not flinch from their belief in a freedom such as the world had never seen, and has yet to be duplicated. They fashioned a fair, but strict, set of prohibitions that focused its force on the power of the government to intrude upon the rights and privacy of its citizens. Are we in greater danger now than then? I think not. Our neophyte nation possessed but a ragtag collection of volunteers to defend our shores, and little military equipment. Now, two and a quarter centuries later, we have a standing army, navy, and air force that certainly is the most powerful by far of any in the world today. Are we at risk? Certainly, but do we demolish the tenets of the very fiber of the being of our nation to meet those challenges? Or do we remain true to what we have always been? Technology, especially electronic technology, tempts the dilettante, is like the biblical serpent to the slothful, and invites abuse.

That threat cannot be allowed to change or diminish the underpinnings of the way of life we espouse. We cannot abandon our beliefs.

A. Lawful Interdiction Methods Exist

News Flash—The Fourth Amendment works! So does the Foreign Intelligence Surveillance Act ("FISA"),[27] and the special court created by FISA, the Foreign Intelligence Surveillance Court ("FISC"). There is no necessity whatsoever, under the guise of "protecting" us from acts of terrorism, to create new vehicles of legally or illegally-sanctioned intrusion into the lives of Americans. Nor is it wise to legalize an illegal program—the NSA spying program; to do so would be constitutionally devastating. The interrelationship of the tri-partite form of government would actually work if the legislative and judicial branches would simply stop rolling over and allowing the executive branch to neuter them. Each branch must fully comprehend and carry out its constitutionally-defined role. This is especially true in light of the fact that advances in technology and science now enable any government to secretly invade a citizen's privacy at will and to whatever extent it desires. In the words of Louis Brandeis: Privacy is the "right to be let

[27] 50 U.S.C. §§ 1801-1846 (2000).

alone-the most comprehensive of rights and the right most valued by civilized men."[28]

I have a friend, a former trial lawyer, who shared a story of a case in the late 1970's in a small town in Vermont. The defendants in a criminal case were distributing marijuana and hashish from a farmhouse well off the beaten path. The Vermont State Police received a tip and, since they could not get physically close, they used devices developed in Viet Nam, a Startron[29] and Javelin,[30] to spy from a great distance.

These devices—even way back then—were able to read a newspaper from as far as two miles away, provided, of course, there were no obstructions. The police chose not to seek a warrant, but rather to surveil. Among the things they watched were the bathroom activities of some of the dopers' girlfriends. As frequently happens in "the often competitive enterprise of ferreting out crime,"[31] there was no independent judicial determination of probable cause, even though it likely existed. My friend reminded me of the curtilage cases, notably *Hester v. United States*[32] and its progeny, and stated he had framed his motion to suppress around the "curtilage" invasion issue. He won much of the motion; the fact of which saved his client about ten years of his life. Had the police obtained a warrant, all evidence almost certainly would have been admissible. The other important point for these considerations is that over thirty years ago, there existed the ability to visually intrude from miles away. Now, just consider where we are today—heat-seeking cameras of phenomenal range; cell phone transponders and microphones; cameras that can read license plates from space; data mining computers that make information retrieval systems, of one generation removed, seem so ancient that they appear to be like writing on stone tablets.

The question remains: does the government have to resort to illegal activity to protect us? Or is it sufficient to simply follow existing law and the principles and requirements of the Constitution?

---

28 Olmstead v. United States, 277 U.S. 438, 478 (1928).

29 Robert C. Power, *Criminal Law: Technology and the Fourth Amendment: A Proposed Formulation for Visual Searches*, 80 J. CRIM. L. & CRIMINOLOGY 1, 28 n.92 (1989). "Startron" is a night vision scope. *Id.*

30 *Id.* at 83 n.262. A Javelin is a nightscope, "capable of magnifying existing light 50,000 times." *Id.*

31 Johnson v. United States, 333 U.S. 10, 14 (1948).

32 265 U.S. 57 (1924).

This debate and inquiry are framed around the desire for freedom as balanced against occasionally necessary intrusions by a government, but premised always on the notion that we have a government that is itself to be governed by restraint. In the post-9/11 world, the necessary restraint has been lost, and although some of it had perished even prior to 9/11, the process has accelerated greatly since that awful day. Science and technology have long since left nothing to deter it save the determination of the humans who utilize it.

There is recently, a wonderful, thoughtful, and well-researched book by David Holtzman titled *Privacy Lost*, which I will now discuss.[33] I commend it to anyone concerned about the future of freedom and privacy in America.

The NSA and the view of the president that it is his absolute right to authorize any wiretap he deems appropriate notwithstanding, there are only two lawful bases for the creation of a legal wiretap: the Federal Wiretap Act[34] and the FISA[35] of a decade later. After 9/11, the USA PATRIOT Act[36] added to the list of crimes for which a wiretap could be legal, now including violent activities, terrorism, and suspected hijacking.[37]

The Federal Wiretap Act is, as it should be, a tightly regulated statute controlled by the courts of the United States. The fundamental procedure is that an application is made; if there is probable cause a judicial warrant is provisionally issued; then there are controls upon the listening, and a report back to the court is mandatory.[38] Thus, not only is there a court-required sanction, but continued judicial oversight.[39]

FISA has been the law of the land since 1978.[40] In its essence, the law is a portion of the solution to the problem of terrorism, which is part and parcel of a new form of espionage. Espionage is defined by Webster's as

---

33 DAVID H. HOLTZMAN, PRIVACY LOST (2006).

34 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified at 18 U.S.C. §§ 2510-2522 (2000)) (known as the Federal Wiretap Act).

35 Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1846 (2000).

36 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, 107 Pub. L. No. 56, 115 Stat. 212 (2001).

37 *Id*.

38 18 U.S.C. §§ 2510-2522 (2000).

