0091-4169/06/9603-1059
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 96, No. 3

Printed in U.S.A.

CRIMINAL LAW

ANGLO-AMERICAN PRIVACY AND SURVEILLANCE

LAURA K. DONOHUE*

TABLE OF CONTENTS

* Fellow, Center for International Security and Cooperation, Stanford University. Special thanks to Paul Lomio, Sonia Moss, and Erika Wayne at the Robert Crown Law Library, for help in acquiring the materials used in this article. I am indebted to Barbara Babcock and Robert Weisberg for suggestions on the American constitutional discussion and to Clive Walker for comments on British surveillance law. This piece is part of a longer study of counterterrorist law in the United Kingdom and United States that will be published this coming year by Cambridge University Press.

INTRODUCTION

In October 2001, President George W. Bush authorized the National Security Agency ("NSA") "to intercept the international communications of people with known links to al Qaida and related terrorist organizations."[1] Four years and two months later, news of the program became public. Attorney General Alberto Gonzales defended the Commander-in-Chief's power to ignore warrants otherwise required under the Foreign Intelligence Surveillance Act or Title III of the Omnibus Crime Control and Safe Streets Act.[2] Congress itself had authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided" the 9/11 attacks.[3] For Gonzales, this meant that the President was acting "at the zenith of his powers" under the tripartite framework set forth by Justice Jackson in *Youngstown v. Sawyer*.[4]

This was not the first time Article II claims backed surveillance programs designed to protect the United States from attack. In the midst of the Cold War, the NSA ran Operations SHAMROCK and MINARET. The Federal Bureau of Investigation ("FBI") orchestrated COINTELPRO and amassed over 500,000 dossiers on American citizens. The Central Intelligence Agency ("CIA") oversaw Operation CHAOS and built a database that tracked 300,000 people. Routine counterintelligence operations disrupted everything from women's liberation to the civil rights movement.

However, in 1978, Congress introduced the Foreign Intelligence Surveillance Act ("FISA") precisely to prevent unchecked executive surveillance of American citizens. And congressional interest in ensuring

---

[1] President's Radio Address, 41 Weekly Comp. Pres. Doc. 1881 (Dec. 17, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051217.html.

[2] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102, 92 Stat. 1786 (1978) (codified as amended at 50 U.S.C. §§ 1801-11 (2000)); Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, tit. 3, 82 Stat. 212 (codified at 18 U.S.C. §§ 2510-20).

[3] Authorization for Use of Military Force, Pub. L. No. 107-40, §2(a), 115 Stat. 224, 224 (2001) (reported as a note to 50 U.S.C. § 1541).

[4] U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 2 (2006) (discussing Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring)).

oversight did not end there: in 1991 Congress amended the 1947 National Security Act to require the President to keep the congressional intelligence committees "fully and currently informed" of surveillance programs underway, including any "significant anticipated intelligence activity."[5]

According to Rep. Jane Harman, instead of telling the full committees in both houses about the recent NSA's domestic spy program, the executive branch only gave notice to the "Gang of Eight"—the majority and minority leaders of both houses, and the chairs and ranking members of the congressional intelligence committees.[6] Although this would have constituted sufficient notification for covert action (which excludes activities aimed at acquiring information), Harmon claimed it stopped short of the statutory requirement.

Wherever one falls in this debate, the NSA program represents only one of many expansions in executive surveillance since 9/11. Legal controls previously introduced to protect citizens' privacy and to prevent the misuse of surveillance powers have been relaxed. What makes the situation qualitatively different now is not just the lowering of the bar: digitization and the rapid advancement of technology mean that the type and volume of information currently available eclipse that of previous generations. And the issue is not confined to the United States. Despite the incorporation of the European Convention of Human Rights into British law, the United Kingdom also appears to be losing privacy in its battle against terrorism.

Part I of this article looks at the American institution of legal controls on the executive branch and their subsequent erosion post-9/11. It explores three changes incorporated in the USA PATRIOT Act: alterations to the Foreign Intelligence Surveillance Act; the introduction of Delayed Notice Search Warrants; and the expansion of National Security Letters. Outside of this legislation, the weakening of the Attorney General guidelines increased the FBI's ability to collect information. The article highlights the Department of Defense's ("DOD") movement into the domestic surveillance realm. It discusses a number of operations both inside and outside the DOD, such as TALON, Echelon, Carnivore, Magic Lantern, TIPS, and the use of watch lists. Part I concludes with a discussion of the data mining efforts underway. The article argues that Total Information

---

[5] Fiscal Year 1991 Intelligence Authorization Act, Pub. L. No. 102-88 (current version at 50 U.S.C. §§ 413-13(b)) (amending the National Security Act of 1947, Pub. L. No. 80-253, §§ 501-03, 61 Stat. 495 (1947)).

[6] Letter from Jane Harman, Representative from Cal., to George W. Bush, President of the United States (Jan. 4, 2006), *available at* http://www.house.gov/harman/press/releases/2006/0104PRnsaprogram.html.

Awareness, ADVISE, and other projects catapult surveillance into another realm. Moreover, while any one program, such as the NSA initiative, may be considered on narrow grounds, the sheer breadth of current powers raises important concerns.

Part II notes that, until recently, no laws governed police and intelligence service information-gathering authorities in the UK. Extraordinary stop and search powers for terrorist-related offences, and warrants for police interference with property provided exceptions. But physical searches of property conducted by the intelligence services, the interception of communications by law enforcement and intelligence agencies, the use of covert surveillance or "electronic bugs," and the running of covert human intelligence sources operated under the legislative and judicial radars. Beginning in the mid-1980s, the European Court began to raise objections to the lack of safeguards and statutory framework. But each time the Court handed down a significant finding against the United Kingdom, the state responded not just by, at least on the surface, meeting the demands of the European Convention of Human Rights, but, it appears, by *expanding* executive surveillance authorities. Moreover, the warrant system introduced retained control within the executive branch. Not subject to judicial review, the standard applied is reasonable suspicion—considerably less robust than probable cause. Like the United States, Britain draws on new technologies; the country leads the world in its use of public surveillance systems.

Having laid out legal developments on both sides of the Atlantic, Part III moves to policy concerns: it begins by briefly exploring the substantive, political, legal, social, and economic risks posed by such measures. It then considers six approaches that would help to mitigate the risks. First is the possibility of creating a property right in personal information. The second centers on the regulation of access, transfer, use, and retention of data. Such efforts would satisfy demands for accountability and transparency in both the public and private sector. A third possibility centers on scaling back the existing powers of the state. Fourth, both countries may contemplate placing limits on what constitutes national security. Fifth, alternative safeguards and oversight structures deserve attention—such as reporting requirements, random audits, the creation of ombudspersons, the insertion of the judiciary, and (in the UK) allowing intercepted communications to be used as evidence. Sixth, preventing countries from introducing ever greater powers of surveillance under the claim that they are only temporary in nature would force legislatures to consider the long-term impact of provisions beyond the immediate terrorist threat.

I. SURVEILLANCE AND THE LAW IN THE UNITED STATES

In 1920, Frank Cobb, the editor of *New York World* wrote, "[t]he Bill of Rights is a born rebel. It reeks with sedition. In every clause it shakes its fist in the face of constituted authority. . . . [I]t is the one guarantee of human freedom to the American people."[7] Cobb had a point: the first of all the amendments puts a bullet in the heart of British licensing practices and the legacy of the Star Chamber, claiming the right to freedom of speech, assembly, and religion. The Fourth Amendment assured, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[8] This provision flew in the face of British writs of assistance, which had been used against the colonists with reckless abandon.[9] But rebellion did not stop there. The Fifth Amendment made a rude gesture towards state agencies that might contemplate torture, demanding that no person "be compelled in any criminal case to be a witness against himself."[10] And due process, in the same clause, provided a bulwark against state violations of individual rights.[11]

While notable in their attempt to limit state power, in none of these measures did the Bill of Rights, on its face, create a general right to privacy. Instead, the Supreme Court considered specific interests to fall under the remit of the Fourth Amendment. "Papers" included letters sent via post.[12]

---

[7] Frank Cobb, La Follette's Magazine (1920), http://www.zaadz.com/quotes/Frank_I_Cobb (last visited June 9, 2006).

[8] U.S. CONST. amend. IV.

[9] The American Revolutionist James Otis declared such writs, "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book." Boyd v. United States, 116 U.S. 616, 625 (1886) (quoting THOMAS COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 368 (The Lawbook Exchange, Ltd. ed., 1998) (1883)). According to Otis, such writs placed "the liberty of every man in the hands of every petty officer." *Id.* John Adams later declared Otis's statement to be the "first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born." *Id.*

[10] U.S. CONST. amend. V; *see also Boyd*, 116 U.S. at 629.

[11] U.S. CONST. amend. V.

[12] Accordingly, the 1792 Postal Act forbade postal employees from opening mail, unless they could not be delivered. Postal Act, Feb. 20, 1792. By 1878, the Supreme Court recognized,

> [l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be.

Ex parte Jackson, 96 U.S. 727, 733 (1878).

The only way to reach them would thus be by a warrant, "issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household."[13] Similarly narrow analysis held for "persons" and "effects." Over time, however, the Judiciary expanded its reading of the Constitution to include a more general right to privacy.

Part I briefly presents the development of this right in relation to state surveillance. What emerges is a story marked by the expansion of executive power as a way to address national security threats, followed by efforts by the Judiciary and Legislature to check the third branch. Post-9/11 augmentations, however, present something different in kind: even as counterterrorism has lowered the protections citizens have against unwarranted state surveillance, new technologies have catapulted state power into an entirely new realm. We have yet to grapple with what the loss of anonymity and movement into psychological surveillance means for the liberal, democratic nature of the state.

A. REASONABLE EXPECTATION OF PRIVACY

Fourth Amendment jurisprudence is well-trodden territory. While it is not the intent of this paper to analyze the central cases, a brief exposition will help to calibrate deviations from ordinary criminal law, which have been introduced to address terrorist crime.

More than a century ago, the Supreme Court ruled that papers and effects obtained unconstitutionally could not be admitted as evidence in a court of law.[14] In 1914, the Supreme Court expanded this "exclusionary rule" to deter law enforcement from violating the Constitution, to prevent the courts from being accomplices, and to increase public trust in the state.[15]

---

[13] *Jackson*, 96 U.S. at 733.

[14] Weeks v. United States, 232 U.S. 383 (1914); *Boyd*, 116 U.S. at 616.

[15] *Weeks*, 232 U.S. 383. Government officers, without a warrant, broke into Weeks's home and seized "all of his books, letters, money, papers, notes, evidences of indebtedness, stock, certificates, insurance policies, deeds, abstracts, and other muniments of title, bonds, candies, clothes, and other property." *Id.* at 387. Justice Day, writing for the Court, admonished,

> [t]he effect of the Fourth Amendment is to put the courts of the United States and Federal officials, in the exercise of their power and authority, under limitations and restraints as to the exercise of such power and authority, and to forever secure the people, their persons, houses, papers, and effects, against all unreasonable searches and seizures under the guise of law. This protection reaches all alike, whether accused of crime or not.

Id. at 391-92. To allow evidence taken in violation of the Fourth Amendment would, in effect, put the judiciary in the position of endorsing unconstitutional behavior. *Id.* at 394; *see also* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE 107-08 (4th ed. 2004).

In the late 19th century, Thomas Cooley began to expand the argument to a right to privacy writ large for criminal law investigations.[16] At the core of such privacy lay the "right to be let alone."[17] Two years later in the *Harvard Law Review*, Louis O. Brandeis and Samuel D. Warren called for greater protection of individual privacy.[18] It took more than a decade, however, for American courts formally to address the right to privacy.

The first shot across the bow came in 1904. New England Life Insurance Company published an advertisement in the *Atlanta Constitution* which featured two pictures: text under the first man, Paolo Pavesich, expressed his delight at buying life insurance. Text under the second photo, of a wretched-looking chap, bemoaned his lack of foresight in purchasing the same.[19] In deciding for Pavesich, who had actually never bought life insurance from the company, the Georgia Supreme Court suggested that the right to privacy derived from natural law and could be ascertained from authoritative legal texts.[20] Until consciously waived, the right to privacy remained.[21]

Just over two decades later, the Supreme Court addressed whether the Bill of Rights implied a right to privacy for criminal law investigations, but the case swam upstream against Prohibition and the moral majority. A multi-million dollar operation in Seattle imported and distributed alcohol throughout the country. For months, federal law enforcement officers tapped the phone lines of people involved in the operation.[22] The evidence implicated everyone from Roy Olmstead, the "leading conspirator" (general manager), to the Seattle police, who received kickbacks in return for turning

---

[16] "[I]t is better sometimes that crime should go unpunished than that the citizen should be liable to have his premises invaded, his desks broken open, his private books, letters, and papers exposed to prying curiosity, and to the misconstructions of ignorant and suspicious persons." ALAN WESTIN, PRIVACY AND FREEDOM 332 (1967) (citing COOLEY, *supra* note 9).

[17] DAVID FELDMAN, CIVIL LIBERTIES AND HUMAN RIGHTS IN ENGLAND AND WALES 516 (2002) (citing COOLEY, *supra* note 9, at 29).

[18] "The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influences of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual." Samuel D. Warren & Louis O. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890). With the Bill of Rights apparently silent on the issue, the authors found the locus for this right in common law, which included protections of privacy in relation to nuisance, and doctrines of relevance and necessity in the discovery phase of trial proceedings. *See* Prince Albert v. Strange, (1849) 64 Eng. Rep. 293 (Ch.); WESTIN, *supra* note 16.

[19] Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68 (Ga. 1905).

[20] *Id.*

[21] *Id.*

[22] Olmstead v. United States, 277 U.S. 438 (1928).

a blind eye. The majority found that because the information had been obtained via auditory means, and no entry of the defendant's house or offices had occurred, the state had not conducted a search. This placed phone taps outside constitutional protection.[23]

Brandeis, who by now had secured a place on the Court, wrote a scathing dissent, in which he claimed that privacy lay implicit in the Fourth Amendment. This measure, moreover, must be adapted to evolving technologies because "'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government."[24] By the turn of the century, the telephone had become an integral part of the fabric of society.[25] It differed from the post in terms of the "evil incident to invasion" of privacy: "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and *all* conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard."[26] In comparison, writs of assistance served as "but puny instruments of tyranny and oppression . . . ."[27] Brandeis went on to reiterate his ideas from the earlier article, penning one of the most famous passages in American constitutional law:

> The makers of our Constitution. . . . [C]onferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[28]

If the legislature wanted to change the law, and make an effort to protect telephone conversations from being intercepted without a warrant, it could. After a series of bills that failed to pass congressional muster, the 1934 Communications Act made the interception of communications and wiretap evidence inadmissible in a federal criminal trial.[29]

---

[23] *Id.* at 464-65.

[24] *Id.* at 472 (Brandeis, J., dissenting).

[25] About.com, Privateline.com Home Page: Welcome!, http://inventors.about.com/?once=true&site=http://www.privateline.com/ (last visited June 9, 2006).

[26] *Olmstead*, 277 U.S. at 475-76 (Brandeis, J., dissenting) (emphasis added).

[27] *Id.* at 476 (Brandeis, J., dissenting).

[28] *Id.* at 478-79 (Brandeis, J., dissenting).

[29] Federal Communications Act of 1934, Pub. L. No. 73-416, ch. 652, 48 Stat. 1064, 1103-04 (1934) (codified as amended at 47 U.S.C. § 605 (2000)).

Critically, for our present purposes, this legislation underestimated the strength of the national security claim—an incessant refrain that, despite being subject to occasional judicial setbacks, accompanied the steady expansion in surveillance through the turn of the 21st century. The 1934 Act became the first of a series of legislative casualties. For although, "[t]aken at face value the phrase 'no person' comprehends federal agents, and the ban on communication to 'any person' bars testimony to the content of an intercepted message," the FBI, concerned about the communist threat, crafted its own understanding of the statute and continued to wiretap.[30] It interpreted the legislation as requiring *both* the interception and disclosure of information in order for the statute to be violated; and it determined that communication within the Executive, a unitary branch, did not count as "divulging" information.[31]

The Bureau's somewhat creative interpretation forced the court to revisit the issue in the late 1930s. This time, the justices overturned *Olmstead* and declared that federal officials did *not* operate above the law.[32] Moreover, because the evidence excluded from trial reflected congressional concern that the inclusion of such information would be "inconsistent with ethical standards and destructive of personal liberty,"[33] any indirect use would also be barred.[34]

In early 1940, Attorney General Jackson responded to the decision by reinstating the general ban on wiretapping. But within months President Roosevelt overturned Jackson's policy. A May 21, 1940 memorandum indicated that "in the President's view the Supreme Court did not intend to have its decision apply to grave matters involving the defense of the nation."[35] He directed the Bureau to return to its wiretap operations for national security. In 1946, Truman affirmed the use of wiretaps for all cases "vitally affecting" the same.[36]

---

[30] LAFAVE ET AL., *supra* note 15, at 328-29.

[31] Socialist Workers Party v. Attorney Gen., 642 F. Supp. 1357, 1390 (S.D.N.Y. 1986).

[32] Nardone v. United States, 308 U.S. 338 (1939); Nardone v. United States, 302 U.S. 379, 380 (1937).

[33] *Nardone*, 302 U.S. at 383.

[34] *Nardone*, 308 U.S. at 340-41 (quoting Gouled v. United States, 255 U.S. 298, 307 (1921)).

[35] *Socialist Workers Party*, 642 F. Supp. at 1390.