39 *Id*. § 2518(6).

40 *See generally* 50 U.S.C. §§ 1801-1846 (2000).

the "practice of spying," but in practical reality it is more.[41] It is also the attendant desire to do harm to the entity spied upon, as those upon whom the spying is being perpetrated are presumably the enemy of those who are doing the spying. FISA and its court are equipped to address the fight against terrorism, as it was equipped to address the spying of every enemy that has existed since FISA was enacted and as strengthened since 9/11.

FISA, and the court created by it, allow for the issuance of warrants for surveillance of our nation's enemies, administer the prosecution procedures of those enemies once caught, and control the dissemination of the evidence to those appropriately able to have access to it.[42] For example, a defense lawyer for a person charged with a crime of espionage against the United States must be cleared by the FBI to the same extent as the nature of the evidence involved in the case. If the crime involves "Top Secret" evidence, then the lawyer must consent to a background check for clearance to a level of "Top Secret." Access to the evidence is monitored by a professional staff and never leaves a secure facility except under guard with prior court approval. This is the appropriate, pre-existing procedure that addresses this category of evidence in the fight against terrorists. The judges of FISC are selected by the Chief Justice of the U.S. Supreme Court.[43] What is important here is that it is a court—a branch of the judiciary—constitutionally charged with balancing powers of the executive branch by its oversight. Or, in the words of too many to count, the decisions are of "a neutral and detached" decision-maker (magistrate). This is, yet again, another example of how we, in the main as a nation, prior to this Administration, have sought to maintain the balance of a tri-partite government. Although, it should be noted, the USA PATRIOT Act diminished the standard from the traditional "probable cause" to "reasonable cause."[44]

B. The NSA and Government Snooping

Where does a secret and warrantless NSA spying program fit within these parameters? Simply put, it does not. However, President Bush reportedly concluded that FISA warrants took too long to obtain, so the

---

41 MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 427 (11th ed. 2003).

42 50 U.S.C. §§ 1801-1846. For example, § 1842 provides the procedure for and format requirements for pen trap devices. Further, the use of the information is governed by 50 U.S.C. § 1845. The Act also provides for congressional oversight. *Id*. § 1846.

43 *Id*. § 1842.

44 50 U.S.C. § 3103 (2000).

NSA spying program was initiated shortly after 9/11.[45] The program, dubbed by the Administration as the "Terrorist Surveillance Program" as part of its effort to lead the public—and Congress—to believe it did not surveil U.S. citizens within the U.S. borders (which it did), authorizes the NSA to wiretap without seeking a warrant.[46] President Bush apparently authorized it in 2002 by secret executive order. "Vast quantities of international telephone and Internet communications were intercepted without court approval."[47] The president originally claimed that only people connected to Al-Qaeda were tapped, but that has been subsequently determined to be false.[48] A president, under the guise of national security, is wiretapping Americans without benefit of the interposition of the courts and without probable cause, simply because he believes his role as "commander in chief" allows him to do so.

It is not only the NSA program that is suspect. The FBI has engaged in a program of attempting to track the locations of cell phone users; but two federal judges, one in New York and the other in Texas, have stopped them (at least temporarily) in the absence of a showing of evidence that a crime had occurred or is in progress.[49] The respective courts in those cases concluded that to allow the FBI to go forward would violate long-standing privacy protections.[50] More recently, in court proceedings, it has been revealed that federal agents are using cell phones to serve as general microphones—to listen to and record conversations not only by the holder of the cell phone, but others in the

---

45 HOLTZMAN, *supra* note 33, at 231. "In 2005, the *New York Times* ran an article revealing that President Bush had signed a secret executive order in 2002 authorizing the NSA to conduct warrantless wiretaps of Americans." *Id.*

46 *Id.*

47 *Id.* "Last year, Bush said he had authorized the NSA to eavesdrop—without warrants—on international calls and international e-mails of people suspected of having links to terrorists when one party to the communication is in the USA." Leslie Cauley, *Bush Lied Repeatedly About Scope of NSA Spying on Americans*, USA TODAY, May 11, 2006, *available at* http://www.unknownnews.org/0605190511NSAspying.html.

48 HOLTZMAN, *supra* note 33; *see also* Cauley, *supra* note 47 ("The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans—most of whom aren't suspected of any crime.").

49 *See, e.g.*, Jonathan Krim, *FBI Dealt Setback on Cellular Surveillance*, WASH. POST, Oct. 28, 2005, at A05. "The FBI may not track the locations of cell phone users without showing evidence that a crime occurred or is in progress, two federal judges ruled, saying that to do so would violate long-established privacy protections." *Id.* These rulings came as controversy increased over the ability of the federal government to conduct domestic surveillance as a result of the broadened powers granted under the USA PATRIOT Act after the 9-11 attacks. *Id.*

50 *Id.*

vicinity—a process that can be accomplished even if the cell phone is not turned on.[51]

An observation: whenever any legislative body takes action based on fear, the results are generally deleterious. The USA PATRIOT Act was conceived in fear; its gestation infested with fear; fear was its midwife; and its infancy fed by fear. The Act presented an invitation to abuse, and of course government agencies have accepted the invitation wholeheartedly. This law was intended to facilitate the interdiction of terrorism and terrorists.[52] Holtzman chronicles the abuses with explanations of each, but here they are referred to generically by type of target. The Act has been used to target anti-war protesters, organized crime, pranksters, the homeless, and artists.[53] It has been utilized to protect the intellectual property of big business.[54] Similarly, the Act was the moving force in the deportation of an ideological undesirable.[55] Of

---

[51] *See, e.g.*, Declan McCullagh & Anne Borache, *FBI Taps Cell Phone Mic as Eavesdropping Tool*, CNET NEWS, Dec. 1, 2006, *available at* http://news.com.com/FBI+taps+cell+phone+mic+as+eavesdropping+tool/2100-1029_3-6140191.html. "The technique is called a 'roving bug,' and was approved by top U.S. Department of Justice officials for use against members of a New York organized crime family who were wary of conventional surveillance techniques such as tailing a suspect or wiretapping him." *Id.*

[52] The very title of the Act reveals the purpose: "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001."