[36] *Id*. Before going further, it is important to distinguish between wiretapping and bugging: the former centers on the interception of electronic communications, whereas the latter involves placing a microphone or recording device at a specific location to pick up in-person conversations. While the Court applied the Communications Act to limit wiretapping, it considered electronic bugs to fall outside legislative intent. In 1942, for instance, the Court found the warrantless use of a detectaphone—a sort of stethoscope that

The next three decades steadily narrowed the circumstances under which wiretapping for criminal law purposes would be allowed. Two important cases reached the Supreme Court: in the first, *Silverman v. United States*, Washington, D.C. police used a "spike mike" to monitor a gambling ring meeting in a row house next door. The foot-long microphone, inserted under a baseboard and into the wall, hit some sort of solid object that served as "a very good sounding board."[37] The Court found the physical penetration of this device into the wall, and its contact with what appeared to be the heating duct, to constitute a search.[38]

The second case, argued three months later, arose from early 20th century counterterrorist efforts. And it spurred the Court to recognize the right to privacy as equal to other rights secured by due process. Over-zealous police officers, waving a paper they claimed was a warrant, broke into Miss Dollree Mapp's home.[39] She grabbed the "warrant" and hid it in her bosom; but the police retrieved it, placed her in manacles, and searched the premises. In a locked trunk in the basement they discovered material unconnected to communists and bomb-throwers—"lewd and lascivious books, pictures, and photographs"—ownership of which counted as a crime under Ohio law.[40] The Court held that the Fourth Amendment exclusionary rule for warrantless searches applied to states through the Fourteenth Amendment.[41]

These cases lent momentum to recognition of a broad, private realm. Then, just four years later, a case involving medical advice provided by a doctor to a husband and wife reached the highest court. Connecticut law made it illegal to provide information to anyone about contraceptive devices.[42] Justice Douglas, writing for the Court, stated, "[t]his law . . . operates directly on an intimate relation of husband and wife and their physician's role in one aspect of that relation."[43] Douglas noted that a

---

could be placed on partition walls to pick up sound waves on the other side—to be outside the scope of the statute. Goldman v. United States, 316 U.S. 129, 133 (1942).

[37] Silverman v. United States, 365 U.S. 505, 506 (1961).

[38] *Id.* at 509. Although *not* part of the holding of the court, another important aspect may have been the role the case played in bringing the justices face to face with emerging electronic technologies, such as parabolic microphones and sonic wave surveillance. In dicta, the Court referred to these and other "frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society." *Id.*

[39] Mapp v. Ohio, 367 U.S. 643, 643 (1961).

[40] *Id.*

[41] *Id.* at 655.

[42] Griswold v. Connecticut, 381 U.S. 479, 480 (1965) (citing CONN. GEN. STAT. §§ 53-32, 54-196 (1958)).

[43] *Id.* at 482.

broader right to privacy existed as part of the First Amendment, such as the right of parents to choose their children's school, or the right to study German.[44] Other cases recognized "privacy in one's associations." Douglas continued, "[i]n other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion."[45] The Court came full circle and embraced Brandeis' view.[46]

By the mid-1960s then, Fourth Amendment jurisprudence, dominated by the "trespass doctrine," had begun to take form. To be unconstitutional, actual, physical penetration of a constitutionally protected *area* had to occur. "'[P]ersons,' [included] the bodies and attire of individuals; 'houses,' [included] apartments, hotel rooms, garages, business offices, stores, and warehouses; 'papers,' such as letters; and 'effects,' such as automobiles."[47] Whether wiretapping and electronic bugging for criminal law purposes, however, constituted a physical search remained far from settled.

In 1967, the Court revisited whether electronic bugging constituted physical trespass. By then, the telephone had completely integrated itself into daily American life. (In 1970, more than sixty-nine million main telephone lines were in use.) Charles Katz, a small-time gambler, used a public phone down the street from his boarding house to place bets. The FBI attached an electronic bug to the outside of the phone booth and recorded his calls to bookkeepers in Miami and Boston.

In a seismic shift, the Supreme Court issued a new edict: "[T]he Fourth Amendment protects people, not places." Justice Stewart, writing for the majority, continued, "[w]hat a person knowingly exposes to the public,

---

[44] *See* Pierce v. Soc'y of Sisters, 268 U.S. 510 (1925) (schooling); Meyer v. Nebraska, 262 U.S. 390 (1923) (German language); *see also Griswold*, 381 U.S. at 481-82.

[45] *Griswold*, 381 U.S. at 483 (citing NAACP v. Alabama, 357 U.S. 449, 462 (1958)).

[46] *Id.* at 494 (Goldberg, J., concurring).

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.

Id. (quoting Olmstead v. United States, 277 U.S. 438, 478 (Brandeis, J. dissenting)).

[47] LAFAVE et al., *supra* note 15, at 127-28 (citing See v. City of Seattle, 387 U.S. 541 (1967) (warehouses); Schmerber v. Calfiornia, 384 U.S. 757 (1966) (bodies); Beck v. Ohio, 379 U.S. 89 (1964) (attire); Clinton v. Virginia, 377 U.S. 158 (1964) (apartments); Stoner v. California, 376 U.S. 483 (1964) (hotel rooms); Preston v. United States, 376 U.S. 364 (1964) (automobiles); Taylor v. United States, 286 U.S. 1 (1932) (garages); United States v. Lefkowitz, 285 U.S. 452 (1932) (business offices); Amos v. United States, 255 U.S. 313 (1921) (stores); *Ex parte* Jackson, 96 U.S. 727 (1878) (letters)).

even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[48] Although the phone booth admittedly was constructed of glass, Katz shut the door.[49] The "presence or absence of a *physical* intrusion" suddenly mattered naught in consideration of the Fourth Amendment.[50]

The court thus replaced the "trespass doctrine" with one based on a "reasonable expectation of privacy." Justice Harlan concurred and refined the holding with a two-prong test to determine whether such an expectation exists: "[F]irst 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.'"[51] In this manner, neither conversations nor activities exposed to the "'plain view' of outsiders" would be considered protected.[52] Similarly, actions that took place in an open field, outside the curtilage of the home, would be fair game.[53]

Justice White in his concurrence, and particularly relevant to our current inquiry, emphasized that the presumption against warrantless searches could be overcome by pressing need. In a rather broad interpretation of footnote twenty-three, where the majority had written only that the case did not address the issue of national security, White suggested that the court had actually acknowledged, "that there are circumstance [sic] in which it is reasonable to search without a warrant."[54] White continued,

> [w]iretapping to protect the security of the Nation has been authorized by successive Presidents. . . . We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.[55]

---

[48] Katz v. United States, 389 U.S. 347, 351 (1967) (citation omitted).

[49] *Id.* at 352.

[50] *Id.* at 353 (emphasis added).

[51] *Id.* at 361 (Harlan, J., concurring). Many of the subsequent cases zeroed in on what was reasonable. *See, e.g.*, Chimel v. California, 395 U.S. 752 (1969) (holding that in the absence of a search warrant, police can only search the area within the arrestee's immediate control).

[52] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[53] The Court carved out an additional exception for hot pursuit. *See* Warden v. Hayden, 387 U.S. 294 (1967).

[54] *Katz*, 389 U.S. at 358. The text of footnote twenty-three reads, "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Id.*

[55] *Id.* at 363-64 (White, J., concurring).

Justice Douglas, joined by Justice Brennan, objected to White's assertion. He pointed out a certain conflict of interest: "Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be."[56] The constitutional responsibility of the Executive is to "vigorously investigate and prevent breaches of national security and prosecute those who violate pertinent federal laws."[57] Douglas concluded,

> [s]ince spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.[58]

The national security issue proved a contentious one, and a sort of de facto double standard evolved. According to the Court, physical surveillance and electronic bugging became subject to a "reasonable expectation of privacy" test. But wiretapping, and surveillance where "national security" might be involved found themselves on a different side of the legal ledger—a side where much looser considerations would satisfy the demands of Article II.

B. NATIONAL SECURITY AND SURVEILLANCE

Prior to the 20th century, the use of surveillance for national security reasons appears to have been limited to times of actual war. In 1776, for instance, the Committee (later Commission) for Detecting and Defeating Conspiracies collected information on suspected spies and sympathizers for the British government.[59] The Continental Congress regularly intercepted and opened mail sent by Tories.[60] The Sons of Liberty themselves evolved into the "mechanics," gathering intelligence for the revolutionists. The drafting of the Constitution halted many of these efforts, and by the start of the Civil War, intelligence-gathering efforts had so stagnated that neither the North nor the South had organized or reliable information on subversives.[61] In 1865, Secretary of State William H. Seward attempted to

---

[56] *Id.* at 359 (Douglas, J., concurring).

[57] *Id.* at 359-60 (Douglas, J., concurring).

[58] *Id.* at 360 (Douglas, J., concurring).

[59] *See* NAT'L COUNTERINTELLIGENCE CTR., A COUNTERINTELLIGENCE READER: AMERICAN REVOLUTION TO POST-WORLD WAR II 2 (Frank J. Rafalko ed., 2004), *available at* http://www.fas.org/irp/ops/ci/docs/ci1/ch1a.htm.

[60] *Id.*

[61] NAT'L COUNTERINTELLIGENCE CTR., *supra* note 59, at 43, *available at*

rectify the matter. He detained scores of individuals and created the Secret Service—a surveillance network that operated across the United States and Canada.[62] Just four months before the end of the war, the Confederacy established a Secret Service Bureau. The extent of its activities, however, remains lost to history; Seward's counterpart, Judah Benjamin, burned all the records.[63] Like the Revolutionary War, the end of the Civil War brought with it a lapse in information-gathering operations within the United States. As the 20th century dawned, however, the Red Scare, and the fear that anarchists, communists, and Bolsheviks lurked in every shadow, heralded the peace-time use of surveillance for national security purposes.

1. The Red Scare

The story of the expansion of domestic intelligence gathering powers for national security purposes is one marked by periodic efforts by Congress and the Judiciary to block executive expansion, followed by determined efforts by the Executive to continue on its path. Even the beginning of the Red Scare echoes this refrain: in May 1908, Congress barred the Department of Justice ("DOJ") from employing the Secret Service in an intelligence-gathering function. Two months later, Attorney General Charles Bonaparte created Special Agents to conduct investigations. The following year Attorney General George Wickersham formalized the decision in the creation of the Bureau of Investigation ("BI").[64] Over the next decade, large scale acts of violence—some engineered by anarchists, others by ordinary criminals—increased.[65] Attorney General A. Mitchell Palmer took the lead. With J. Edgar Hoover's assistance, he initiated a series of purges, arresting and deporting

---

http://www.fas.org/irp/ops/ci/docs/ci1/ch2a.htm.

[62] *See id.* (citing FREDERICK BANCROFT, THE LIFE OF WILLIAM H. SEWARD 260 (1990)).

[63] *Id.*

[64] History of the FBI: Origins 1908-1910, http://www.fbi.gov/libref/historic/history/origins.htm (last visited June 9, 2006). The BI did not become known as the Federal Bureau of Investigation until 1932. History of the FBI: The New Deal 1933-Late 30s, http://www.fbi.gov/libref/historic/history/newdeal.htm (last visited June 9, 2006).

[65] On May Day 1919, for instance, thirty-six bombs entered the postal system, addressed to prominent Americans. A month later, one found its way to then Attorney General A. Mitchell Palmer's home. In 1920, a wagon bomb exploded in lower Manhattan, killing over thirty people and injuring hundreds more. The attack caused some two million dollars in damage. House of Morgan Bombed, http://pbskids.org/bigapplehistory/business/topic15.html (last visited June 9, 2006).

thousands of "undesirable aliens." In one day alone, the feds rounded up some 4,000 people in 33 cities.[66]

Palmer's zealotry could hardly be overstated. In 1920 he wrote an article in *Forum* making *The Case Against the "Reds"*:

> Like a prairie-fire, the blaze of revolution was sweeping over every American institution of law and order a year ago. It was eating its way into the homes of the American workmen, its sharp tongues of revolutionary heat were licking the altars of the churches, leaping into the belfry of the school bell, crawling into the sacred corners of American homes, seeking to replace marriage vows with libertine laws, burning up the foundations of society.[67]

Palmer castigated Congress for failing to act.

Having mistaken the ends of the anarchist movement for the start of an American Revolution, however, Palmer soon found himself the butt of jokes and popular disdain. Experts later put the estimated number of Communist Party USA members at the time at some 26,000—a drop in the bucket of the more than 106 million people who lived in the United States—hardly a blaze of revolution "burning up the foundations of society."[68] Nevertheless, the extraordinary use of executive power during peace time set a precedent—one not lost on Hoover.

The Justice Department came off the Palmer raids with a less than pristine reputation. In 1924, Harlan Fiske Stone replaced Palmer as Attorney General. Determined to clamp down on domestic intelligence gathering, Stone demanded the BI Director's resignation, initiated an immediate review of all people working at the agency, and insisted that only "men of known good character and ability"—and preferably legal training—be given positions.[69] He appointed Hoover as the new BI Director. The Bureau, however, retained the extensive dossiers it had built up from 1916 to 1924. Under pressure from the highest levels of the executive branch, the policy soon was reversed, allowing the FBI to continue wiretapping for national security reasons.[70]

---

[66] ROBERT K. MURRAY, RED SCARE: A STUDY IN NATIONAL HYSTERIA, 1919-1920, at 213 (Greenwood Press 1980) (1955).

[67] A. Mitchell Palmer, *The Case Against the "Reds,"* 63 FORUM 173, 174 (1920), *available at* http://chnm.gmu.edu/courses/hist409/palmer.html.

[68] THEODORE DRAPER, THE ROOTS OF AMERICAN COMMUNISM 189 (1957) (CPUSA membership numbers). Population figure reflects U.S. Official Census Estimate for 1920, http://www.tsl.state.tx.us/ref/abouttx/census.html (last visited June 9, 2006).

[69] Memorandum from Harlan Fiske Stone, Attorney Gen., Dep't of Justice, to J. Edgar Hoover, Dir., Fed. Bureau of Investigation (May 13, 1924), *cited in* NAT'L COUNTERINTELLIGENCE CTR., *supra* note 59, at 157, *available at* http://www.fas.org/irp/ops/ci/docs/ci1/chap4.pdf.

[70] In 1930, the Treasury Department's Bureau of Prohibition ("BP") merged with the BI.

On August 24, 1936, President Roosevelt met with Hoover to discuss "the question of the subversive activities in the United States, particularly fascism and communism."[71] He wanted the Bureau to provide him with "a broad picture of the general movement and its activities as may affect the economic and political life of the country as a whole." Hoover sent a letter to all field offices ordering them "to obtain from all possible sources information concerning subversive activities being conducted in the United States by Communists, Fascists, representatives or advocates of other organizations or groups advocating the overthrow or replacement of the Government of the United States by illegal methods."[72] He established a procedure that provided for the systematic collection and reporting of information. Hoover emphasized the importance of secrecy, "in order to avoid criticism or objections which might be raised to such an expansion by either ill-informed persons or individuals having some ulterior motive." Wary of the legislative branch, he continued, "[c]onsequently, it would seem undesirable to seek any special legislation which would draw attention to the fact that it was proposed to develop a special counter-espionage drive of any great magnitude."[73]

Field offices, carefully shielding the Bureau's surveillance program from public scrutiny, obtained data from "public and private records, confidential sources of information, newspaper morgues, public libraries, employment records, school records, et cetera."[74] Some information related to entirely lawful (and constitutionally-protected) activities. Child care centers, political re-election campaigns, Christian organizations, and the National Association for Advancement of Colored People ("NAACP") all merited attention.[75]

Although the BI at the time had halted its wiretapping, BP, which frequently intercepted electronic communications, continued to do so after the merger. The BI then changed its policy to bring the rest of the bureau into line with BP practices. Socialist Workers Party v. Attorney Gen., 642 F. Supp. 1357, 1390 (1986).

[71] *Socialist Workers Party*, 642 F. Supp. at 1375-76 (citing Memorandum from J. Edgar Hoover, Dir., Fed. Bureau of Investigation, to all FBI field offices (Aug. 24, 1936)).

[72] NAT'L COUNTERINTELLIGENCE CTR., *supra* note 59, at 161, *available at* http://www.fas.org/irp/ops/ci/docs/ci1/chap4.pdf (citing Memorandum from J. Edgar Hoover, Dir., Fed. Bureau of Investigation, to all FBI field offices (Sept. 5, 1936)).

[73] *Id.* (citing Memorandum from J. Edgar Hoover, Dir., Fed. Bureau of Investigation, enclosed with letter from Cummings to the President (Oct. 20, 1938)).

[74] *Id.* at 179, *available at* http://www.fas.org/irp/ops/ci/docs/ci1/chap4.pdf (citing Memorandum from J. Edgar Hoover, Dir., Fed. Bureau of Investigation, to all field offices (Dec. 6, 1939)).

[75] *See generally id.* at 180-81, *available at* http://www.fas.org/irp/ops/ci/docs/ci1/chap4.pdf.

As the Iron Curtain descended, Congress renewed its debate on the use of wiretaps. But communist fever had swept the U.S. By 1945, the Dias Committee, formed to look into subversive elements within the United States, had turned into a permanent standing Committee on Un-American Activities. And so bills attempting to regulate electronic wiretaps met with little success. When a prominent espionage case burst onto the national scene, Hoover's tactics appeared warranted. The case also brought into sharp relief the disparity between the requirements of criminal law surveillance and national security claims. Efforts by the Judiciary, however, to reign in the Executive met with little practical effect.

Judith Coplon, the defendant in the case, embraced all things Soviet.[76] Upon graduation from Barnard College, she took a position with the Justice Department. DOJ quickly promoted her to the foreign agent registration department, where she had access to FBI reports on suspected subversives. Coplon began funneling the Bureau reports to the KGB. Her reports demonstrated uncanny insight into the Soviet Union. Hoover became suspicious and placed her under surveillance. The FBI arrested her with classified materials in her handbag and charged her with treason.