[53] HOLTZMAN, *supra* note 33, at 226-29. In 2004, Drake University was ordered under the authority of the USA PATRIOT Act to surrender all documents regarding an anti-war conference held on its campus. *Id.* at 226. Additionally, a "Justice Department report refers to more than a dozen cases in which federal authorities have used the Act to investigate private citizens, order surveillance, use wiretaps, and seize assets in nonterrorism criminal cases . . . . Money laundering, drug trafficking, blackmail and white-collar crimes are just a small sampling. . . ." *Id.* at 227. As for pranksters, the Justice Department is prosecuting a citizen as a terrorist for pointing a hand-held laser at an airplane. *Id.* Further, a homeless man in New Jersey was arrested as a terrorist for loitering in a train station. *Id.* Steve Kurtz, an artist who used materials he created in a home laboratory for sculpture materials, was impacted by the USA PATRIOT Act when his wife of twenty years died of heart failure at their home. *Id.* at 230. When medical authorities tending to Mrs. Kurtz noticed the laboratory equipment, the FBI was notified and they sealed off his home, confiscating everything including his wife's body. *Id.* He was labeled as a "bioterrorist" by the FBI and was indicted for "mail and wire fraud" and faces up to twenty years in prison. *Id.*

[54] *Id.* at 228. The FBI invoked the USA PATRIOT Act to obtain financial records from the ISP of an individual who ran a fan web site dedicated to the television show *Stargate SG-1*. *Id.* The fan was allegedly engaged in criminal copyright infringement and because of his world wide contacts via his website, he was alleged to have been engaged in a conspiracy against the Motion Picture Association. *Id.*

[55] *Id.* Sami-Al-Hyssayen, a student at the University of Idaho, was arrested for his work as webmaster for the Islamic Assembly of North America. *Id.* As part of his job, he maintained links to outside web sites, some of which advocated criminal activity. *Id.* Although he was ultimately found not guilty of terrorism, in exchange for that verdict, he agreed to be deported. *Id.*

course, it has also been used to target Muslims.[56] How is it done? Technology is the fulcrum—surveillance, wire taps, telephone taps, computers bugs—all weapons in the arsenal of the contemporary government watchers.

One of the many ironies of the NSA domestic surveillance spying program is that there was a Justice Department investigation conducted, but not into the legality or illegality of the program itself.[57] Rather the investigation was undertaken to determine the identity of those who had leaked information confirming the existence of the program. Instead of determining whether the NSA program violated our laws—FISA,[58] the Stored Communications Act,[59] and/or the Electronic Communications Privacy Act[60]—the top law enforcement agency of the nation is looking to identify the people who informed the public of the wrongdoing of its government.[61]

Congress has the power to create rules governing any surveillance based on the Constitution's structure of shared power over the nation's defense.[62] The president may possess some inherent authority to monitor the communications of Americans in the name of national security, but it is neither unilateral nor unlimited. The Congress, when it passed FISA, made repeated findings of the importance that any surveillance conform with the judicial checks and balances requirements of the Fourth Amendment. All of this was done because it has become evident over the years that the NSA, or any other agency of the government, was not to be trusted absolutely. In earlier decades, the NSA had created files on such "threats" as Dr. Benjamin Spock, Joan Baez, and Martin Luther King, Jr.[63] Indeed, the NSA attempted to surveil all Quakers in the United States, except, of course, the Quaker President, Richard M. Nixon.[64] Had it included the former president in its effort, the NSA might have avoided Watergate.

---

56 *Id*. at 228-29. "The *New York Times* reported that thirty-four credible human rights complaints were made by Arab and Muslim immigrants over a six month period in 2003." *Id*.

57 HOLTZMAN, *supra* note 33, at 231.

58 50 U.S.C. §§ 1841-1846 (2000).

59 47 U.S.C. § 222 (2000).

60 18 U.S.C. §§ 2510-2522 (2000).

61 Dan Eggen, *Size & Scope of the Interagency Investigative Tool Worry Civil Libertarians*, WASH. POST, Dec. 26, 2006, at A07.

62 U.S. CONST. art. 1, §§ 1, 8.

63 HOLTZMAN, *supra* note 33, at 220 n.14.

64 *Id*.

But the year 1978 appears to be too long ago to have kept the congressional memories fresh; the collective memory seems to have forgotten the four precepts of FISA. First, Congress must have full and complete disclosure of all surveillance programs.[65] Second, Congress commanded that the statutory procedures it created—FISA—would be the "exclusive" procedures for conducting surveillance of Americans in the name of national security.[66] Third, Congress required a judicial check on every wiretap of the electronic communications of Americans in this country.[67] Fourth, and finally, the Congress, through FISA, required that court orders be predicated upon probable cause either that the target of electronic surveillance was an "agent of a foreign power" (a term very broadly defined in the law) or was an American citizen knowingly conspiring with or aiding such an agent.[68]

Although FISA has been amended a number of times since its 1978 enactment, including several changes effected by the 2001 USA PATRIOT Act, these four requirements/prohibitions have never been removed or weakened.[69] They have remained in full force and effect, serving the nation well since their enactment almost thirty years ago. Indeed, at a public hearing in 2000, before the House Intelligence Committee, then NSA Director, General Mike Hayden (now head of the CIA), testified explicitly that if the NSA believed it necessary to surveil a U.S. person in the United States, the NSA must secure—and always did secure—a court order.[70] Now, other than new enemies, and new responders in the government, what has changed? Not the warrant requirement under FISA; that remains the law of the land in 2007 as it did in 2000 when General Hayden so testified.