Coplon's trial attracted national attention. Few bought her story on the stand: that Valentin Gubitchev, her KGB handler, had seduced her, while she, innocent in the ways of the world, fell victim to his attentions. The presence of classified documents she attributed to pressure from work and the need to catch up in the evenings. Sentenced to ten years, Coplon immediately flew to Manhattan for a second, joint conspiracy trial with Gubitchev. It quickly became clear that the FBI had conducted illegal wiretaps, and destroyed evidence, in violation of federal law. Although convicted and sentenced to fifteen years, the appeals court determined that the wiretap evidence against Coplon could not be admitted, and that her arrest without a warrant violated federal law. The court dismissed all charges.

On the one hand, the case underscored the presence of subversives. On the other hand, it exposed Hoover's surveillance to the eye of the courts. But such judicial oversight proved ineffective. The Bureau continued to wiretap.[77]

Once again, in the early 1950s, the conflict between personal privacy and the Red threat came to a head. Outrage at inroads into the former,

---

[76] The following account is drawn from MARCIA MITCHELL & THOMAS MITCHELL, THE SPY WHO SEDUCED AMERICA: LIES AND BETRAYAL IN THE HEAT OF THE COLD WAR—THE JUDITH COPLON STORY (2002); Judith Coplon: American Spy for Soviets, http://www.angelfire.com/oz/1spy/Coplon.html (last visited June 9, 2005).

[77] WESTIN, *supra* note 16, at 177.

expressed in the highest court in the land, however, fell on deaf ears. Justice Jackson wrote:

> Science has perfected amplifying and recording devices to become frightening instruments of surveillance and invasion of privacy, whether by the policeman, the blackmailer, or the busybody. That officers of the law would break and enter a home, secrete such a device, even in a bedroom, and listen to the conversation of the occupants for over a month would be almost incredible if it were not admitted.[78]

Herbert Brownell, who had become Attorney General in 1953, responded to Jackson's remarks with a memorandum to the Director of the FBI that again illustrated executive disregard for the Judiciary: "I recognize that for the FBI to fulfill its important intelligence function, considerations of internal security and the national safety are paramount and, therefore, may compel the unrestricted use of this technique in the national interest."[79] Brownell then went one step further, announcing that new "emergency anti-Communist" legislation would legalize electronic surveillance.[80] The House Judiciary Committee held hearings on the matter, and the following year the Eisenhower Administration presented its bill. The Republican leader of the House, Charles Halleck, threw the gauntlet—all "loyal" citizens would see the Administration's proposal as an "anti-traitor bill."[81]

2. Title III

Despite executive efforts to steamroll Congress, concern at the extent to which law-abiding citizens (read legislators) fell subject to executive branch surveillance spurred a series of hearings. The Moss Subcommittee and the Senate Judiciary Committee led the charge. Then in 1964, the Senate Subcommittee on Administrative Practices and Procedures, headed by Senator Edward V. Long, began hearings. As evidence emerged, outrage swept the nation, and (although the private sale of surveillance devices soared) a consensus emerged from radical left to hard right that some sort of control ought to be imposed.[82] President Johnson issued an unpublished memorandum, banning wiretapping; but, once again, he carved out an exception for national security.[83]

---

[78] Irvine v. California, 347 U.S. 128, 132 (1954).

[79] Socialist Workers Party v. Attorney Gen., 642 F. Supp. 1357, 1391 (1986).

[80] WESTIN, *supra* note 16, at 181.

[81] *Id.* at 182.

[82] *Id.* at 199-200.

[83] The Presidential memorandum, issued June 30, 1965, authorized wiretaps "in connection with investigations related to national security." *Socialist Workers Party*, 642 F. Supp. at 1391.

In 1967, the United States Supreme Court again weighed in on the issue. The Court struck down a New York surveillance statute on the grounds that it failed to include, *inter alia*, a requirement that the officer applying for the warrant believe that a particular offence had been or was about to be committed, or that the officer describe the property involved or conversations to be intercepted.[84]

Six months later, the Court again spoke, creating a reasonable expectation of privacy.[85] The Executive jumped on the bandwagon, giving lip service to the Court's concern. But once again, it retained for itself the very exception that had led to such widespread use of wiretaps: national security. President Johnson announced in his 1967 State of the Union address:

> We should protect what Justice Brandeis called the 'right most valued by civilized men'—the right of privacy. We should outlaw all wire-tapping—public and private—wherever and whenever it occurs, *except when the security of the nation is at stake*—and only then with the strictest safeguards. We should exercise the full reach of our Constitutional powers to outlaw electronic "bugging" and "snooping."[86]

The following year Congress introduced Title III of the Omnibus Crime Control and Safe Streets Act.[87]

Title III, which went beyond the Supreme Court's decision, continues to govern the use of wiretaps for ordinary criminal law investigations. It created prior judicial authorization and established the circumstances under which an intercept order could be issued. The legislation required probable cause that a crime had been or was about to be committed. The communications to be intercepted had to be relevant to the particular offence. The officer applying for the warrant had to specify the person, location, description of communications, name of person requesting, and length of time, with a thirty day limit. Any extensions would be subject to earlier restrictions.[88] Title III limited wiretaps to twenty-six specified

---

[84] Berger v. New York, 388 U.S. 41 (1967). The Court suggested that "roving" wiretaps would be unacceptable, that a warrant would have to be executed promptly, pursuant to a showing of probable cause and that the order would need to include a formal termination date so as not to leave the decision to the discretion of the officer. *Id.* at 59-60. The Court also suggested that exigent circumstances might be able to overcome the notice requirement. *Id.* at 60.

[85] Katz v. United States, 389 U.S. 347 (1967).

[86] President Lyndon Johnson, State of the Union Address (Jan. 10, 1967), *available at* http://www.janda.org/politxts/State%20of%20Union%20Addresses/1964-1969%20Johnson/LBJ67.html (emphasis added).

[87] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III § 802, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-20 (2000)).

[88] *Id.*; *see also* LAFAVE ET AL., *supra* note 15, at 333.

crimes: including, *inter alia*, murder, kidnapping, extortion, gambling, counterfeiting, and drugs—all, coincidentally, activities associated with terrorist organizations. Importantly, Title III made wiretaps harder to obtain than ordinary search warrants. The warrant had to indicate that normal investigative procedures would not suffice. Nevertheless, and relevant to our current discussion, Congress specifically excepted national security, leaving such investigations firmly in the executive domain.[89]

In a landmark decision handed down four years later, and another attempt by the Judiciary to reign in the executive branch, the Supreme Court held that Title III did not *authorize* the Executive to engage in electronic surveillance for national security purposes; rather, it simply reflected congressional neutrality.[90] This left the Court open to consider whether warrantless domestic wiretapping for national security fell within the constitutional remit of the Executive. The Court determined that it did not. While the duty of the state to protect itself had to be weighed against "the potential danger posed by unreasonable surveillance to individual privacy and free expression,"[91] such "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the executive branch."[92]

Justice Jackson, again writing for the Court, recognized that executive officers could hardly be regarded as neutral and disinterested: "Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. . . . [T]hose charged with this . . . duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[93] He highlighted the dangers: "[U]nreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[94] Domestic security surveillance thus did not fall under one of the exceptions to the warrant requirement under the Fourth Amendment.[95] Jackson rejected the government's suggestion that national security matters were "too subtle and complex for judicial evaluation."[96] Nor did he accept that "prior judicial approval will fracture the secrecy essential to official intelligence

---

[89] Omnibus Crime Control Act, § 802 (codified as amended at 18 U.S.C. § 2511(3)); *see also* PHILIPPA STRUM, PRIVACY: THE DEBATE IN THE US SINCE 1945 141-44 (1998).

[90] United States v. U. S. Dist. Court, 407 U.S. 297, 308 (1972).

[91] *Id.* at 314-15.

[92] *Id*. at 316-17.

[93] *Id*. at 317 (internal citation removed).

[94] *Id.*

[95] *Id.* at 320.

[96] *Id*.

gathering."[97] The former would suggest that such surveillance might not be warranted in the first place; the latter had long been an aspect of ordinary criminal activity.

Once again, the executive branch largely ignored this decision. Wiretapping of domestic individuals and organizations under the guise of national security continued. The Federal Bureau of Investigation, National Security Agency, Central Intelligence Agency, and Department of Defense all held their course. While much has been written about the executive excesses that occurred during this time, I briefly discuss a handful to underscore the breadth and depth of the abuses that occurred under the Executive's Article II claims.

3. Executive Excess

The salient point to be drawn from the excesses that principally occurred between 1945 and 1975 is that surveillance, conducted under the auspices of national security, became an instrument of political power. Each operation began as a limited inquiry and gradually extended to capture more information from a broader range of individuals and organizations. Each targeted American citizens. And each remained insulated, until the Church hearings, from congressional or judicial oversight.

a. NSA: Operation SHAMROCK and MINARET

Operation SHAMROCK began in World War II, when the military placed censors at RCA Global, ITT World Communications, and Western Union International. Keen to maintain the flow of intelligence at the close of the war, DOD told the companies to continue forwarding intercepts, assuring them that they would be exempt from criminal liability or public exposure as long as Truman remained in the White House. From 1949 until 1975 the project continued (from 1952 under the control of the National Security Agency) without the knowledge of subsequent Presidents. To keep the project under the radar, NSA deliberately refrained from formalizing the relationship in any sort of (traceable) document.[98] By the 1970s, from the magnetic tapes that recorded all telegraph traffic, the NSA was selecting approximately 150,000 messages per month for its analysts to read and circulate.

---

[97] *Id*.

[98] *See Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Agencies*, 94th Cong. Vol. 5 (1975) [hereinafter *Church Committee* Vol. 5].

Operation SHAMROCK put the government in the position of asking private industry to break the law, not execute it. The United States Code prohibited the interception or decryption of diplomatic codes or messages.[99] It also outlawed the transfer of information "concerning the communication intelligence activities of the United States or any foreign government" to unauthorized persons.[100] The law required the President to designate individuals engaged in communications intelligence activities. Yet from 1949 forward, no President was even aware that the companies and their executives surveilled all telegraphs entering, leaving, or circulating within the United States. The project also stands out in creating a political interest in the companies to guarantee that certain administrations remained in office, thus ensuring that criminal prosecution would not follow.

While Operation SHAMROCK represented a broad, information-gathering effort, NSA also undertook a project that placed particular "individuals or organizations involved in civil disturbances, anti-war movements, [or] demonstrations" under surveillance.[101] Project MINARET maintained a Top Secret classification, named agents only. The charter specified that although NSA instigated the project, it would not be identified with the operation.[102]

The evolution of this program demonstrates the tendency of surveillance operations to expand. Initially, NSA focused on American citizens traveling to and from Cuba. The agency expanded the list to individuals believed to threaten the President. The FBI added domestic and foreign entities, saying that they were "extremist persons and groups, individuals and groups active in civil disturbances, and terrorists."[103] The Bureau of Narcotics and Dangerous Drugs expanded the remit to include "the abuse of narcotics and dangerous drugs."[104] In 1971, the executive branch specifically requested that the NSA monitor international terrorism.[105] And so by 1971, the program extended to *all* criminal activity,

---

[99] An Act for the Protection of Government Records, ch. 57, 48 Stat. 122 (1933), (current version at 18 U.S.C. § 952 (2000))**.**

[100] An Act to Amend Certain Titles of the U.S. Code, Ch. 655, § 24(a), 65 Stat. 719 (1951) (codified as amended at 18 U.S.C. § 798).

[101] *Church Committee* Vol. 5, *supra* note 98, at 150 (Charter for Sensitive SIGINT Operation Minaret (C)).

[102] *Id.*

[103] *Id.* at 12 (emphasis added).

[104] *Id*. (Memorandum from the Bureau of Narcotics and Dangerous Drugs to Dir., Nat'l Sec. Agency Fort George G. Meade, Md., Request for COMINT of Interest to Bureau of Narcotics and Dangerous Drugs ("BNDD")).

[105] *Id.* at 14.

as well as foreign support for or basing of, subversive activity.[106] In October 1973, NSA terminated the program, having placed hundreds of thousands of Americans engaged in constitutionally-protected political protest under surveillance.[107]

What makes this vast, expensive machinery of particular note is that it appears to have been relatively ineffective. When pressed repeatedly whether acts of terror in fact had been prevented, General Allen testified in Congress that only one event had been so disrupted.[108] Moreover, rather than information coming bottom-up (*from* the surveillance being conducted *to* concluding what threats faced the state), considerable pressure ran top-down to find *something* linking foreign organizations to civil disturbances.[109] Such pressure became a refrain played through many major intelligence gathering operations.

b. FBI: COINTELPRO and the Security Index/ADEX

NSA was not the only federal agency conducting surveillance. Without either the President or Attorney General's knowledge, Hoover's Federal Bureau of Investigation ran an operation code-named COINTELPRO.[110] From 1936 through 1976, the FBI disrupted domestic organizations.[111] In autumn 1956, Hoover approved COINTELPRO-CPUSA, under which the Bureau conducted more than 1,300 operations.[112] Six years later, FBI Headquarters initiated COINTELPRO-SWP, which

---

[106] *Id.* at 156 (Memorandum from Noel Gayler, Vice Admiral, U.S. Navy, Nat'l Security Agency Director, to Sec'y of Defense and Attorney Gen. (Oct. 1, 1973)).

[107] *Id.*

[108] *Id.* at 12-13.

[109] *Id.*

> In the area[] of . . . terrorism . . . the emphasis placed by the President on a strong, coordinated Government effort was clearly understood. There also was no question that there was considerable Presidential concern and interest in determining the existence and extent of foreign support to groups fomenting civil disturbances in the United States.

Id. at 13 (statement of General Allen).

[110] *See Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Agencies*, 94th Cong. (1975); *Supplementary Detailed Staff Reports of the Intelligence Activities and the Rights of Americans: Book III, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. (1976) [hereinafter *Final Report*]; *see also* COINTELPRO: THE FBI'S SECRET WAR ON POLITICAL FREEDOM (Cathy Perkus ed., 1975).

[111] Socialist Workers Party v. Attorney Gen., 642 F. Supp. 1357, 1376, 1384, 1396 (S.D.N.Y. 1986).

[112] *Id.* at 1384-85.

carried out 46 operations.[113] And in 1968, COINTELPRO-New Left began, introducing a further 285 operations.[114]

These programs involved a wide range of activities aimed at left-leaning organizations and the anti-war movement: the FBI provided leaders' past criminal records and "derogatory material regarding . . . marital status" to the media; it sent anonymous letters to exacerbate racial tension; and, it made false claims about members of the organizations.[115] The Bureau distributed fake newspapers on campuses. It contacted the Better Business Bureau in New York City with untrue allegations to interrupt organizations' fundraising efforts.[116] The FBI "caused antiwar activists to be evicted from their homes; disabled their cars; intercepted their mail; wiretapped and bugged their conversations . . . prevented them from renting facilities for meetings; incited police to harass them for minor offenses; sabotaged and disrupted peaceful demonstrations; and instigated physical assaults against them."[117] The FBI conducted interrogations to "enhance the paranoia in [Leftist] circles and . . . to get the point across there is an FBI agent behind every mailbox."[118] The organization extended its interviews to the workplace, where it questioned supervisors, as well as religious organizations and neighborhoods.

These disruptive actions complemented general surveillance of groups considered a threat to the state. As with Operations SHAMROCK and MINARET, the number of people targeted gradually expanded. Initially the FBI focused on just CPUSA. The list soon grew to include the Socialist Workers Party. In 1964, the Bureau added the KKK and other Aryan organizations. By 1965, the civil rights movement had become a focus, with leading figures such as Martin Luther King, and organizations such as the NAACP coming within the Bureau's remit. In the late 1960s, the FBI further extended its list to include "Black Nationalist" groups, such as the Southern Christian Leadership Council, the Student Nonviolent Coordinating Committee ("SNCC"), and the Nation of Islam.[119] Prominent

---

[113] *Id.*

[114] *Id.* at 1384.

[115] *Id.* at 1385-88.

[116] *Id.* at 1388.

[117] GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 490 (2004).

[118] *Socialist Workers Party*, 642 F. Supp. at 1389.

[119] The Southern Christian Leadership Council was founded in 1957 and led by Martin Luther King. In 1960, the Student Nonviolent Coordinating Committee formed and began focusing on non-violent actions, particularly in the south, to protest white domination. *See* Clayborne Carson, *Civil Rights Movement*, http://liberationcommunity.stanford.edu/clayarticles/enc_of_am_const.htm (last visited June 9, 2006). Clayborne Carson, *Civil*

leaders—H. Rap Brown (a member of the SNCC and later member of the Black Panthers), Elijah Muhammad (a member of the Nation of Islam), and Malcolm X (a member of the Nation of Islam until his 1964 founding of the Organization of Afro-American Unity)—came under twenty-four/seven observation. The FBI also became suspicious of all "dissident" parties within the Democratic block, such as Students for a Democratic Society (SDS).[120] Although, after an extensive investigation, the Bureau concluded that the Communist Party was not behind the anti-war movement, the FBI continued to attend and record teach-ins and anti-war rallies.[121]

Successive presidential directives provided general authority for the FBI to conduct investigations into espionage and sabotage. However, the manner in which the Bureau carried out such investigations involved outright violations of American law. The Socialist Workers' Party ("SWP"), which first came under Hoover's eye in 1940, provides a salient example.

The SWP based its political aims on the writings of Karl Marx, V.I. Lenin and Leon Trotsky.[122] Article II of its constitution called for "the abolition of capitalism through the establishment of a Workers and Farmers Republic."[123] The organization sought what it considered a democratically elected government: a series of elected local councils which would then elect the central government. The organization supported the freedom to form political parties. It also advocated "basic individual rights and freedoms such as freedom of speech and religion and due process of law."[124] This put the organization at odds with Trotskyist and Marxist organizations in the Soviet Union, which the SWP faulted for adopting a totalitarian regime. While the organization embraced the current electoral process as the mechanism for reform, the ultimate goal was to bring about a revolution, where the ruling classes would use violence, forcing those

---

Rights Movement, *in* ENCYCLOPEDIA OF THE AMERICAN CONSTITUTION 411-12 (Leonard W. Levy et al. eds. 2000). Nation of Islam was a black, religious organization, founded in 1930 and led by Elijah Muhammad. *See* Claude A. Clegg, *Message from the Wilderness of North America: Elijah Muhammad and the Nation of Islam, c. 1960*, 1 J. MULTIMEDIA HIST. 1 (1988), *available at* http://www.albany.edu/jmmh/vol1no1/elijahmuhammad.html.

[120] Tom Hayden founded SDS in 1959. It symbolized the break and creation of the "New Left." A Kent State protest led by the SDS gave rise to severe National Guard actions that further divided the country. After a number of splinter groups broke off from the organization, a power struggle for control emerged. By 1972, the organization ceased to operate. *See* Old American Red Groups, http://reds.linefeed.org/past.html (last visited June 9, 2006).

[121] *See* STONE, *supra* note 117, at 488.

[122] *Socialist Workers Party*, 642 F. Supp. at 1364.

[123] *Id.* at 1369.

[124] *Id.* at 1369-70.

subjected to take up arms in defense—essentially, a transformation of the state.

This goal, however, did not mean that the organization was engaged in violence. SWP leaders stated in court that terrorism contradicted their central philosophy, as "it distracts attention and efforts from the development of a mass movement, and also subjects the militants to police action and loss of life."[125] The SWP repeatedly criticized terrorist attacks, such as the 1972 Black September attack on Israeli Olympians, and the assassination of the Spanish Prime Minister two years later. It did not undertake violent actions. In more than thirty years of intense surveillance, not one prosecution of any member occurred. On the contrary, a considerable amount of evidence indicated that the organization spent extensive time discussing and debating Marxist economic and social theory, the war in Vietnam, the plight of agricultural workers in California, and the civil rights movement. As the district court noted, "[a]ll of the above are unquestionably lawful political activities, which a group such as the SWP has a clear constitutional right to carry out."[126]

For thirty-six years the Bureau kept the SWP under strict surveillance. In the process the FBI committed more than 204 burglaries. Agents broke into SWP and Young Socialist Alliance offices in New York, Newark, Chicago, Detroit, Boston, and Milwaukee, as well as members' homes in Detroit, Newark, Hamden (Connecticut), and Los Angeles.[127] "Black bag" jobs—the Bureau's short-hand for break-ins in which they stole or photocopied papers—yielded 9,864 documents.[128] These contained information that ranged from the group's activities, finances, and legal matters, to members' personal lives. These break-ins also allowed the FBI to hide surveillance devices. Between 1943 and 1963, agents conducted approximately 20,000 wiretap days and 12,000 electronic bug days on the SWP alone.[129] The FBI clearly knew that the break-ins violated the law. An internal memorandum dated July 19, 1966 noted:

> We do not obtain authorization for 'black bag' jobs from outside the Bureau. Such a technique involves trespass and is clearly illegal; therefore, it would be impossible to obtain any legal sanction for it. Despite this, 'black bag' jobs have been used because they represent an invaluable technique in combating subversive activities of a clandestine nature aimed directly at undermining and destroying our nation.[130]

---

[125] *Id.* at 1373.
[126] *Id.* at 1375.
[127] *Id.* at 1394.
[128] *Id.* at 1393.
[129] *Id.* at 1389.
[130] *Id.* at 1394.

In order to get past the legal issues, the FBI followed what it called a "Do Not File" procedure: the Special Agent in Charge prepared an informal record of all black bag operations, which he placed in his personal safe. Bureau Inspectors would then read the memorandum and destroy it.[131]

Outside of direct surveillance, the FBI ran approximately 1,300 informants, most of who were paid to gather additional information.[132] The Bureau obtained some 12,600 additional documents in this manner. These papers included membership lists, financial records, financial budgets and projections, minutes of meetings, mailing lists, and correspondence.[133] Informants further provided the Bureau with records on what occurred at the meetings, and personal information on the members and their families, such as "marital or cohabitational status, marital strife, health, travel plans, and personal habits."[134] In more than thirty years, out of 1,300 sources, and thousands of reports and documents, not a single informant reported any instance of "planned or actual espionage, violence, terrorism or [efforts] to subvert the governmental structure of the United States."[135] Nevertheless, the FBI paid SWP members to disrupt operations, directing them to discourage recruitment, lower dues, and diminish contribution levels.[136]

In 1973, the SWP filed suit against the Attorney General. Complicated by the DOJ's efforts to maintain strict secrecy under the claim of national security, the case took thirteen years to reach the Supreme Court. Much of the information about these programs has emerged in the years since. At the time they were being conducted, the public had no idea of their extent until the Citizens' Commission to Investigate the FBI (an anti-war group) broke into an FBI office and took roughly one thousand pages of confidential information.[137] In April 1971, Hoover announced the cessation of COINTELPRO. Despite this announcement, and the FBI's claim that it had terminated "domestic security" break-ins, such actions continued.[138]

---

[131] *Id.* at 1395. The Bureau also maintained a "JUNE mail" system, where documents were placed in a "Special File Room." *See* Athan G. Theoharis, *FBI Surveillance: Past and Present*, 69 CORNELL L. REV. 883, 888 (1984).

[132] Socialist Workers Party v. Attorney Gen., 444 U.S. 903, 903 (1979) (White, J., dissenting).

[133] *Socialist Workers Party*, 642 F. Supp. at 1382.

[134] *Id.* at 1379.

[135] *Id.* at 1380.

[136] *Id.* at 1382.

[137] STONE, *supra* note 117, at 494-95.

[138] Theoharis, *supra* note 131, at 884-85. In 1978, for example, criminal prosecutors indicted previous Acting FBI Director L. Patrick Gray, Acting FBI Associate Director W. Mark Felt, and FBI Assistant Director Edward Miller for authorizing burglaries during the Bureau's investigation of the Weather Underground. At the trial, memos encouraged the use

The Bureau complemented COINTELPRO with other programs. Starting in 1940, the FBI maintained a list of citizens for potential detention without trial. In 1943, Attorney General Francis Biddle, aware of the absence of any congressional authorization for the list, ordered its termination. Hoover, however, ignored the Attorney General and simply renamed the Custodial Detention List the "Security Index."[139] In 1949, the Attorney General and the Secretary of Defense agreed to an Emergency Detention Plan based on the directory. Although Congress specifically passed legislation in 1950 to govern the potential detention of American citizens at a time of national emergency,[140] the Attorney General told Hoover to ignore the new law. The FBI's list, which by then numbered some 19,577, went well beyond the limits established by Congress.[141] And it had important and very real consequences: every forty-five days the FBI interviewed the landlords and employers of every person on it.[142] This created social pressure on those suspected of disloyalty—not only an inroad into individual privacy, but an act with important implications for citizens' freedom of speech, movement and association. In 1971, the DOJ renamed the Security Index the "Administrative Index" ("ADEX"). It broadened the number of names on it to include anyone involved in civil disturbances. The Church Hearings in 1976 uncovered the existence of ADEX, prompting the FBI to discontinue it.

c. CIA: Operation CHAOS

Like the NSA and the FBI, the CIA also ran a domestic counterintelligence project, code-named Operation CHAOS. It grew from pressure placed by the Johnson and Nixon Administrations to find a link between the anti-war movement and overseas actors.[143] Although the CIA issued four formal reports to Johnson and one to Nixon, denying any connection, political pressure to find ties between domestic and foreign entities continued.[144] In the process of gathering data, the CIA placed more than 300,000 American citizens under surveillance.[145] An average of one

---

of "innovative techniques"—a euphemism, the government admitted, which meant break-ins. *Id.* at 884-85.

[139] *Final Report*, *supra* note 110. When Truman took office, the FBI told the new Attorney General, Tom Clarke, about the file. He offered no objection. *Socialist Workers Party*, 642 F. Supp. at 1395.

[140] Emergency Detention Act, 50 U.S.C. tit. II §§ 811-26 (2000).

[141] *Socialist Workers Party*, 642 F. Supp. at 1395.

[142] *Id.* at 1395.

[143] *Church Committee* Vol. 5, *supra* note 98; *see also* STONE, *supra* note 117, at 488.

[144] STONE, *supra* note 117, at 490-91.

[145] THE ROCKEFELLER COMM'N, REPORT TO THE PRESIDENT BY THE COMMISSION ON CIA

thousand individual reports per month flowed from the CIA to the FBI. The CIA also shared specific information with the White House. Like the FBI with respect to "black bag" jobs, the Agency was entirely aware that its actions pushed legal bounds. In the midst of the operation, Director of Central Intelligence Richard Helms wrote to the White House, "this is an area not within the charter of this Agency, so I need not emphasize how extremely sensitive this makes the paper."[146] Nevertheless, the Attorney General consistently claimed that, under his Article II authority, the President had the power to authorize electronic surveillance of U.S. citizens without court order.[147] Efforts to challenge Operation CHAOS in court hit a brick wall: because the information had been classified at the highest level, claimants could not gain access to demonstrate that particular individuals had been targeted.[148]

CHAOS was only one of a variety of surveillance programs run by the CIA at that time. For example, in 1967, Project MERRIMAC, aimed at protecting CIA employees and facilities against anti-war protestors, infiltrated and monitored a number of anti-war organizations, such as SDS and the Women's Strike for Peace. The same year Project RESISTANCE began to compile information on radical organizations in the United States, bringing more than 12,000 individuals, mostly students, under surveillance.[149]

d. DOD: Operation CONUS

The military, for its part, also conducted surveillance. Operation CONUS maintained files on more than 100,000 political activists and orchestrated data exchange between some 350 military posts. The list of targets included Senators Adlai Stevenson, III, J. William Fulbright, and Eugene McCarthy, Congressman Abner Mikva, singer Joan Baez, and civil rights leader Martin Luther King, as well as civil liberties organizations,

---

ACTIVITIES WITHIN THE UNITED STATES (1975).

[146] STONE, *supra* note 117, at 493.

[147] The government claimed, e.g., that:

> [A]ny President who takes seriously his oath to 'preserve and protect' and defend the constitution will no doubt determine that it is not unreasonable to utilize electronic surveillance to gather intelligence information concerning those organizations which are committed to the use of illegal methods to bring about changes in our form of government and which may be seeking to foment violent disorders.

JASON EPSTEIN, GREAT CONSPIRACY TRIAL 111-12 (1970). Epstein goes on to paraphrase the government's claim that where national security is at stake, it is the Executive, not the Judiciary, which interprets the law. *Id.*

[148] *See, e.g.*, Halkin v. Helms, 690 F.2d 977 (D.C. Cir. 1982).

[149] STONE, *supra* note 117, at 491.

such as the ACLU, Americans for Democratic Action, the NAACP, the American Friends Service Committee, and the Southern Christian Leadership Conference.[150] Army intelligence agents attended meetings and submitted reports to headquarters, describing the name of the organization, date of the gathering, speakers, attendees, and whether a disorder occurred. The army drew from open sources and law enforcement databases. The substance of the reports ranged from targets' political views to their sex lives and financial conditions.[151]

In early 1970, the Senate weighed in. The Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary held hearings on the degree to which the military engaged in domestic surveillance. As Congress turned up the heat, the army began its own, internal review, the result of which was the suspension of the blacklist.[152]

In 1972, the Supreme Court addressed the constitutionality of this program.[153] Chief Justice Berger, writing for the Court, indicated that surveillance alone, particularly when drawn from open source material, did not prove a chilling effect on First Amendment activities. The claimants had not demonstrated any illegal wiretap or electronic bugging, breaking and entering, or concrete damage.[154] Justice William O. Douglas, in a vigorous dissent, wrote:

> The act of turning the military loose on civilians even if sanctioned by an Act of Congress, which it has not been, would raise serious and profound constitutional questions. Standing as it does only on brute power and Pentagon policy, it must be repudiated as a usurpation dangerous to the civil liberties on which free men are dependent.[155]

CONUS used undercover agents to infiltrate civilian groups and open confidential files. Stealth and secrecy, coupled with cameras and electronic ears, allowed the army to gather information, which it then distributed back to civilian law enforcement agencies. Douglas thundered,

> [t]his case involves a cancer in our body politic. It is a measure of the disease which afflicts us . . . . The Constitution was designed to keep government off the backs of the people. The Bill of Rights was added to keep the precincts of belief and

---

[150] *See* Laird v. Tatum, 408 U.S. 1 (1972); STONE, *supra* note 117, at 493.

[151] STONE, supra note 117, at 487; *see also* ATHAN THEOHARIS, SPYING ON AMERICANS: POLITICAL SURVEILLANCE FROM HOOVER TO THE HUSTON PLAN (1978).

[152] *Laird*, 408 U.S. at 7-8 (discussing the letter from the Under Secretary of the Army to Senator Sam J. Ervin, Chairman of the Senate Subcommittee on Constitutional Rights, announcing a change in army policy).

[153] *See id.* at 1-40.

[154] *Id.* at 11.

[155] *Id.* at 24 (Douglas, J., dissenting).

> expression, of the press, of political and social activities free from surveillance. The Bill of Rights was designed to keep agents of government and official eavesdroppers away from assemblies of people. The aim was to allow men to be free and independent and to assert their rights against government. There can be no influence more paralyzing of that objective than Army surveillance.[156]

CONUS did not represent the first time the military had gathered extensive information on civilians. An *amicus curiae* filed by a group of former army intelligence agents claimed that "[a]rmy intelligence has been maintaining an unauthorized watch over civilian political activity for nearly thirty years." The brief referred to the Corps of Intelligence Police actions from 1917 to 1924, when a massive surveillance operation "involved the use of hundreds of civilian informants, the infiltration of civilian organizations and the seizure of dissenters and unionists, sometimes without charges."[157] The agents continued, "[t]hat activity was opposed—then as now—by civilian officials on those occasions when they found out about it, but it continued unabated until postwar disarmament and economies finally eliminated the bureaucracy that conducted it."[158]

4. The Church Committee

The programs described above do not represent the only surveillance operations underway. For instance, in 1969, President Richard Nixon, concerned that tax-exempt funding assisted anti-government groups, pressed the Internal Revenue Service ("IRS") to create its own surveillance arm to "collect relevant information on organizations predominantly dissident or extremist in nature and on people prominently identified with these organizations."[159] By 1974, the Activist Organizations Committee (renamed the Special Services Staff) had 2,873 organizations and 8,585 people on file. The IRS distributed this information to the FBI, Secret Service, Army Intelligence, and the White House. The IRS conducted targeted audits and investigations of those on its list.[160]

In 1970, the Treasury Department initiated a program to obtain citizens' library records. What began as a single Treasury visit to the Milwaukee Public Library to determine who had read books on explosives soon burgeoned into similar moves in Richmond, California, Cleveland,

---

[156] *Id.* at 28 (Douglas, J., dissenting).

[157] *Id.* at 27 (Douglas, J., dissenting) (quoting Brief for A Group of Former Army Intelligence Agents as Amici Curiae at 29-30, *Laird*, 408 U.S. 1 (No. 71-288)).

[158] *Id.* at 27-28 (Douglas, J., dissenting) (citing Brief for A Group of Former Army Intelligence Agents, *supra* note 157).

[159] STONE, *supra* note 117, at 493.

[160] *Id.*

Ohio, and Atlanta, Georgia. The American Library Association ("ALA") Executive Board immediately issued a statement affirming its commitment to keeping records confidential.[161] It directed librarians to resist federal trawling missions until a court of competent jurisdiction found good cause. The ALA later extended confidentiality to "database search records, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services."[162] Although the FBI continued to try to access library records, the ALA stood firm.[163] In support of the ALA, thirty-eight states and the District of Columbia passed statutes to prevent the Executive from gaining access to readers' records.[164]

As rumors about these and other projects began to circulate, Congress entered the ring. Between 1965 and 1974, the legislature held forty-seven hearings and issued reports on privacy-related issues.[165] Senator Frank Church's hearings between 1973 and 1976 stood out amongst these, becoming symbols of the era. From assassination to covert operations, the proceedings shed light on the darkest corners of the executive branch.

Not everyone, though, felt such inquiry to be appropriate. In words that echo today's counterterrorist discussions in Congress, Senator Tower asserted,

> we are confronted in this world by a very powerful adversary that would not hesitate to resort to military means to achieve its political objectives. A powerful adversary that itself, through its clandestine activities and overt activities, generates military activity all over the world . . . thereby jeopardizing the peace and security of everybody . . . . [W]e cannot draw this in strict terms of war and peace, in terms of whether or not the United States is actually at war. We are in effect in a war of sorts.[166]

Indeed, the tone of the hearings was, at times, almost apologetic for daring to ask questions. Concern centered on attempting to "balance the right to privacy against the need for national security."[167]

---

[161] OFFICE FOR INTELLECTUAL FREEDOM, AM. LIBRARY ASS'N, INTELLECTUAL FREEDOM MANUAL 154-55 (5th ed. 1996) [hereinafter ALA MANUAL]; *see* also HERBERT FOERSTAL, SURVEILLANCE IN THE STACKS: THE FBI'S LIBRARY AWARENESS PROGRAM (1991).