---

65 50 U.S.C. § 1808 (2000). "On a semiannual basis the attorney general shall fully inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, and the Committee on the Judiciary of the Senate, concerning all electronic surveillance under this title." *Id*. § 1808(a)(1).

66 *Id*. § 1808.

67 *Id*. § 1842. Judicial oversight is required via the detailed procedure laid out in this section for obtaining a warrant. *See id*. § 1842(a)-(b).

68 *Id*. § 1842(a)(1) (providing that an application may be made to install a pen trap device if it is to obtain foreign intelligence information not concerning a United States person or that the application was not based on protected first amendment activities); *see also id*. § 1801(b).

69 *Id*. §§ 1841-1846, *as amended* by Pub. L. No. 95-511 (1998); Pub. L. No. 105-272 (2001); Pub. L. No. 107-56 (2001); Pub. L. Nos. 107-108 and 108-458 (2004); Pub. L. No. 109-177 (2006).

70 *Hearing Before the House Permanent Select Comm. on Intelligence*, 106th Cong. (Apr. 12, 2000) (statement of Gen. Mike Hayden).

The largely somnambulant post-9/11 Congress reacted concerning disclosures of the NSA spying program, as mentioned earlier, with two different bills, one by Senator Specter, the other by now-former Senator DeWine.[71] Senator Arlen Specter of Pennsylvania, a highly respected member of the Senate, a former U.S. Attorney, and immediate past chairman of the Senate Judiciary Committee proposed Senate Bill 2453 on March 15, 2006, titled the "National Security Surveillance Act of 2006."[72] It is important to note, were he able to get the bill passed, Senator Specter would have changed the law to adjust the four pillars of FISA.[73] Much like Congress seems to have lost its way after 9/11, the Bill would neuter the most important elements of FISA. In so doing, the Congress would cede any involvement in checks and balances as envisioned by the Founding Fathers. Partisan politics aside, why would any legislative body, in this form of government, do such a thing? The answer is simple, but overwhelmingly disturbing—Congress had abandoned its prerogatives.

Mandatory congressional oversight would have disappeared under the Specter bill.[74] Congress would legislate without investigating because the Judiciary Committee, according to the White House, has no right to obtain facts concerning how the executive branch is executing FISA (or ignoring it). This is true, in spite of the fact that Congress is entitled to full disclosure of all surveillance programs.[75] This represents an absolute abdication of responsibility.

Senator Specter's bill would have repealed the requirement that the president follow the FISA warrant rules; it also would have done away with the criminal penalties for violations.[76] The president, in this

---

71 National Security Surveillance Act, S. 2453, 109th Cong. (2006); Terrorism Prevention Act of 2006, S. 3848, 109th Cong. (2006).

72 National Security Surveillance Act, S. 2453, 109th Cong. §§ 1-9 (2006).

73 S. 2453, 109th Cong. §§ 4-7.

74 S. 2453, 109th Cong. §7.

75 50 U.S.C. § 1808 (2000).

76 S. 2453, 109th Cong. §§ 8, 706. Section 8 states that:

> It is in our Nation's best interest for Congress to use its oversight power to establish a system to ensure that electronic surveillance programs do not infringe on the constitutional rights of Americans, while at the same time making sure that the President has all the powers and means necessary to detect and track our enemies.

Section 706 provides emergency authorization for the President to authorize electronic surveillance without a warrant.

scenario, would be forgiven of any criminal misconduct, no matter how egregious, as would be all of his subordinates.[77]

The bill would have made judicial oversight optional.[78] The administration could, if it chose, seek the approval of the courts, or alternatively not, as the case may be. In other words, it would have given the president the option of following the law or ignoring it. Such a scenario certainly was never intended to prevail in our system of government, based as it is on specified and limited government powers and respect for the courts and for individual privacy.

The Specter bill also would have eliminated the "probable cause" requirement, meaning there could be electronic surveillance of you or me, for any reason or no reason.[79] The decision would be purely at the discretion of whatever executive branch employee made it.[80] When one considers how insubstantial the hurdle of "probable cause" is generally for law enforcement, the scenario allowed by the Specter bill would constitute a gift-wrapping of all of our freedoms and tossing them down the drain.

The ACLU proposed an appropriate alternative to the Specter and DeWine bills in the previous, 109th Congress.[81] This bill, the "Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006," would have accomplished exactly what the title indicated. Its salient points were a re-emphasis of the exclusivity of FISA for electronic surveillance, while maintaining a warrant requirement (although the time strictures would be relaxed).[82] It also streamlined and added resources for this specialized court. In particular, this 2006 legislation would have extended the emergency electronic surveillance period from three days to seven, which either the NSA or the FBI could initiate, provided the Attorney General was notified within twenty-four hours and the application was made within seven days.[83] The Attorney General could also delegate authority to approve applications to a Deputy Attorney General or an Assistant Attorney General for National

---

77 S. 2453, 109th Cong. §§ 8, 706.

78 S. 2453, 109th Cong. §§ 6, 704.

79 S. 2453, 109th Cong. § 703(a).

80 *Id.*

81 Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, S. 3877, 109th Cong. (2006).

82 *Id.* For example, section 201 would have extended the time stricture from 72 hours to 168 hours. *Id.* § 201.