[162] AM. LIBRARY ASS'N, POSITION STATEMENT ON THE CONFIDENTIALITY OF LIBRARY RECORDS, *available at* http://www.ala.org/ala/aasl/aaslproftools/positionstatements/aaslpositionstatementconfidentiality.htm.

[163] The "Library Awareness Program" was an FBI effort to recruit library staff to aid in surveillance of Soviet use of technology information in libraries. *See* Anne Klinefelter, *The Role of Librarians in Challenges to the USA PATRIOT Act*, 5 N.C. J.L. & TECH. 219, 223 (2004).

[164] STRUM, *supra* note 89, at 151.

[165] *Id.* at 150-51.

[166] *Church Committee* Vol. 5, *supra* note 98, at 64.

[167] *Id.* at 65.

While cognizant of these reservations, the Church Committee persevered. It found that the Executive had undertaken covert surveillance of citizens purely on the basis of political beliefs, even when such ideas posed no threat of violence or illegal actions.[168]

The Executive responded to the Church Committee's findings with a series of actions to curb surveillance. In 1976, President Ford banned the NSA from intercepting telegraphs. He also forbade the CIA from conducting electronic or physical surveillance of American citizens. The new FBI director, Clarence Kelly, publicly apologized for the Hoover era.[169] Attorney General Edward Levi, like Harlan Fiske Stone after the Red Scare in 1920, introduced guidelines that required the FBI to have "specific and articulable facts" indicating criminal activity before opening an investigation. Although they lacked legal force, the guidelines could serve in a judicial setting as a way to calibrate the organization's actions.[170] Each one of these protections has now been eliminated. I will return to this in Part I.D.

Although the Executive also made noise about wanting to protect privacy more generally, subsequent legislation introduced by the Nixon Administration, to put it mildly, lacked teeth.[171] The Privacy Act ostensibly regulated the collection, maintenance, use, and dissemination of citizens' personal data.[172] The statute allowed the CIA to exempt its files from any legal requirement to provide citizens access.[173] Any agency with law

---

[168] The Committee continued,

> [t]he Government, operating primarily through secret informants . . . has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity . . . . FBI headquarters alone has developed over 500,000 domestic intelligence file.

Final Report, *supra* note 110, at 5-6.

[169] STONE, *supra* note 117, at 496.

[170] James Q. Wilson, *The Case for Greater Vigilance*, TIME, May 1, 1995, at 73; *see also* STONE, *supra* note 117, at 496-97.

[171] During the Church Hearings, President Nixon appointed a Domestic Council Committee on the Right of Privacy. He gave the committee four months to draft "direct, enforceable measures." Vice President Ford, who chaired the committee, objected strongly to a number of Senators' calls for the creation of a Federal Privacy Board. Instead, he backed the conclusions of a 1973 Department of Health, Education, and Welfare report, "Records, Computers, and the Rights of Citizens," which proposed a "code of fair information practices." STRUM, *supra* note 89, at 152-56.

[172] Privacy Act of 1974, 5 U.S.C. § 552a (2000).

[173] GINA MARIE STEVENS, AM. LAW DIV., PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS 6 (2003).

enforcement, prosecution, or probation activities could exempt identification information, criminal investigative materials, and reports assembled between arrest and release.[174] Moreover, any national security information held by any agency could be exempted, as well as any Secret Service files, or law enforcement material.[175] The statute allowed data to be shared within and between government agencies.[176] Although the kind of information that could be obtained had to be gathered for a lawful purpose, what constituted a "lawful purpose" was left up to the agency. Citizens could request information about files on themselves, but the legislation failed to include any timeframe for a response. Congress left the implementation of the legislation to an understaffed, under-funded Office of Management and Budget ("OMB").[177]

With these gaping holes, not surprisingly, a commission appointed in 1977 by President Jimmy Carter found that the difficulty with the Privacy Act was "that agencies have taken advantage of its flexibility to contravene its spirit."[178] The review added, "[t]he Act ignores or only marginally addresses some personal-data record-keeping issues of major importance now and for the future."[179] Consequently, the legislation "has not resulted in the general benefits to the public that either its legislative history or the prevailing opinion as to its accomplishments would lead one to expect."[180] In 1986, the United State's General Accounting Office ("GAO") similarly reported on the poor implementation of the Privacy Act.[181] The DOJ noted in 2004, "[t]he Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. Moreover, even after more than twenty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored."[182]

---

[174] *Id.*

[175] *Id.*

[176] 5 U.S.C. § 552a(b); *see also* Stevens, *supra* note 173, at 7.

[177] STRUM, *supra* note 89, at 153.

[178] PERSONAL PRIVACY IN AN INFORMATION SOCIETY: THE REPORT OF THE PRIVACY PROTECTION STUDY COMMISSION (transmitted to President Jimmy Carter on July 12, 1977), *available at* http://www.epic.org/privacy/ppsc1977report/ c1.htm.

[179] *Id.* at 4.

[180] *Id.*

[181] STRUM, *supra* note 89, at 153-54.

[182] *See* U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 (2004), *available at* http://www.usdoj.gov/04foia/1974intro.htm; *see also* STRUM, *supra* note 89, at 154-56.

5. The Foreign Intelligence Surveillance Act

As the extent of the domestic surveillance operations emerged, Congress attempted to scale back the Executive's power while leaving some flexibility to address national security threats.[183] The legislature focused on the *targets* of surveillance, limiting a new law to foreign powers, and agents of foreign powers—which included groups "engaged in international terrorism or activities in preparation therefor."[184] Congress distinguished between U.S. and non-U.S. persons, creating tougher standards for the former.[185] The Foreign Intelligence Surveillance Act ("FISA") considered any "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication," as well as other means of surveillance, such as video, to fall under the new restrictions.[186] Central to the statute's understanding of surveillance was that, by definition, consent had not been given by the target. Otherwise, the individual would have a reasonable expectation of privacy and, under ordinary circumstances, the Fourth Amendment would require a warrant.[187]

FISA provided three ways to initiate surveillance: Attorney General Certification, application to the Foreign Intelligence Surveillance Court ("FISC"), and emergency powers. Of these, the second serves as the principal means via which surveillance is conducted.[188]

---

[183] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, tit. 1, § 102, 92 Stat. 1786 (1978) (codified as amended at 50 U.S.C. §§ 1801-11 (2000)).

[184] 50 U.S.C. §1801(a)(4). An agent of a foreign power is anyone, other than a U.S. person who, *inter alia*, "knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power." *Id.* § 1801(b)(2)(C). "International terrorism" incorporated three elements: (a) acts dangerous to human life and in violation of criminal law; (b) the intent to influence government policy or to intimidate or coerce a civilian population; and (c) acts that "occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum." *Id.* § 1801(c)(1)-(3).

[185] The former included citizens and resident aliens, as well incorporated entities and unincorporated associations with a substantial number of U.S. persons. Non-U.S. persons qualified as an "agent of a foreign power" by virtue of membership—e.g., if they were an officer or employee of a foreign power, or if they participated in an international terrorist organization. *Id.* § 1801(i). U.S. persons had to engage *knowingly* in the collection of intelligence contrary to U.S. interests, the assumption of false identity for the benefit of a foreign power, and aiding or abetting others to the same. *Id.* § 1801(b).

[186] *Id.* § 1801(f)(1); *see also id.* § 1801(f)(4); DANIEL BLINKA, ELECTRONIC SURVEILLANCE: COMMENTARIES AND STATUTES (2004).

[187] 50 U.S.C. §1801 (f)(1)-(4).

[188] Under the first, the President, through the Attorney General, has the authority to collect information related to foreign intelligence—*without judicial approval*—for up to one year. The Attorney General must attest in writing, and under oath, that the electronic

Under this mechanism, to open surveillance on a suspect, the executive branch applies to FISC, a secret judicial body, for approval.[189] The application must provide the name of the federal officer requesting surveillance and the identity of the target (if known), or a description of the target.[190] It must include a statement of facts supporting the claim that the target is a foreign power (or an agent thereof) and that the facilities to be monitored are currently, or expected to be, used by a foreign power or her agent.[191] Probable cause must be presented that the individual qualifies as a foreign power and will be using the facilities surveilled.[192] The application must describe the "nature of the information sought and the type of communications or activities to be subjected to the surveillance." Importantly, the court is not required to determine that probable cause exists as to whether any foreign intelligence information will be uncovered.[193] The application requires a designated national security or

surveillance will be directed at communications between foreign powers or from property under their control, that "no substantial likelihood" exists that a US person will be party to the communications, and that every effort will be made to minimize the acquisition, retention, and dissemination of information relating to U.S. persons. *Id.* § 1802(a)(1), (h)(1), (a)(2). Under the third approach, emergency powers, where the Attorney General reasonably determines that "an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information," she must inform a judge that the decision has been made to engage in the activity. The Attorney General has twenty-four hours from the initiation of authorization to submit a full application. In the event that the application is ultimately denied, an exclusionary rule applies to any information gathered in the interim. Although the law requires that, in the event that the application is denied, notice be given to the target of emergency surveillance, such notice may be suspended for ninety days and, thereafter, indefinitely, subject to an *ex parte* showing of good cause. *Id.* § 1805(f), (j); *id.* § 1811.

[189] Following 9/11, Congress expanded FISC, which initially consisted of seven United States' district judges from different circuits, to eleven judges, three of whom had to reside in the vicinity of Washington, D.C. 50 U.S.C. § 1803(a) (2000 & Supp. 2004). The judges serve a maximum of seven years. *Id.* § 1803(d). Consistent with the original statute, three additional judges, all chosen by the Chief Justice, constitute a special review panel. *Id.* § 1803(b). Writs of certiorari can be submitted from this court to the Supreme Court. *Id.* Although initially only the President or Attorney General filed applications, in 1979 President Jimmy Carter issued an Executive Order extending the number of officials authorized to certify the application to the court to include the Secretary of State, Secretary of Defense, Director of Central Intelligence, Director of the Federal Bureau of Investigation, Deputy Secretary of State, Deputy Secretary of Defense, and Deputy Director of Central Intelligence. Exec. Order No. 12,139, 44 Fed. Reg. 30,311 (1979).

[190] 50 U.S.C. § 1804(a)(1), (3).

[191] *Id.* § 1804(a)(4).

[192] *Id.* § 1805(b).

[193] *Id.* § 1804(a)(6). Here the FISA procedures depart from regular criminal law, which requires probable cause that the information sought will be obtained. *See* LAFAVE, *supra* note 15, at 364-65.

defense officer to certify that the information is related to foreign intelligence, and that "such information cannot reasonably be obtained by normal investigative techniques."[194] It must specify how the surveillance is to be affected (including whether physical entry is required).[195] It includes all previous applications involving the "persons, facilities, or places specified in the application,' and actions taken by the court on these cases must accompany the application.[196] The form includes an estimate of time required for surveillance and requires an explanation as to why authority should not terminate at the end of the requested period.[197] Finally, if more than one surveillance device is to be used, the applicant must address the minimization procedures and describe the range of devices to be employed.[198] In addition to this information, the judge may request additional data.[199]

In 1994, Congress amended the statute to allow for warrantless, covert physical searches (not just electronic communications' intercepts) when targeting "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers."[200] The statute requires that there be no substantial likelihood that the facilities targeted are the property of a U.S. person.[201] Applications must include the same information as for electronic surveillance.[202] Twice a year the Attorney General informs Congress of the number of applications for physical search orders, the number granted, modified, or denied, and the number of physical searches that ensued.[203]

In addition to the above powers, FISA provided the authority for the installation and use of pen register and trap and trace devices for international terrorism investigations.[204] The Attorney General, or a designated attorney, must submit an application in writing and under oath either to the FISA court or to a United States Magistrate Judge specifically appointed by the Chief Justice to hear pen register or trap and trace

---

[194] *Id.* § 1804(a)(7).
[195] *Id.* § 1804(a)(8).
[196] *Id.* § 1804(a)(9).
[197] *Id.* § 1804(a)(10).
[198] *Id.* § 1804(a)(11).
[199] *Id.* § 1804(d).
[200] *Id.* § 1821(a)(1)(A)(i).
[201] *Id.* § 1822(a)(1)(A).
[202] *Id.* § 1823.
[203] *Id.* § 1826.
[204] Pen registers obtain the number dialed from a particular phone; trap and trace devices act as a caller ID record. *Id.* § 1842(a)(1).

applications on behalf of the FISA court.[205] The application must include information to show that the device has been, or will in the future be, used by someone who is engaging or has engaged in international terrorism or is a foreign power or agent thereof.[206] Thus, a U.S. citizen, thought to be engaged in international terrorism, may be the target of the pen register or trap and trace device. No notice is required for individuals targeted under this power. The order can be granted for up to ninety days, with an additional ninety-day extension.[207] As with electronic surveillance, in the event of an emergency the Attorney General can authorize the installation and use of a pen register or trap and trace device without judicial approval.[208] A proper application must be made to the appropriate authority within forty-eight hours.[209] Information thus obtained *can* be used in court proceedings, although reasonable effort must be made to inform the target that the government "intends to so disclose or so use such information."[210]

Despite the safeguards included in the requirements for FISA applications, a legitimate question could be raised as to whether the court merely serves as a rubber stamp function. Between 1979 and 2003, FISC only denied three out of 16,450 applications submitted by the executive branch.[211] Federal officials claim that this simply reflects the professionalism of the executive branch; an application that would not pass muster would simply be stopped before reaching the court.[212] While this

---

[205] *Id.* § 1842(a)-(b). As with the application for electronic surveillance, the applicant must include the official's name seeking surveillance, as well as certification that "the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation." *Id.* § 1842(c)(1)-(2).

[206] *Id.* § 1842(c)(A).

[207] *Id.* § 1842(e).

[208] *Id.* § 1843(a).

[209] *Id.* § 1843(a)(2).

[210] *Id.* § 1845(c). Following the 9/11 attacks, Congress relaxed the requirement for factual proof: the applicant no longer must demonstrate why she believes the telephone line will be used by an individual engaged in international terrorism. Instead, the applicant must only demonstrate that the information likely to be gained does not directly concern a U.S. person and that the information will be relevant to protect against international terrorism. This provision, hotly contested by civil libertarians, was scheduled to sunset Dec. 31, 2005. *See* Uniting and Strengthening America by Proving Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub. L. No. 107-56, § 215, 115 Stat. 272 (codified as amended at 50 U.S.C. §1861 (2000 & Supp. 2001)) [hereinafter USA PATRIOT Act]; 18 U.S.C. § 214 (2000). Instead, Congress made it permanent. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, § 102, 120 Stat. 192 (2006).

[211] *See generally* Foreign Intelligence Surveillance Act, http://fas.org/irp/agency/doj/fisa (last visited June 9, 2006). Statistics compiled by author.

[212] Interview with Department of Justice officials, in S.F., Cal. (2003); in San Jose, Cal.

ratio does not significantly depart from the number of requests denied for ordinary wiretap applications, considering the lowered standards of proof required, and the increasing tendency to use FISA for U.S. persons and criminal investigations, it presents troubling issues.

Also of concern is the increasing use of these powers. Between 1978 and 1995, the Executive made just over five hundred new applications per year. Since 1995, however, the numbers have steadily grown, with a sudden burst in the post-9/11 era: in 2002, the number leapt to 1228 and in 2003 to 1727 applications. For the first time in history, in 2002 and 2003, DOJ requested *more* wiretaps under FISA than under ordinary wiretap statutes. This suggests a significant shift in the executive government's strategy for gathering information. Under FISA, law enforcement must cross a much lower threshold, and is not subject to the same Fourth Amendment restrictions as in the ordinary criminal code. I will return to this in considering the impact of the USA PATRIOT Act and DOJ's use of FISA as a tool in ordinary criminal prosecution.

While FISA pushed back on the worst excesses of the McCarthy era, efforts by the Executive to obtain personal information continued. The next section details further expansions in the powers available.

C. THE INFORMATION AGE

The 1970s signaled a sudden acceleration of telephony and digital technology. Public unease at inroads into privacy continued, but the Executive steadily chipped away at FISA.[213] Under the banner of counterterrorism, the 1994 Communications Assistance for Law Enforcement Act and the 2001 USA PATRIOT Act provided the state even greater access to information.[214]

(2004); in N.Y., N.Y. (2005).

[213] *See, e.g.*, *Privacy and 1984: Public Opinions on Privacy Issues: Hearing Before a Subcomm. of the H. Comm. on Government Operations*, 98th Cong. 38 (1984) (Southern New England Telephone submission) (citing increasing public concern with computer threat to privacy: 1974 = 38%, 1976 = 37%, 1977 = 41%, 1978 = 54%).

[214] The 1986 Electronic Communications Privacy Act brought new technologies under the rules previously applied to telephones: the Wiretap Act, which extended authorities to cellular technologies, the Pen Register Act, and the Stored Communications Act. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). Two minor statutes provided some additional protection of personal data: the 1988 Video Privacy Protection Act prohibited video service providers from releasing data without either a court order or consent from its customers. 18 U.S.C. § 2710. The same year, the Computer Matching and Privacy Protection Act required that federal agencies create procedural agreements and Data Integrity Boards before exchanging information. 5 U.S.C. § 552a.