83 S. 3877, 109th Cong. § 203, 105(g)(3).

Security.[84] In addition, the ACLU-backed proposal allowed for additional judges and appropriations for the same.[85] It also provided document security procedures and a specific personnel increase in needed areas.[86] Finally, the FISA improvement bill would have allowed for streamlined procedures to facilitate the needs of the government in protecting the nation.[87]

All told, the ACLU proposal would have met the needs of twenty-first century priorities so that law enforcement would not be hampered in its battle against terrorists and acts of terrorism. Indeed, it would have enhanced the capabilities of law enforcement while maintaining what should be a universally cherished standard of privacy, unless and until there is a reason for intruding on it. By maintaining the interposition of a court (though a secret one) and a warrant requirement (though a relaxed one) there is an intermediate step, and a need to justify an intrusion that is, and should be, fundamental to a free society. In the context of refusing a blank check for the executive branch, and reinforcing the involvement of the judiciary, the legislature would take an important step toward the re-promulgation of a system of checks and balances that has eroded significantly since September 11th.

Aside from the illegal secret listening and snooping NSA program, this administration has been extremely active through the ordinary channels of FISA. Since the 9-11 terrorist attacks, FISA warrants have increased by seventy-five percent.[88] In 2000, a year before the attacks, there were 1,003 approved FISA warrants.[89] Since the attacks, and post-PATRIOT Act, there were 1,724 warrants approved in 2003, and 1,754 in 2004.[90] These warrants, almost never declined by the court, have been obtained to break into homes, offices, hotel rooms, and automobiles.[91] They have also been used to install hidden cameras, search luggage, eavesdrop on telephone conversations, watch from great distances, pry into safety deposit boxes, and intercept emails.[92] However, every one of these, no matter the nature of the intrusion, was accompanied by a warrant, administered presumably pursuant to either a probable cause

---

84 S. 3877, 109th Cong. § 206.
85 S. 3877, 109th Cong. § 204.
86 S. 3877, 109th Cong. §§ 205-206.
87 *Id.*
88 The Associated Press, *Government Wiretaps, Searches up 75 Percent*, Apr. 1, 2005, www.truthout.org/cgi-bin/artman/exec/view.cgi/37/10080.
89 *Id.*
90 *Id.*
91 *Id.*
92 *Id.*

standard or the USA PATRIOT Act "reasonable cause" standard.[93] Even though the court is secret, somewhere in each instance there is a paper trail, and perhaps a somewhat therapeutic pause in law enforcement zeal while the determination was made to secure the warrant. In short, the Fourth Amendment is at least a part of the equation, giving the individual citizen at least a fighting chance that his or her privacy was afforded due protection.

IV. NEW SURVEILLANCE REDUNDANCE

The Administration's fellow travelers are not limited to the Congress and its attendant reluctance—at least until just recently with the new majority in the 110th Congress—to stand and be counted. There are many others whose involvement comes about in a variety of ways with a significant emphasis on money. One only need look at the total of the Homeland Security Grants of Fiscal Year 2005 to know of the enormous amount of dollars being spent, and the nature of the expenditures. The "State Homeland Security Grant Program" awarded a total dollar amount of $1,062,285,226.[94] The "Law Enforcement Terrorism Prevention Program" awarded $386,285,537.[95] The "Citizen Corps Program" awarded $13,485,708.[96] The total awards for Fiscal Year 2005 were just under $1,500,000,000.[97]

Was this money well spent to preserve our lives *and* our freedom? A simple analysis of the use of the funds in several locations might answer those questions. For example, in Chicago, there is a rapidly expanding "Homeland Security Grid" that currently has at least 2,250 cameras, with more being added each year thanks to federal funding.[98] In 2006, Chicago completed a 900-mile fiber-optic grid connected to a $43 million operations center that is constantly monitored by police officers, with each camera costing $60,000.[99] This money might be considered well-

---

93 18 U.S.C. § 3103a(b)(1) (Supp. IV 2004).

94 HOMELAND SECURITY GRANTS FY05, http://www.dhs.gov/xlibrary/assets/Grants_Summary_StLocal.xls (last visited Feb. 5, 2007).

95 *Id.*

96 *Id.*

97 *Id.*

98 Electronic Privacy Information Center, *Spotlight on Surveillance*: *More Cities Deploy Camera Surveillance Systems with Federal Grant Money* (May 2005), http://www.epic.org/privacy/surveillance/spotlight/0505/ hereinafter EPIC].

99 *Id.*; *see also* Hal Dardick, *City Will Keep Eyes Peeled Big Time*, CHI. TRIB., Feb. 11, 2005, at C1 (detailing the extensive camera system that Chicago planned to implement including a fiber optic grid of over 1,000 miles and "biochemical sensors to watch for signs of terrorism").

spent if it had actually decreased the threat of terrorism and if it did not coincidentally intrude into the legitimate privacy of its citizens. On a related point, in 2004, a Milwaukee, Wisconsin study found that law enforcement officials in such cities as Detroit, Michigan; Miami, Florida; and Oakland, California; abandoned the use of programs utilizing these surveillance systems because they had little demonstrable effect on crime prevention.[100]

Currently, a number of American cities are looking to Great Britain's surveillance system when developing their own. London already has more than 200,000 cameras, with more than four million deployed throughout the country.[101] In Great Britain, estimates indicate there is one camera for every fourteen people, and that the average Briton is on camera over 300 times a day.[102] Yet "studies have shown these systems have little effect on crime." [103] "It is [much] more effective to place more officers" in a location and keep it well lighted.[104] If it is true that these types of surveillance units do not significantly impact crime, then how effective are they at interdicting terrorist activity? As a partial answer to this question no bomber has been caught in Britain as a result of the country's extensive camera system.

"According to a January [2003] report by J.P. Freeman, a security market-research firm in Newtown, Connecticut, [some] twenty six million . . . cameras" had, at that time, been installed worldwide.[105] More than eleven million of those had been installed in the United States, and many more by now.[106] Some municipalities are now incorporating

---

100 EPIC, *supra* note 98*; see also* Ryan Davis, *Surveillance Cameras May Soon Be Coming to a Street Near You*, BALT. SUN, Mar. 16, 2005, at 1B. The Milwaukee study found that "cities were most commonly using closed-circuit surveillance located in police cars, interrogation rooms, government buildings, for special events and in high crime areas." *Id.* Despite improving technology, only 20% of police agencies surveyed in the study found that these cameras were effective in reducing crime. *Id.*

101 EPIC, *supra* note 98

102 *Id*.