1. 1994 Communications Assistance for Law Enforcement Act

With the breakup of Ma Bell and the spread of digital technology and fiber optic networks, the FBI became increasingly concerned that it would not be able to trace or intercept certain forms of private communications.[215] In 1991, 1992, and 1993, the ACLU, the Electronic Frontier Foundation, Computer Professionals for Social Responsibility, and more than twenty communications companies, successfully beat back efforts by the FBI to introduce a Digital Telephony law.[216] The FBI's Advanced Telephony Unit fought back, estimating that, by 1995, some forty percent of intercepted communications would be encrypted.[217] The GAO viewed the Bureau's initiative as unneeded and potentially detrimental to American competitiveness.[218] In addition to general privacy concerns, numerous groups expressed concern that back doors would open the way for hackers to enter otherwise secure systems.[219] But in 1994, the FBI triumphed. The Communications Assistance for Law Enforcement Act ("CALEA") required telecommunication companies to create special access for the government.[220]

The FBI immediately tried to strengthen its new tool. Within a year, for instance, the FBI announced plans to require telecoms to be able to wiretap one out of a thousand calls in the U.S., and one out of hundred calls in major U.S. cities *simultaneously*.[221] Fierce opposition erupted, forcing the Bureau to adopt a scaled-back capacity requirement.[222] The FBI called for cellular telecommunications companies to be able to pinpoint the precise location of a customer in less than a second.[223] This regulation contradicted the plain language of the statute, which exempted from call-identifying

---

[215] From the 1970s forward, the telephony field witnessed an accelerating trend towards electronic switches, digital processing, and optical transmission. As of 1993, eighty percent of the switches were digital. These switches made it difficult for law enforcement to trace calls. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE : THE POLITICS OF WIRETAPPING AND ENCRYPTION (1998); OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE, OTA-BP-ITC-149, at 29-30 (1995).

[216] STRUM, *supra* note 89, at 161.

[217] DIFFIE & LANDAU, *supra* note 215, at 183.

[218] *Id.* at 184.

[219] *Id.*

[220] Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002 (2000).

[221] FBI Implementation of the Communications Assistance for Law Enforcement Act, Initial Notice, 60 Fed. Reg. 53,643 (Oct. 16, 1995); *see also* STRUM, *supra* note 89, at 162; DIFFIE & LANDAU, supra note 215, at 197.

[222] FBI Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, Final Notice of Capacity, 63 Fed. Reg. 12,218 (Mar. 12, 1998); *see also* STRUM, *supra* note 89, at 162.

[223] DIFFIE & LANDAU, *supra* note 215, at 197.

information any data "that may disclose the physical location of the subscriber (except as can be determined from the telephone number)."[224]

Left and Right in Congress agreed: the FBI was overreaching. In March 1998, Republican Representative Bob Barr introduced a bill to delay CALEA's implementation.[225] He complained that Congress intended the FBI to have "only a consultative role in the implementation of CALEA" and that the telecommunications industry "develop the technical standards necessary."[226] The FBI, however, had stepped outside its consultative role, simultaneously trying to expand its power. Moreover:

> The capabilities proposed to be included by the FBI are costly, technically difficult to deploy or technically infeasible, and raise significant legal and privacy concerns. . . . The FBI is now threatening enforcement action and the denial of appropriate cost reimbursement to the industry if its proposed capabilities are not deployed by the industry.[227]

In 2003, the FBI informed the FCC that Voice-over Internet Protocol ("VoIP") consumed an increasing percentage of Internet traffic. Unwilling to risk the public wrath that would accompany even more inroads into the electronic realm, in March 2004, the FBI petitioned the FCC for expedited rulemaking, which would have expanded CALEA to the Internet.[228] In a joint statement that brought together such diverse bedfellows as the ALA, Sun Microsystems, Americans for Tax Reform, and the ACLU, those opposed asserted that it would be unlawful, unwise, and unnecessary to grant law enforcement's demands.[229] The FCC tried to "compromise," by suggesting that CALEA only be applied to "managed" VoIP systems. In

---

[224] 47 U.S.C. § 1002(a)(2)(B).

[225] Communications Assistance for Law Enforcement Act Implementation Amendments of 1998, H.R. 3321, 105th Cong. (2d Sess. 1998), *available at* http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.3321.IH:.

[226] 144 Cong. Rec. H850 (daily ed. Mar. 4, 1998) (statement of Rep. Barr).

[227] *Id.*

[228] The document requested that the agency issue a Declaratory Ruling "that broadband access services and broadband telephony services [and push-to-talk 'dispatch' service] are subject to CALEA." Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act III (proposed Mar. 10, 2004) (submitted by John G. Malcom, Patrick W. Kelley, and Robert T. Richardson).

[229] Joint Statement of Industry and Public Interest, before the Federal Communications Commission, Washington, D.C., in the matter of Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, at 1 (proposed Apr. 27, 2004) (submitted by James X. Dempsey, John B. Morris, Jr., Lara M. Flint, and Bruce J. Heiman). The changes, moreover, would mean a significant alteration of the structure of the Internet. *See* DIFFIE & LANDAU, *supra* note 215, at 19.

addition to issues of privacy and precedent, this "solution" penalized companies jumping in the game early—a dynamic hitherto critical for the growth of the Internet.

2. 2001 USA PATRIOT Act

Six days after the 9/11 attacks, Representative James Sensenbrenner, Chair of the House Judiciary Committee, stepped out of the shower at his home in Wisconsin and overheard a familiar voice on the television: John Ashcroft calling on Congress to pass the Administration's antiterrorism legislation within a week. Sensenbrenner, for whom this came as something of a surprise, immediately got on the telephone to demand a copy of the bill. The draft, which arrived by fax, numbered hundreds of pages and included, *inter alia*, the indefinite suspension of the writ of habeas corpus in the United States. Sensenbrenner, sitting on his porch, put a red line through the measure.[230] The next six weeks became an exercise in high politics.[231]

Even as the executive branch sought significantly broader powers, it insisted on haste: in the Senate, the bill bypassed committee markup and went straight behind closed doors. The House held only one hearing, at which the Attorney General served as the only witness.[232] At 3:43 a.m. on the morning of the vote, the final bill reached print. Legislators, many of whom were even unable to read the text because of the anthrax scare, were given only the opportunity to vote thumbs up or thumbs down—with no chance of further amendment.[233] The Speaker ruled the one legislator who tried to debate parts of the act out of order.[234] Throughout this process the Executive made it very clear that either one supported what the Administration proposed or one was pro-terrorist. Attorney General Ashcroft announced to the Senate Judiciary Committee,

> [t]o those who scare peace-loving people with phantoms of lost liberty, my message is this: your tactics only aid terrorists, for they erode our national unity and diminish our resolve. They give ammunition to America's enemies, and pause to America's friends. They encourage people of good will to remain silent in the face of evil.[235]

---

[230] Interview with Rep. James Sensenbrenner, in Palo Alto, Cal. (Spring 2003).

[231] *See* Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145 (2004).

[232] Jim Dempsey, Ctr. for Democracy and Tech., D.C., Guest Lecture at Stanford University Law School (Jan. 24, 2005).

[233] Interview with Rep. James Sensenbrenner, *supra* note 230.

[234] Dempsey, *supra* note 232.

[235] *The Homeland Security Act of 2002*, 107th Cong. 107-50 (2001) (statement of Attorney General John Ashcroft).

The 2001 USA PATRIOT Act *did* have an immediate and far-reaching impact on civil liberties, despite Ashcroft's admonition. To make the statute more palatable, Congress placed sunset provisions on some of the most intrusive powers, setting them to expire December 31, 2005. But in July 2005, the House of Representatives voted not just to renew them, but to make fourteen out of sixteen of the new measures permanent—narrowly defeating an effort to limit the provisions to another four years.[236]

The House version clashed with the Senate's renewal bill, which offered greater protection for individual rights. In autumn, the proposed texts met in conference. By December 8, Representative Sensenbrenner was able to submit the report to the House of Representatives where, six days later, it passed 251 to 174.[237] Legislators twice extended the deadline, first to February 3, then to March 10, to give both Houses the opportunity to discuss the measures in more depth.[238]

In the end, the USA PATRIOT Improvement and Reauthorization Act of 2005 made all but two of the temporary surveillance powers in the USA PATRIOT Act permanent; roving wire taps under FISA, and FBI authority, with a court order, to obtain tangible items (books, records, papers, and documents) for foreign intelligence and international terrorism investigations became subject to a four-year sunset provision.[239] The Improvement Act incorporated some protections for individual rights.[240] The legislation also introduced new counterterrorist powers, as well as anti-drug measures aimed at preventing the bulk purchase of ingredients used in the manufacture of methamphetamine.[241]

As President Bush signed the Improvement Act into law, he credited the earlier legislation for breaking up terror cells in Ohio, New York, Oregon and Virginia.[242] He implied that it assisted in the prosecution of

---

[236] *House Approves Renewal of Patriot Act: Critics Voice Concern over Civil Liberties*, CNN.COM, July 22, 2005, http://www.cnn.com/2005/POLITICS /07/21/patriot.act [hereinafter *House Approves*]

[237] Roll no. 627, Dec. 14, 2005.

[238] *See* S. Res. 2167, 109th Cong. (2005) (enacted); Sheryl Gay Stolberg, *Key Senators Reach Accord on Extending the Patriot Act*, N.Y. TIMES, Feb. 10, 2006, at A14.

[239] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, tit. I §§ 102-03, 120 Stat. 192 (2006).

[240] *See, e.g.*, *id.* at § 115 (judicial review of national security letters), § 119 (audit of use of national security letters).

[241] Combat Methamphetamine Epidemic Act of 2005, Pub. L. No. 109-177, tit. VII, 120 Stat. 192 (codified as amended in scattered sections of 18 U.S.C.).

[242] Press Release, White House, President Signs USA PATRIOT Improvement and Reauthorization Act The East Room (Mar. 9, 2006) *available at* http://www.whitehouse.gov/news/releases/2006/03/20060309-4.html.

terrorists in California, Texas, New Jersey, Illinois, Washington, and North Carolina.[243] And he welcomed the continuation and expansion of the previous powers as part of the war on terror.[244] This section looks at three of the most significant authorities addressed in the original legislation and renewal measures: FISA alterations, delayed notice search warrants, and national security letters.

a. FISA Alterations

The 2001 USA PATRIOT Act made two important changes to FISA: It allowed applications where foreign intelligence constituted only "a significant purpose" for the investigation, and it authorized the state to obtain tangible objects.

In the former area, where previously FISA applications required that the gathering of foreign intelligence be *the* reason for search or surveillance, the new legislation allowed for applications when foreign intelligence provided merely *a significant* reason.[245] The Attorney General quickly seized on this and issued guidelines that said such authorization could be sought even if the primary ends of the surveillance related to ordinary crime.[246] These guidelines effectively collapsed the wall between the FBI's prosecution and intelligence functions, allowing the organization to go around the Fourth Amendment.

Although FISC had operated for nearly three decades in complete secrecy, in May 2002, it published its opinion for the first time to protest Ashcroft's guidelines.[247] The court required that the state re-build the wall between the Bureau's prosecution and intelligence functions. FISC centered its directive on the statutory minimization requirement. The court raised concerns about abuse: it noted, for instance, that in September 2000, the government had admitted that it had made "misstatements and

---

[243] *Id.*

[244] *Id.*

[245] USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272 (codified as amended at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000 & Supp. 2001))*; see also id.* §§ 201 (codified as amended at 18 U.S.C. § 2516), 207 (codified as amended at 50 U.S.C. § 1805(e)(1)), 805 (codified as amended at 18 U.S.C. § 2339A).

[246] Memorandum from Attorney Gen. John Ashcroft, to the Dir. of the Fed. Bureau of Investigation, the Assistant Attorney Gen., the Criminal Div. Counsel for Intelligence Policy, and United States Attorneys (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html ("[The USA PATRIOT Act] allows FISA to be used *primarily* for a law enforcement purpose, as long as a significant foreign intelligence purpose remains.").

[247] *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 621 (Foreign Intel. Surv. Ct. 2002).

omissions of material facts" in some seventy-five of its counterterrorism applications.[248] The court recognized the reasons a wall had been placed between intelligence and criminal investigations. It suggested that "the 2002 procedures appear to be designed to . . . substitute FISA for Title III electronic surveillances and Rule 41 searches."[249] FISC expressed concern that:

> [C]riminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence, and when use of FISA can cease because there is enough evidence to arrest and prosecute.[250]

Such measures did not appear to be reasonably designed "to obtain, produce, or disseminate foreign intelligence information."[251] And so, the court imposed conditions.

For the first time in the history of FISC, the government appealed. The Executive argued that Congress' intent in changing the wording from "the" to "a significant" reason was, precisely, to eliminate the wall between intelligence and law enforcement agencies. The legislative history did not support the primary purpose test.[252] The executive branch claimed, moreover, that attempts to impose minimization were so intrusive as to "exceed the constitutional authority of Article III judges."[253]

Six months later, the three-judge appellate court appointed by Chief Justice Rehnquist issued its first opinion.[254] The decision reversed the lower court's ruling.[255] It suggested that FISA was never meant to apply only to foreign intelligence information relative to national security, but that it could also be used for ordinary criminal cases.[256] And it went even further: the appeals court interpreted the USA PATRIOT Act to mean that the *primary* purpose of the investigation could, indeed, be criminal investigations, "[s]o long as the government entertains a realistic *option* of dealing with the agent other than through criminal prosecution . . . ."[257]

---

[248] *Id.* at 620.

[249] *Id.* at 623.

[250] *Id.* at 624.

[251] *Id.* at 625.

[252] *In re* Sealed Case Nos. 02-001, 02-002, 310 F.3d 717, 722 (Foreign Intel. Surv. Ct. Rev. 2002).

[253] *Id.*

[254] *Id.*

[255] *In re All Matters*, 218 F. Supp. 2d at 746.

[256] *In re Sealed Case*, 310 F.3d at 727-39.

[257] *Id.* at 735 (emphasis added).

Stopping a conspiracy, for instance, would suffice.[258] To reach this conclusion, the court rejected the Fourth Circuit's finding in *United States v. Troung*, which rejected warrantless search and surveillance once a case crossed into a criminal investigation.[259] The appeals court suggested that *Troung* may even have been at fault for contributing "to the FBI missing opportunities to anticipate the September 11, 2001 attacks."[260] The court added that "special needs" may provide further justification for departing from constitutional limits.[261] Ashcroft hailed the decision, which reversed two decades of court policy, as "a giant step forward."[262]

This shift raises deeply troubling constitutional issues.[263] The Fourth Amendment requires a warrant to be issued by a neutral and detached magistrate, a finding of probable cause that a particular crime has been committed, and the designation of which places will be searched or which items will be seized.[264] The way FISA previously withstood challenge was, precisely, the *purpose* for which it was directed; this purpose allowed it to fall outside the warrant requirements of the Fourth Amendment.[265] By eviscerating purpose from the equation, the appeals court eliminated the basis on which the statute passed constitutional muster.

The second significant change to FISA rested on the type of information that could be obtained by the Executive. While FISA granted

---

[258] *Id.*

[259] United States v. Troung, 629 F.2d 908 (4th Cir. 1980).

[260] *In re Sealed Case*, 310 F.3d at 744.

[261] *Id.* at 745.

[262] Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1244 (2002).

[263] *See* O'Connor, *supra* note 262, at 1249 ("Searches conducted pursuant to these provisions, which are not primarily for foreign intelligence purposes, cannot pass constitutional muster. The conclusion to the contrary by the FISCR in *In re Sealed Case* is predicated upon internally inconsistent logic, selective editing and application of judicial decisions and statutory language, and a disregard for the legislative history of FISA."); *see also* Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306 (2004).

[264] U.S. CONST. amend. IV.

[265] O'Connor, *supra* note 262, at 1260 (under *Keith*, "criminal surveillance for any purpose other than foreign intelligence, even for a purpose that directly implicates national security, cannot escape the constraints of the Fourth Amendment"). Criminal surveillance must either satisfy the Fourth Amendment's warrant and probable cause requirements, or fall under an exception—namely, foreign intelligence. Moreover, the decision flies in the face of judicial and Congressional history. The United States Courts of Appeals for the First, Second, Fourth, and Eleventh Circuits all previously understood FISA to be for foreign intelligence or international terrorist purposes. These interpretations were consistent with the actual text of the statute. *See In re* All Matters Submitted to Foreign Intelligence Surveillance Court., 218 F. Supp. 2d 611, 625 (Foreign Intel. Surv. Ct. 2002).

broad access to electronic surveillance, it did not specifically empower the state to obtain business records. Following the Oklahoma City bombing, Congress expanded FISA orders to include travel records.[266] The USA PATRIOT Act provided further access to any business or personal records.[267] It also changed the standard under which FISC would be *required* to grant the order. Where previously specific and articulable facts had to demonstrate that the target represented a foreign power (or an agent thereof), the legislation eliminated the need for a particularized showing.[268] Thus, under the USA PATRIOT Act, the person seeking the records only has to say that the "records concerned are sought for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities." What constitutes an investigation is wholly within the domain of the executive branch—a definition that Ashcroft relaxed following the passage of the USA PATRIOT Act (a preliminary investigation is now sufficient.) This means that FISA can be used to gather records of individuals who are not themselves the target of any investigation, nor an agent of a foreign power. In fact, entire databases could be obtained in this manner, as long as "an authorized investigation" exists.[269]

Not only did the USA PATRIOT Act make these changes to FISA, but the manner in which the Executive obtained authorization for surveillance also shifted. As discussed above, applications to the FISA court are not the only way to initiate surveillance of non-U.S. persons. In the first twenty-

---

[266] Replies by Peter P. Swire, Patriot Debates: A Sourceblog for the USA PATRIOT Debate, http://www.patriotdebates.com/sections-214-and-215 (last visited June 9, 2006). Just two months before the Oklahoma City attack, President William J. Clinton issued Executive Order 12,949, which expanded the use of FISA for physical searches. *See* Exec. Order 12,949, 60 Fed. Reg. 8169 (Feb. 13, 1995).

[267] Under Section 501,

> (a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities.

USA PATRIOT Act, Pub. L. No. 107-56, § 501, 115 Stat. 272 (codified as amended at 50 U.S.C. § 1861 (2000 & Supp. 2001). This measure, assumedly, allows FISA to "trump" privacy laws that govern the dissemination of records. Swire, *supra* note 263, at 1331.

[268] *Id.*

[269] The statute added a rather insignificant stipulation drawn from the original FISA, that such an order could only follow if the "investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This, of course, left open the possibility of an investigation based "substantially" or "largely" upon protected activities. USA PATRIOT Act, § 501(a); *see also* Swire, *supra* note 263, at 1335.

three years of the statute's existence, attorneys general sporadically made use of the emergency category: in total, approximately fifty-five such orders issued. In the eighteen months following 9/11, however, this number dramatically increased: in 2002 alone, Ashcroft signed more than 170 emergency foreign intelligence warrants.[270]

b. Delayed Notice Search Warrants

One of the most concerning innovations in the USA PATRIOT Act affected the notice requirement for physical searches. Section 213, which applies to all federal criminal investigations—not just those conducted for counterterrorism—eliminates the "knock and announce" requirement long considered integral to determining whether or not a search warrant is deemed reasonable. In delayed notice, or "sneak and peek" search warrants, the government must only demonstrate reasonable cause to believe that notice may cause an adverse result, in order to prevent an individual from learning that the state appropriated their property or placed them under surveillance. While delayed notice was already provided by the Electronic Communications Privacy Act ("ECPA") and by the Second and Ninth Circuits Courts of Appeal, the USA PATRIOT Act allowed an indefinite suspension in notice. This provision is not subject to a sunset clause.

Like roving wiretaps, the USA PATRIOT Act was not the first time delayed notice search warrants appeared on the legislative stage.[271] Proposed in anti-drug bills, and then attached to a Bankruptcy Bill, Congress rejected the FBI's efforts to make it law. 9/11, however, presented another opportunity. Accordingly, the provision in the USA PATRIOT Act is not limited to terrorism; law enforcement can use it now for any crime on the books. Since the statute's passage, the state has used it to break into a judge's chambers, to look into health care fraud, and to investigate check swindling.[272] In July 2005, the Justice Department told

---

[270] Dan Eggan & Robert O'Harrow, Jr., *U.S. Steps Up Secret Surveillance: FBI, Justice Dept. Increase Use of Wiretaps, Records Searches*, WASH. POST, Mar. 24, 2003, at A1, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A16287-2003Mar23; *see also* James Bovard, *Surveillance State: Since September 11, A Flood of Federal Legislation Has Reduced American Freedom Without Increasing Our Safety*, AM. CONSERVATIVE, May 19, 2003, at 1, *available at* http://www.amconmag.com/05_19_03/cover.html.

[271] Roving wiretaps are authorized in the USA PATRIOT Act § 206 (codified as amended at 50 U.S.C. § 1805(c)(2)(B)). Through April 2005, the powers had been used forty-nine times. Gary Fi & Anne Marie Squeo*, Bipartisan Fix for Patriot Act Takes Shape: Both Parties in Congress Share Misgivings About Provisions on Libraries, Searches, Wiretaps,* WALL ST. J., Apr. 6, 2005, at A4.

[272] *American After 9/11: Freedom Preserved or Freedom Lost? Hearing Before the S.*

the House Judiciary Committee that only twelve percent of the 153 sneak and peek warrants it received were related to terrorism investigations.[273] What was illegal in the break-ins conducted under COINTELPRO has now become legal.

In its 2006 renewal of the USA PATRIOT Act, Congress added "enhanced oversight" of these powers. The legislation requires the judiciary to report to the Administrative Office of the courts, within thirty days of issuing a delayed notice search warrant: (a) the fact of the warrant application; (b) whether it was granted as applied, modified, or denied; (c) the length of the delay in notifying the subject of the search and the number and duration of any extensions; and, (d) the offense specified in the warrant or application.[274] Beginning in September 2007, this information will be provided to Congress.[275]

c. National Security Letters

The USA PATRIOT Act augmented the FBI's ability to bypass warrant requirements—under Title III *or* FISA—entirely.[276] Section 505, innocuously entitled "Miscellaneous National Security Authorities," enhanced the amount and type of information that could be obtained via national security letters ("NSLs"), bringing Internet Service Providers ("ISPs") within its remit and expanding the type of information that could be obtained to include credit card records, bank account numbers, and information pertaining to Internet use (such as protocol addresses and session times).[277] Importantly, the statute placed a gag order on anyone served with such administrative subpoenas.[278] It also broadened the range

---

Comm. on the Judiciary, 108th Cong. (2003) (statement of James X. Dempsey, Executive Dir., Ctr. for Democracy & Tech.) *available at* http://www.cdt.org/testimony/031118dempsey.pdf. (referencing a Department of Justice letter of Oct. 24, 2003 to Senator Stevens detailing the use of § 213 for non-terrorism-related purposes).

[273] Letter from Rep. James Sensenbrenner to the Chairman of the Comm. on the Judiciary (July 12, 2005), *available at* http://www.house.gov/judiciary_democrats/responses/dojpatriothrgquestionresp71205.pdf.

[274] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 114, 120 Stat. 192 (2006).

[275] *Id.*

[276] The district court found the lack of subsequent judicial process to be unconstitutional as applied, making it unnecessary to consider a facial challenge to § 2709 on Fourth Amendment grounds. Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004). The non-disclosure provision was unconstitutional on its face for failing to pass First Amendment muster. *Id.*

[277] USA PATRIOT Act § 210 (codified as amended at 18 U.S.C. § 2703(c)(2) (2000 & Supp. 2001)).

[278] National Security Letters draw their authority from one of four sources: The 1947

of officials who could request the information.[279] Where previously requests for information had to provide specific and articulable facts that established the target as a foreign power (or agent thereof),[280] the new NSL powers merely had to be *relevant* to *any* "authorized investigation to protect against international terrorism or clandestine intelligence activities."[281] The Bush Administration quickly attempted to make NSLs available to the CIA and Pentagon, without intervention of the DOJ.[282]

National Security Act authorizes investigative agencies to request financial records and information, consumer reports, and travel records for individuals with access to classified information, where such individuals are under investigation for sharing the information with foreign powers. National Security Act of 1947, 50 U.S.C. § 402 (2000). The Fair Credit Reporting Act provides for the FBI and certain government agencies to obtain consumer information in the course of investigations into international terrorism. Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681. The 1978 Right to Financial Privacy Act allows for the FBI to obtain financial records as part of their investigation into international terrorism and espionage. Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401-22. And, prior to 9/11, the Electronic Communications Privacy Act empowered the FBI, in the course of investigations into international terrorism or espionage, to request electronic communication related to agents of a foreign power from banks, credit agencies, and internet service providers. *See* Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2709. Although the Fourth Amendment applies to administrative subpoenas, because they are constructive searches, courts have *not* in the past required either a warrant or probable cause for them to be issued. Instead, the subpoena must only be "reasonable": that is, it falls within the agency's remit, the request is finite, and information is relevant to an appropriate inquiry. What makes such subpoenas constitutional, however, is that the party subpoenaed must have the opportunity to "obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply." *See Doe*, 334 F. Supp. 2d at 495 (2004) (quoting See v. City of Seattle, 387 U.S. 541, 544-45 (1967)). Even if granted *after* they are issued, a neutral tribunal can determine whether their issuance is compatible with the Fourth Amendment. Unlike NSLs, most administrative subpoenas do not require secrecy, or they limit secrecy to particular circumstances. *Id.* at 485.

[279] Section 505 expanded *who* could request the information from requiring that the request be made by an FBI official at the level of Deputy Assistant Director or above, to allowing *any* FBI Special Agent in charge of a field office to issue NSLs to obtain consumer reports, financial records, or electronic communications. Memorandum from Gen. Counsel, Nat'l Security Law Unit, Fed. Bureau of Investigation, to All Field Offices National Security Letter Matters, Ref: 66F-HQ-A1255972 Serial 15 (Nov. 28, 2001), *available at* http://sccounty01.co.santa-cruz.ca.us/bds/govstream/BDSvData/non_legacy/Minutes/2003/20030429/PDF/084.pdf [hereinafter FBI Memorandum].

[280] 18 U.S.C. § 2709(b)(1)(B).

[281] The practical effect of this, in the words of the Department of Justice, means that the FBI could issue an NSL stating, e.g., "[a] full international terrorism investigation of subject, a U.S. person, was authorized . . . because he may be engaged in international terrorism activities by raising funds for HAMAS." FBI Memorandum, *supra* note 279.

[282] Swire, *supra* note 263, at 1333 nn.185-86 (citing Eric Lichtblau & James Risen, *Broad Domestic Role Asked for CIA and the Pentagon*, N.Y. TIMES, May 2, 2003, at A21).

The application of NSLs to ISPs immediately implicated a broad range of institutions. The legal definition meant that traditional ISPs, such as America Online, Juno and UUNET, as well as companies whose cables and phone lines carry the traffic, would qualify.[283] It also incorporated companies that provide email but are not ISPs, like Microsoft and Netscape. It captured any service that creates mailing lists, such as Yahoo! Groups service. And it incorporated any library, school, or company that provides physical access to the Internet.[284] Indeed, evidence exists that some portion of the hundreds of NSLs served immediately following 9/11 related to libraries.[285] A study conducted by the University of Illinois found that in the twelve months following 9/11, federal agents made at least 545 visits to libraries to obtain information about patrons, affecting just over ten percent of the libraries polled.[286] Libraries, however, did not have the sole honor of receiving NSLs. In December 2003, the FBI letters sent to hotels in Las Vegas and required them to turn over access to all customer records between December 22, 2003 and January 1, 2004.[287] In similar fashion, the

---

[283] *In re* Doubleclick Inc., 154 F. Supp. 2d 497, 511 n.20 (S.D.N.Y. 2001).

[284] Brief for Electronic Frontier Foundation et al. as Amicus Curiae in Support of Plaintiffs John Doe and American Civil Liberties Union, Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (No. 04 Civ. 2614).

[285] A joint FOIA request filed by the ACLU, EPIC, American Booksellers for Free Expression, and the Freedom to Read Foundation, yielded five pages (entirely redacted) of institutions on whom NSLs had been served between October 2001 and January 2003. These pages are available at http://www.aclu.org/patriot_foia/FOIA/NSLlists.pdf. The lower court interpreted the missing names as numbering in the "hundreds." *Doe*, 334 F. Supp. 2d at 502.

[286] LEIGH S. ESTABROOK, LIBRARY RESEARCH CTR., PUBLIC LIBRARIES AND CIVIL LIBERTIES (2003), *available at* http://lrc.lis.uiuc.edu/web/PLCL.html. For a discussion of the impact of the USA PATRIOT Act on libraries in particular, see Klinefelter, *supra* note 163; Susan Nevelow Mart, *Protecting the Lady from Toledo: Post-USA PATRIOT Act Electronic Surveillance at the Library*, 96 LAW LIBR. J. 449 (2004). Although the § 215 changes to FISA would also have allowed the FBI to obtain these records, the FBI made use of NSLs instead. In response to an inquiry from James Sensenbrenner, the Chair of the House of Representatives' Judiciary Committee, Daniel J. Bryant, the Assistant Attorney General suggested that "the more appropriate tool [than § 215] for requesting electronic communication transactional records would be a National Security Letter (NSL)." Letter from Daniel J. Bryant, Assistant Attorney Gen., to James Sensenbrenner, Chairman, Comm. on the Judiciary, U.S. House of Representatives (July 26, 2002), *available at* http://www.lifeandliberty.gov/subs/congress/hjcpatriotactcombinedresponses3.pdf. A memorandum from Attorney General John Ashcroft to the Director of the Federal Bureau of Investigation, Robert Mueller, supports this reading; it confirmed that, as of 2003, § 215 had yet to be used. Memorandum from John Ashcroft, Attorney Gen., to Robert Mueller, Dir. of the Fed. Bureau of Investigation (Sept. 18, 2003) *available at* http://www.cdt.org/security/usapatriot/030918doj.shtml.

[287] The authorization for these NSLs came from the Intelligence Authorization Act for 2004. *See* discussion *infra*.

FBI obtained data from airlines, and hotels in the vicinity.[288] Even these few letters implicated an estimated 270,000 people, with no individualized suspicion to back them.[289] Internet service providers, too, have been inundated with requests. Mr. Al Gidari, a Seattle privacy lawyer who represents America Online, AT&T Wireless and Cingular states that "[d]emands for information have soared as much as five times over pre-September 11 levels."[290] The Associated Press reports, "[a]t one major Internet backbone provider, requests for information 'have gone through the roof.'"[291]

According to the *Washington Post*, the government now issues more than 30,000 National Security Letters each year, more than a hundred times the annual number prior to 9/11.[292] They have become routine procedure for preliminary investigations and also during the "threat assessment" stage, far before a formal investigation commences. Over five dozen FBI supervisors have been given the authority to issue NSLs.[293] There is no statutory limit on how much information can be gathered, or how many people can be targeted in each one of these letters.

Perhaps most concerning is the lack of control on who has access to the information, how long it is kept, and the manner in which it is used. In 2003, Attorney General Ashcroft withdrew a 1995 guideline that required the FBI destroy NSL information on American citizens or residents if such data proved "not relevant to the purposes for which it was collected."[294] In its place, Aschroft required the FBI to keep all records collected, and authorized them to disseminate such information to any federal agency. The same order stipulated that the Bureau use "data mining" technology to trawl through its rapidly-expanding files to try to find links between people. In January 2004, the FBI created an Investigative Data Warehouse. This

---

[288] JAY STANLEY, AM. CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN CONSTRUCTION OF A SURVEILLANCE SOCIETY, 13 n.51 (2004) (citing Editorial, *Surveillance City*, LAS VEGAS REV. J., Jan. 11, 2004, *available at* http://www.reviewjournal.com/lvrj_home/2004/Jan-11-Sun-2004/opinion/22961926.html).

[289] *Id.*; *see* Rod Smith, *Sources: FBI Gathered Visitor Information Only in Las Vegas*, LAS VEGAS REV. J., Jan. 7, 2004, *available at* http://www.reviewjournal.com/lvrj_home/2004/Jan-07-Wed-2004/news/22934251.html.

[290] *Net Effect: Antiterror Eavesdropping: Privacy Advocates Worry Civil Rights May Be Trampled*, ASSOCIATED PRESS, May 27, 2002, *available at* http://tinyurl.com/xmai [hereinafter *Net Effect*].

[291] *Id.*

[292] Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A1.

[293] *Id.*

[294] *Id.*

organization uses the same technology that the CIA depends upon, and which it is barred from using in similar fashion on American citizens.[295] Ashcroft also changed the guidelines to allow the FBI to incorporate commercially-available databases, such as ChoicePoint and LexisNexis. I return to the issue of data mining, below.

An important point to remember in the collection of this information is that it is subject neither to judicial review, nor detailed congressional oversight. In four years, the FBI has only provided Congress with classified statistics on the number of NSLs issued, the type of information obtained (financial, credit, or communication), and the number of U.S. persons targeted. These reports omit an entire category of NSLs, as well as other federal agencies' use of the same. Although Congress requested in 2004 that the Attorney General describe the scope of NSLs and provide the "process and standards for approving" them, eighteen months have now passed without a reply. As for the effectiveness of the device for counterterrorist purposes, the Bush Administration has not offered a single example of when the use of an NSL interrupted a terrorist attack.[296]

To date, two cases have made it to the courts. The first involved an Internet service provider. From the beginning, the plaintiff was in a precarious position: according to the USA PATRIOT Act, an individual served with an NSL could not disclose to *anyone* that the FBI had requested this information,[297] a stipulation that ostensibly included an attorney or even a court of law. (The renewal statute now allows individuals served with an order to discuss the matter with an attorney and those necessary to obtaining the information requested.[298])

In this case, the FBI telephoned Doe and told him that he would be served with an NSL.[299] The document, printed on FBI letterhead, directed him to provide certain information.[300] It informed him that the NSL provisions in the USA PATRIOT Act prohibited Doe or his employees, "from disclosing to *any person* that the FBI has sought or obtained access to information or records."[301] The FBI instructed him to deliver the records in person, not to use the postal system, and not to mention the NSL in any

---

[295] *Id.*

[296] *Id.*

[297] Doe v. Ashcroft, 334 F. Supp. 2d 471, 479 (S.D.N.Y. 2004) (citing 18 U.S.C. § 2709(c) (2000)).

[298] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 116(a), 120 Stat. 192 (2006).

[299] *Doe*, 334 F. Supp. 2d at 478.

[300] *Id.* at 479.

[301] *Id.*

telephone conversation.[302] Doe spoke with attorneys at the ACLU, refused to provide the information requested, and instead brought suit.[303]

The District Court held that a provision that barred recipients from disclosing receipt of NSLs, as applied, violated the Fourth Amendment because it did not allow for any judicial process.[304] Judge Victor Marrero, who wrote the opinion, noted that in nearly twenty years, not a single judicial challenge had been brought to the issuance of an NSL.[305] He suggested, "it would be . . . naïve to conclude that § 2709 NSLs, given their commandeering warrant, do anything short of coercing all but the most fearless NSL recipient into immediate compliance and secrecy."[306] The court subjected the gag order, which counted as both a prior restraint and a content-based restriction, to strict scrutiny.[307] It found that the indefinite nature of the ban on disclosure was not narrowly tailored to further the Government's interest in pursuing its counterterrorist strategy, stating that while the national security arguments may be valid ones, "in the end . . . the Government cannot cast § 2709—a blunt agent of secrecy applying in perpetuity to all persons affected in every case—as narrowly-tailored."[308] In short, this would potentially compel secrecy "even under some decidedly non-sensitive conditions or where secrecy may no longer be justifiable under articulable national security needs."[309] The court added,

> an unlimited government warrant to conceal, effectively a form of secrecy per se, has no place in our open society . . . . When withholding information from disclosure is no longer justified, when it ceases to foster the proper aims that initially may have supported confidentiality, a categorical and uncritical extension of non-disclosure may become the cover for spurious ends that government may then deem too inconvenient, inexpedient, merely embarrassing, or even illicit to ever expose to the light of day.[310]

---

[302] *Id.* According to Doe, he asked the FBI agent whether he could contact an attorney. The agent states, in contrast, that he was informed that Doe would be consulting a lawyer. *Id.*

[303] *Id.*

[304] "[R]eady availability of judicial process to pursue such a challenge is necessary to vindicate important rights guaranteed by the Constitution or by statute." *Id.* at 475. The court also held that, as applied, the demand that ISPs produce customer records potentially infringed citizens' First Amendment rights of anonymous speech and association. *Id.* at 506.