103 *Id*.; *see also* Davis, *supra* note 98.

104 EPIC, *supra* note 98; *see also* BRANDON C. WELSH AND DAVID P. FARRINGTON, HOME OFFICE RESEARCH, DEVELOPMENT AND STATISTICS DIRECTORATE, CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW, RESEARCH STUDY 252 (Aug. 2002).

105 Dan Farmer & Charles C. Mann, *Surveillance Nation: Part One*, TECH. REV., Apr. 2003, at 34, 36. Farmer and Mann discuss throughout how the low priced surveillance technologies can assist citizens in protecting their safety and property, at the same time, "as these informal intelligence-gathering networks overlap and invade our privacy, that very security and convenience could evaporate." *Id.* at 34.

106 *Id*. at 36.

sound-surveillance devices with cameras.[107] However, the use of these cameras by the government, and the images captured, is questionable.

A. Are the Priorities in Order?

The FBI purports to be the point entity in the "War on Terrorism" and yet there is evidence that valuable resources have been utilized gathering information on antiwar and environmental activists. "'They don't know where Osama bin Laden is, but they're spending money watching people like me,' said environmental activist, Kirsten Atkins."[108] Atkins's license plate number had shown up in an FBI terrorism file after she had attended a protest in Colorado Springs against the lumber industry.[109]

In 2006, "an FBI counterterrorism official showed the class, at the University of Texas at Austin, 35 slides listing militia, neo-Nazi, and Islamist groups."[110] "Senior Special Agent Charles Rasner said one slide, labeled 'Anarchism,' was a federal analyst's list of groups that people intent on terrorism might [well be] associate[d] with. The list included Food Not Bombs, which mainly serves vegetarian food to homeless people . . ."[111]

What is troubling about these incidents, and numerous others, is that this is indicative of a culture, a thought process. Remembering that these are the same genre of people who are manning the electronic and visual surveillance apparatus, what does such overreaching portend?

Does all of this mean we have become what science fiction writer David Brin called in 1998 "the transparent society?"[112] "The far-sighted Brin underestimated how quickly technological advances . . . would make universal surveillance" a very real probability.[113] Modern-day microprocessors have become immensely powerful, network transmissions incredibly fast, hard drives larger, electronics cheaper, and software more sophisticated and powerful.[114] Improvements are made daily. This makes it imperative that manipulators of information and surveillance be held accountable. They must also be controlled by

---

107 *Id.*
108 Nicholas Riccardi, *FBI Keeps Watch on Activists*, L.A. TIMES, Mar. 27, 2006, at A1.
109 *Id.*
110 *Id.*
111 *Id.*
112 Farmer & Mann, *supra* note 105, at 36.
113 *Id.*
114 *Id.*

effective laws and aggressive enforcement of those laws. By 2023 (if not sooner), experts predict that any large organization with resources of just $10 million "will be able to devote the equivalent of a contemporary PC to monitoring every one of the projected 330 million people who will then be living in the United States."[115] So it is not only the government that is a subject of concern, but the private sector as well.

B. Defective Data Records

Of equal importance, as are the law and the responsibility of the government keeper's, is the care taken in creating the databases and the information contained within them. In 2003, Marc Rotenberg, Executive Director of the Electronic Privacy Information Center ("EPIC"), a non-profit research organization in Washington, D.C., stated: "What seem to be small scale, discrete systems end up being combined into large databases." [116] He pointed, by way of example, to the then-recent, voluntary efforts of a variety of merchants in Washington, D.C.'s affluent Georgetown to pool and integrate their in-store, closed-circuit television networks, to make the combine recorded activity available to the police.[117] In his concern, Rotenberg viewed the collection and consolidation of individual surveillance networks into big government and industry programs as "a strange mix of public and private, and it's not something that the legal system has encountered much before."[118]

The question, among others, of these conglomerate databases is, what if there is defective information contained within them? According to the experts, this is so commonplace as to be beyond question. The result is a potentially monster database being used to shadow, target, and move against innocent citizens.

Computer scientists use the term "GIGO" (garbage in, garbage out) to describe the situation of erroneous information becoming a part of a database.[119] Once in, it skews the validity of the database.[120] Whether people are buying bread or building bombs, governments and commercial enterprises are trying to predict their behavior, through such "data mining" (recall the movie "Minority Report"). The process of predicting behavior is an integration of data from widely diverse

115 *Id.* at 38.
116 *Id.* at 40.
117 *Id.*
118 *Id.*
119 *Id.*
120 *Id.*

sources. Starting with the Internet and proceeding along to such things as library records, credit-card receipts, customer cards, and financial or medical records, data miners use such information to form their predictions. But—and this is a significant "but"—there are problems.

The first problem, of course, is the premise on which data mining is based—that disparate bits of data on a diverse universe of people (e.g., all people who travel by air) can be employed to predict behavior of a very small number (e.g., persons planning to hijack an airliner). Also, of course, is the fact that all of these sources are filled with errors. Names are misspelled, one digit is off, information becomes out of date by a move or a change of Internet provider, and most importantly, formatting distinctions between different databases can cause distortions and information loss when merged.[121] Perhaps the buyer of bread becomes the bomber and the suspected bomber is merely buying bread.

Larry English, of Information Impact, a database consulting company in Brentwood, Tennessee, stated: "It is routine to find in large customer databases defective records . . . at rates of at least 20 to 35 percent."[122] Given the government's track record, which includes maintenance of "watch lists" containing names of such well-known public officials as Massachusetts Senator Edward Kennedy and Georgia Congressman John Lewis, it is only fair to presume that secret government databases suffer from such errors of at least a similar magnitude.

Effective use of large surveillance databases can be problematic aside from the fact it destroys the notion of privacy. The systems are already in place; it is their use which must be responsible, careful, and lawful. Reactive use, rather than proactive use, might be one starting point. For example, the 2002 Washington, D.C., sniper search might have utilized the surveillance cameras to pinpoint repeat blue Chevy appearances on cameras at the scenes as opposed to attempting to predict that a person or persons who was disgruntled, had trouble at home, and was militarily-trained, was the shooter.

Gene Spafford, Director of Purdue University's Center for Education and Research in Information Assurance and Security, said in 2003: "Almost all of the pieces of a surveillance society are already here. It's

---

121 *See generally* Steven W. Dummer, *Secure Flight and Dataveillance, A New Type of Civil Liberties Erosion*: *Stripping Your Rights When You Don't Even Know It*, 76 MISS. L.J. 583 (2006).

122 Farmer & Mann, *supra* note 105, at 40.

just a matter of assembling them."[123] That process has had an additional three years to continue. The "War on Terror" makes it absolutely certain it has continued. Where do the invalid answers from the tracking systems affect us? Invalid answers can be harmless. If Victoria's Secret mistakenly mails one percent of its spring catalogue to people who are not interested in lingerie, the price exacted to both consumer and company is small. However, if we are discussing a national terrorist tracking system, and the rate of error is that same one percent (an unrealistically low estimate), then it will produce enormous numbers of false alarms, sending investigators on too many wild goose chases, and perhaps worst of all, mis-label innocent Americans.[124] As Spafford stated: "A 99 percent hit rate is great for advertising, but terrible for spotting terrorism."[125]

Where do we demand oversight to combat these errors in the databases of the governments? Is it acceptable in this society for a lawyer from Portland, Oregon to spend time in jail because of an error in recording a fingerprint in Madrid, Spain (considering the attendant prejudice and perhaps lifelong label)? Fingerprint technology is far more easily controlled than that of computers, webs, and networks. Yet, at least the government and much of corporate America is rushing headlong into a surveillance society rife with errors and without adequate safeguards of either electronics or law.

C. "One DOJ" Database

According to a December 26, 2006 article in the *Washington Post*, the Department of Justice is building a massive database that allows state and local police to search millions of files from the FBI, DEA, and other federal law enforcement agencies.[126] As of December 26, 2006, the database is purported to hold over one million case records, and "is projected to triple in size over the next three years."[127] There is no report concerning this new database as to what, if any, procedures have been utilized by the government to ensure that information contained within it is correct, current, relevant, and without errors. The goal is to give all federal, state, and local law enforcement access to all records of cases

---

123 *Id.* at 37.

124 *Id.*

125 *Id.* at 43.

126 Dan Eggen, *Justice Dept. Database Stirs Privacy Fears: Size and Scope of the Interagency Investigative Tool Worry Civil Libertarians*, WASH. POST, Dec. 26, 2006, at A07.

127 *Id.*

containing personal information about people, many of whom have not been arrested or charged with any crime.

Deputy Attorney General, Paul McNulty, said, in a memo sent the week before Christmas to the FBI, U.S. Attorneys, and other senior Justice officials, that federal authorities will "accelerate . . . efforts to share information from both open and closed cases."[128]

The "garbage in, garbage out" proviso discussed previously is especially relevant to this database as there are no controls on what an individual agent puts into a criminal, or worse, potential criminal file. Rumor, innuendo, and the lies of informants are part and parcel of the entire criminal investigative process. That apparently will not stop this progression of "OneDOJ," unless Congress intervenes.

D. The Department of Justice: Investigation of Its Role in the NSA Program

In November 2006, the Inspector General for the Department of Justice reported to the House Judiciary Committee that the office had "decided to open a program review that will examine the Department's controls and use of information related to the program," but the investigation is not expected to address whether the controversial program is an unconstitutional expansion of the power of the president, as its critics and a federal judge in Detroit, Michigan have charged.[129] A Justice Department spokesman, Brian Roehrkasse, stated that the agency welcomed the review, and that the Justice Department believes the review "will assist Justice Department personnel in assuring that the department's activities comply with the legal requirements that govern the operation of the program."[130]

The Inspector General's office, however, rejected the request by more than three dozen Democrats to investigate the secret program, which monitors phone calls and emails between people in the U.S. and abroad when a link to terrorism is suspected.[131] One of the goals of this investigation could be a determination as to whether the spying program

---

128 *Id.*

129 Letter from Glenn A. Fine, Inspector General, U.S. Dep't of Justice, to Zoe Lofgren, Member of the U.S. House of Representatives (Nov. 27, 2006), *available at* http://www.house.gov/lofgren/112706_DOJ_NSA_ Investigation.pdf; *see also* ACLU v. Nat'l Security Agency, 438 F. Supp. 2d. 754 (E.D. Mich. 2006).

130 Dan Eggen, *Justice Dept. to Examine Its Use of NSA Wiretaps*, WASH. POST, Nov. 28, 2006, at A10.

131 *Id.*

is in compliance with FISA, discussed previously.[132] I would like to pose a rhetorical question in that regard. Unless the NSA spying program had a double secret (the author is reminded of the double secret probation that Dean Wormer placed on the "Animal House" fraternity in the movie of the same name) application for judicial authorization for electronic surveillance, and/or searches, of those suspected of espionage and international terrorism, then how can there be compliance with FISA?

One observation that critics and questioning Democrats have made was the timing of the announcement of the investigation. The request for additional clearances was made on October 20, 2006, just prior to the election, and were approved just after the elections.[133] Of course, Attorney General Gonzales had been pushing the former Republican-led Congress to pass what amounts to an ex post facto legalization of the program as discussed earlier concerning the Specter and/or the DeWine bills. Those bills died in the 109th Congress as well they should.[134]

V. THE BALANCE BETWEEN SECURITY AND A FREE SOCIETY—WHERE ARE WE TODAY?

Again, a quote from Mr. Justice Brandeis is *apropos* to what is confronted in the world we have inherited today. Justice Brandeis predicted:

> Subtler and more far-reaching means of invading privacy have become available to the government. . . . Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . "It is not the breaking of his doors, and the rummaging of his drawers that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property."[135]

---

132 Bruce Fein, *Trusting the White House*, WASH. TIMES, http://washingtontimes.com/commentary/20070108-114405-3884r.htm (last visited Jan. 9, 2007).

133 *Id.*

134 *Id.*

135 Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) (quoting Entick v. Carrington, 19 Howell's State Trials 1030, 1066 (1765)).

A more prescient pronouncement would be hard to find.

At least two federal judges, one in Texas and one in New York, have upheld traditional "probable cause" standards in denying the FBI the ability to track the movements of cell phone users in the absence of a showing that a crime had occurred or was in progress.[136] The judges did, however, approve other requests in those cases including the logging of calls made and those received.[137] A reasonable translation of that ruling is that the FBI should investigate and not take short cuts, but when there is in fact evidence of criminal misconduct, they will get what they want. At least, in these two cases, we have come full circle with the recognition that the Fourth Amendment is still the law of the land, and that, as it persists, there is vitality to the concept of constitutional freedom in this country.

There is also welcome evidence that the new, Democrat-led Congress is forcing the legislative branch of our government to begin re-asserting its role in ensuring that the executive branch operates within the bounds of the law and the Constitution. The very first hearing of the Senate Judiciary Committee in the 110th Congress, for example, considered and received testimony on the role of data mining and its impact on privacy rights of American citizens.[138] A week later, the Attorney General was intensely questioned before the same panel of Senators about secret surveillance, warrantless opening of mail, and other invasions of privacy.[139] If these early actions by the 110th Congress are followed by two years of real oversight, and passage of protective legislation like Senator Russ Feingold's Senate Bill No. 236, a bill to require reports to Congress on federal agency use of data mining,

---

136 Krim, *supra* note 49, at A5.

137 *Id.*

138 *See e.g.*, Rebecca Carr, *Privacy Advocates Blast Data Mining; 'Completely Out of Control': Senate Panel Told Fed's Programs Infringe on Individual's Rights*, ATLANTA J.-CONST., at 5C (stating that a panel of privacy experts told the Senate Judiciary Committee that congressional oversight is needed to ensure that the federal government's data-mining programs are not interfering with individual privacy rights); Carol Eisenberg, *Leahy to Seek Data-Mining Oversight*, NEWSDAY, Jan. 11, 2007, at A24 (stating that in his first hearing as chairman of the Senate Judiciary Committee, Sen. Patrick Leahy promised to make congressional oversight of government data mining programs his top priority).

139 *See Taps*, NEW REPUBLIC, Feb. 5, 2007, at 7. *Taps* recounts Gonzales's first appearance before the democratically controlled Senate Judiciary Committee, in which he found himself assailed by members of both parties. Specifically, Gonzales was questioned about: (1) authority to open the mail of American citizens without a warrant; (2) the details of the governments new surveillance program; and (3) a recent speech in which he declared that a judge will never be in the best position to know what's in the national security interest of the country. *Id.*

introduced on January 10, 2007, there just might be some real constitutional light at the end of the dark tunnel in which we have been living since September 11.[140]

We must not, however, be content with minimalist efforts without sustaining power. We must always remember that power, of any government, once attained is never easily relinquished. This Article has emphasized the electronic in its purview, but an old fashioned communication system note provides a reaffirmation of this most fundamental of principles of government power acquisition. On January 8, 2007, it was widely reported that, as President Bush signed a recent postal reform bill, he added a signing statement that, though this law allegedly enforced existing postal privacy, allowed the opening of mail by federal agents for "exigent circumstances" without the interposition of a warrant.[141] Will Congress step in here too and force the president, believing himself all-powerful, as a self-proclaimed "commander-in-chief" to abide by the Constitution to which he swore an oath in 2001 and again in 2005? Of course, it is not just the current president. History teaches us that each president considers the powers granted or taken by his predecessors to constitute a floor, not a ceiling, for the powers he will enjoy.

For its part, the Bush Administration announced January 17, 2007, that it would suspend the "Terrorist Surveillance Program," which is the name it gave to the program of warrantless eavesdropping on American citizens in the United States without any court orders.[142] The Administration stated that it would henceforth run activities conducted under that program through the FISC.[143] This announcement reflects the reality of a president no longer being able to count on a somnambulant Congress to ratify or at least not conduct serious oversight of his activities in this area, and the announcement is therefore a welcome step. However, insofar as this Administration has in the past simply changed the name of problematic programs and then continued them, the Congress must conduct vigorous and continued oversight to understand, in much greater degree than it has thus far, exactly what the Administration has been doing in this regard. Once Congress has done so, it must then take steps to ensure that the Administration actually

---

140 *See* S. 236, 110th Cong. (2007).

141 *See* Fein, *supra* note 132 (describing the December 20th presidential signing statement).

142 *See* James Vicini, *Bush Won't Reauthorize Eavesdropping* (Jan. 17, 2007), *available at* http://today.reuters.com/news/articlenews.aspx?type=topNews&storyid=2007-01-17T204435Z_01_N17341517_RTRUKOC_0_US-SURVEILLANCE-BUSH.xml.

143 *Id.*

stops the unlawful and unconstitutional practice of surveilling American citizens without court orders.