[305] *Id.* at 502. Note, however, that the citation used by the court in the case is inaccurate: footnote 145 refers to a letter from July 26, 2002.

[306] *Id.* at 504.

[307] *Id.* at 511.

[308] *Id.* at 516; *s*ee also *id.* at 511-16 for the court's discussion.

[309] *Id.* at 519.

[310] *Id.* at 520.

The court concluded, "[a]t that point, secrecy's protective shield may serve not as much to secure a safe country as simply to save face.[311]

In the second case, FBI agents served George Christian, who managed thirty-six Connecticut libraries' digital records, with an NSL.[312] The document demanded "all subscriber information, billing information and access logs of any person" using a particular computer at one of the branches.[313] Like the plaintiff in the earlier lawsuit, Christian refused to provide the FBI with the records.[314] Instead, his employer, Library Connection Inc., brought suit.[315]

Once again, the case turned on the gag order. Christian claimed that it amounted to a prior restraint, which caused irreparable harm—it made it impossible for him to participate in the public debate surrounding the introduction of no less than eight bills before Congress that were aimed at further tailoring NSL powers.[316]

The district court granted the preliminary injunction against the Government to prevent the gag order from going into effect.[317] The court reasoned that it looked like Christian had a high likelihood of success on the merits, and irreparable harm would be created by him not being able to participate in the dialogue.[318] As a content-based prior restraint, the order had to pass strict scrutiny.[319] But while the state had a general interest in national security, no specific harm would be caused by revealing Christian's identity.[320] The district court concluded, "[e]specially in a situation like the instant one, where the statute provides no judicial review of the NSL or the need for its non-disclosure provision . . . the permanent gag provision . . . is not narrowly drawn to serve the government's broadly claimed compelling interest of keeping investigations secret."[321] The court considered the measure "overbroad as applied with regard to the types of information that it encompasses."[322]

---

[311] *Id.*

[312] Gellman, *supra* note 292, at A1.

[313] Doe v. Gonzales, 386 F. Supp. 2d 66, 70 (D. Conn. 2005).

[314] *Id.*

[315] Gellman, *supra* note 292, at A1.

[316] Doe v. Gonzales, 126 S. Ct. 1, 3 (2005).

[317] *Id.* at 3.

[318] *Id.* at 2.

[319] *Id.*

[320] *Id.*

[321] *Id.* (quoting Emergency Application to Vacate Stay, Doe v. Gonzales (D. Conn.) at 22-23 [hereinafter Emergency]).

[322] *Id.* (quoting Emergency, *supra* note 321, at 23). The court found the ban "particularly noteworthy" in light of the fact that proponents of the Patriot Act have "consistently relied

A panel of the Second Circuit reversed the district court's decision and granted the motion to stay the injunction, pending an emergency appeal.[323] Justice Ginsburg, who sat as Circuit Judge for the appeal, refused to hold that vacatur of stay was warranted.[324] She noted the speed with which the case was going through the Court of Appeals and recognized that the ALA, of which the entity in question was a member, was free to note in its lobbying efforts that one of its member had been served with NSL.[325]

As perhaps suggested by the number of NSL-related bills circulating in 2005, the effort to expand national security letter authority did not stop with the USA PATRIOT Act. Neither that statute nor the 1986 ECPA imposed penalties for refusal to cooperate. In 2003, the DOJ prepared to close this loophole. Section 129 of the leaked draft "Enhancing Domestic Security Act"—colloquially known as USA PATRIOT II—provided for criminal penalties.[326] Although leading Republicans and Democrats in Congress immediately condemned PATRIOT II, in September 2004, Representative Sensenbrenner introduced the "Anti-terrorism Intelligence Tools Improvement Act of 2003." This bill provided for up to five years in prison for a violation of the gag orders.[327] The session closed before the bill passed.[328] But in March 2006, the Administration managed to incorporate a penalty of up to five years' imprisonment and/or a fine, into the USA PATRIOT Act renewal statute.[329]

---

on the public's faith [that the Government will] apply the statute narrowly . . . ." *Id.* (quoting Emergency, *supra* note 321, at 26 (quoting Attorney General John Ashcroft, Remarks at Memphis, Tenn.: Protecting Life and Liberty (Sept. 18, 2003), *available at* http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm (characterizing as "hysteria" fears of the Executive's abuse of the increased access to library records under the Patriot Act and stating that "the Department of Justice has neither the staffing, the time[,] nor the inclination to monitor the reading habits of Americans. No offense to the American Library Association, but we just don't care."))).

[323] *Id.* at 1.

[324] *See id.*

[325] *Id.* at 4-5.

[326] U.S. Dep't of Justice, Domestic Security Enhancement Act of 2003, Section by Section Analysis (Jan. 9, 2003) (unpublished internal memorandum) *available at* http://www.publicintegrity.org/docs/PatriotAct/story_01_020703_doc_1.pdf.

[327] *Anti-Terrorism Intelligence Tools Improvement Act of 2003: Hearing on HR 3179 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 108th Cong. (2004), *available at* http://thomas.loc.gov/cgi-bin/bdquery/z?d108:HR03179:@@@L&summ2=m&.

[328] *See* Anti-Terrorism Intelligence Improvement Act of 2003, H.R. 3179, 108th Cong, *available at* http://www.govtrack.us/congress/bill.xpd?bill=h108-3179.

[329] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 117, 120 Stat. 192 (2006).

One month after President Bush signed the USA PATRIOT Act, the DOJ constructed a new interpretation of the United States Code: where before NSLs could only be used in a formal investigation, they now could be used in preliminary inquiries.[330] The "certification" process, meant to provide a check on the use of these powers, became a rubber stamp: the DOJ provided all field offices with a boilerplate paragraph to be inserted into all NSLs at paragraph two.[331] The language, drafted in Washington, D.C., ensured that the proper requirements for certification would be met, regardless of the actual state of the inquiry or investigation being conducted by the field office.[332] DOJ also instructed the field offices not to include a date range for credit record requests, "because these requests seek all records where the consumer maintains or has maintained an account."[333] The Attorney General granted more than five dozen supervisors the authority to issue NSLs.

Most notable in the expansion of powers, in December 2003, the Bush Administration quietly signed the Intelligence Authorization Act for Fiscal Year 2004 into law.[334] The legislation included one sentence that modified a section of the 1978 Right to Financial Privacy Act. The language was almost inscrutable.[335] The net effect was to allow the FBI to issue NSLs in a domain where previously only Treasury and Intelligence agents could go. Moreover, it empowered all of these agencies to issue NSLs to an even broader range of institutions. The obscure cross-reference in the text to "section 5312 of title 31" means that NSLs can now be issued to banks, credit unions, thrift stores, brokers in securities or commodities, currency exchanges, insurance companies, credit card companies, dealers in precious metals, stones, or jewels, pawnbrokers, loan or finance companies, travel

---

[330] FBI Memorandum, supra note 279, at 2.

[331] *Id.*

[332] *Id.* at 5.

[333] *Id.*

[334] Intelligence Authorization Act for Fiscal Year 2004, Pub. L. No. 108-177, § 374, 117 Stat. 2599 (2003) (codified as amended at 12 U.S.C. § 3414 (2000 & Supp. 2001)) [hereinafter Intelligence Authorization Act]; *see also* Kim Zetter, *Bush Grabs New Power for FBI*, WIRED NEWS, Jan. 6, 2004, *available at* http://www.wired.com/news/privacy/0,1848,61792,00.html.

[335] *See* Intelligence Authorization Act, *supra* note 334:

> For purposes of this section, and sections 1115 and 1117 insofar as they relate to the operation of this section, the term 'financial institution' has the same meaning as in subsections (a)(2) and (c)(1) of section 5312 of title 31, United States Code, except that, for purposes of this section, such term shall include only such a financial institution any part of which is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.

Id. § 374(d).

agencies, any business that transfers funds, telegraph companies, car, airplane, and boat sellers, real estate agents, the United States Postal Service, state and local government entities involved in the preceding, and casinos.[336] Like the NSLs to electronic communications service providers, a gag order prevents these entities from revealing that they have received a demand for information.

When the House of Representatives passed the first version of its renewal bill, Sensenbrenner argued against using temporary provisions any further, claiming that there was no evidence that the powers had been abused, and asserting that they had been subjected to "vigorous oversight."[337] Yet efforts by minority members of the Senate Intelligence Committee to obtain hearings on the use of surveillance authorities—including the state of NSLs—had met with little success.[338] Setting aside for a moment the issues raised by having the same party control both the Executive and the Legislature, the USA PATRIOT Act contained minimal requirements for congressional oversight.

The 2006 renewal statute partially addressed this deficiency. For NSLs, it requires the Attorney General to submit an aggregate report to Congress each April, laying out the total number of NSLs made by the DOJ.[339] It also requires the Inspector General of the DOJ to audit "the effectiveness and use, including any improper or illegal use" of NSLs issued by DOJ.[340] This includes: (a) reviewing the NSLs issued from 2003 to 2006; (b) a description of any "noteworthy facts or circumstances" (such as the illegal use of the power); (c) an evaluation of how useful NSLs are as an investigative tool; (d) an examination of how the information is collected, retained, and analyzed by DOJ and others; and, (e) an examination of how such information is used.[341] The report, which is to be unclassified but can contain a classified annex, is to be submitted within a year to the Judiciary Committees and Select Committees on Intelligence in House and Senate.[342] The statute also requires the Attorney General and Director of National Intelligence to submit a joint report on the feasibility

---

[336] *See* 35 U.S.C. § 5312.

[337] *House Approves*, *supra* note 236.

[338] Interview with Sen. Ron Wyden, at Stanford Law School, in Palo Alto, Cal. (Feb. 17, 2006).

[339] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 118, 120 Stat. 192 (2006).

[340] *Id.* § 119.

[341] *Id*.

[342] *Id.* §§ 119-20.

of applying minimization procedures to protect constitutional rights of U.S. persons.[343]

The renewal act provided some other protections, such as exempting libraries that function as traditional book lenders and offer Internet access from being served with NSLs, allowing the appeal of gag orders, and not requiring that the recipient of the NSL provide the FBI with the name of any attorney consulted about the search.[344] Despite these welcome provisions, the broader power to collect massive amounts of information on citizens remains. Minimal restrictions are placed on who sees the information, how long it is kept, and the purposes to which it is directed. And a classified annex means that substantial amounts of information may still be kept secret from public scrutiny. The renewal act, moreover, provides for a one-year delay before a gag order can be appealed.[345]

D. WEAKENING OF THE ATTORNEY GENERAL GUIDELINES

As the above section demonstrates, despite the history of broad executive use of surveillance authority, and the strictures introduced in the 1970s to try to protect privacy and limit use of these powers, subsequent legislation expanded the executive branch's ability to obtain citizens' private information. A similar story accompanies the administrative procedures adopted to implement statutory measures.

The onslaught began as soon as the Attorney General revised the guidelines to reflect concerns raised in the course of the Church Committee hearings. Pointing to the tendency of organizations to go dormant, before again becoming violent, one Special Agent in Charge argued "that provisions for such activity should be made in the Attorney General's guidelines to cover such situations prior to violent and/or detrimental reactivations of such organizations."[346] In 1982, FBI Director William Webster announced during Senate hearings that the DOJ would be reviewing the guidelines to take account of the fact that some "terrorist groups" were "no different from other criminal enterprises."[347] The following year Attorney General William French Smith weakened the Levi

---

[343] *Id.* § 120.

[344] James Kuhnhenn, *Patriot Act renewal clears hurdle in Senate*, MERCURY NEWS.COM, Feb. 16, 2006, http://www.mercurynews.com/mld/mercurynews/news/politics/13890847.htm.

[345] USA PATRIOT Improvement and Reauthorization Act § 115.

[346] Theoharis, *supra* note 131, at 890 (citing Memorandum from SAC, Pittsburgh to William Webster, FBI Dir., FBI 100-56839-293 (Mar. 14, 1979)).

[347] *Id.* at 890 (quoting *Rules on FBI's surveillance of Political Groups to Change*, N.Y. TIMES, June 25, 1982, at B14 (quoting FBI Dir. William Webster)).

guidelines by eliminating probable cause. Instead, surveillance could follow whenever there was a "reasonable indication" of criminal activity.[348] Smith also broadened the provision to allow for a "limited preliminary inquiry." This category collapsed the preliminary and limited investigatory divisions established by Levi, with the effect of allowing all investigatory techniques—short of wiretaps, mail opening, and the gathering of envelope information—in the preliminary stage.[349] Smith doubled the length of time the Bureau could conduct such investigations (from 90 days to 180 days), with authorization available for further extensions. Smith did not require that the Bureau give notice in writing to DOJ, nor did agents need to obtain direct authorization. Instead, the attorney general "may, as he deems necessary, request the FBI to prepare a report on the status of the investigation."[350]

In 1989, Attorney General Richard Thornburgh made minor amendments to the guidelines, expanding them slightly. On Attorney General Janet Reno's watch, although the text did not change after the Oklahoma City bombing, FBI Director Louis Freeh announced that he would interpret the guidelines more expansively.[351] The practical effect meant that while, in the past, the FBI had been reluctant to go after groups that advocated violence unless there was some indication an imminent threat existed, agents could now initiate investigations where groups advocated violence for political or social ends, if agents determined that the organizations had the *ability* to carry out the threats.

Following the attacks of 9/11, Attorney General Ashcroft overhauled the guidelines. He issued two documents. The first, as previously discussed, eliminated the wall between prosecution and intelligence investigations. Either side could act to initiate, operate, continue, or expand FISA searches or surveillance. The second gave the FBI the authority to enter anywhere open to public (which includes surfing the Internet, attending religious gatherings, and taking notes at political meetings) to obtain data that *may* be relevant to criminal activity.[352] It did not require

---

[348] OFFICE OF LEGAL POLICY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/TERRORISM INVESTIGATIONS, *reprinted in FBI Domestic Security Guidelines: Oversight Hearing Before the H. Comm. on the Judiciary,* 98th Cong. 67, 79 (1983).

[349] See, for example, the discussions at EPIC Attorney General's Guidelines Page. http://www.epic.org/privacy/fbi/ (last visited June 9, 2006).

[350] Theoharis, *supra* note 131, at 890-91 (quoting *Attorney General's Guidelines on Domestic Security/Terrorism Investigations*, 32 CRIM. L. REP. (BNA) 3092 (1983)).

[351] *Terrorism Hearings Before the Subcomm. On Crime of the H. Comm. on Int'l Relations*, 104th Cong. (1995) (testimony of FBI Dir., Louis Freeh).

[352] OFFICE OF LEGAL POLICY, U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S

suspicion of actual criminal or terrorist activity.[353] This allowed for what one commentator referred to as the "routine mining of commercial databases for personal information," without any limits on with whom or to what extent this information could be shared.[354]

Ashcroft's memo essentially collapsed the different stages of an investigation. Where before agents would have to check leads, then conduct a preliminary investigation, and, if enough evidence emerged, then move to open a full investigation, from June 2002 on, agents could rapidly move to the third stage.[355] The guidelines gave the Special Agent in Charge the authority to initiate and renew investigations, so long as notification was sent to headquarters.[356] Perhaps the most startling aspect of the new guidelines is that they *require* the FBI to maintain a database of all investigations.[357] This information can be shared with the DOJ, other federal agencies, and state or local criminal justice agencies. The data collection powers are particularly strong where terrorism is concerned.[358]

As in the Vietnam era, the FBI appears to be using these powers to place anti-war demonstrators under surveillance. According to the *New York Times*, the Bureau is amassing "extensive information on the tactics, training and organization of antiwar demonstrators." The FBI defends its position, claiming it is simply trying to identify "anarchists and 'extremist elements'"—not monitor "the political speech of law-abiding protesters."[359] Yet during anti-war protests in New York City, questionnaires used by the police included queries on political party affiliation, voting record, and view of the President. In 2005, a Freedom of Information Act ("FOIA") suit filed by the ACLU revealed that the FBI has expanded its surveillance to environmental and political organizations. The ACLU, Greenpeace, and other civil groups have been the target of Bureau surveillance.[360]

GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS 6 (2002), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf [hereinafter AG TERRORISM GUIDELINES].

[353] Swire, *supra* note 263, at 1355.

[354] *Id*.

[355] AG TERRORISM GUIDELINES, *supra* note 352, at 2.

[356] *Id.* at 19.

[357] *Id.* at 21.

[358] *Id.* at 21-22.

[359] Eric Lichtblau, *FBI Scrutinizes Antiwar Rallies; Officials Say Effort Aims at 'Extremist Elements,'* N.Y. TIMES, Nov 23, 2003, at 1.

[360] Editorial, *FBI Files Are Chilling*, CONTRA COSTA TIMES, July 22, 2005.

E. SURVEILLANCE OPERATIONS

As was previously noted, the National Security Agency's surveillance program is not the only NSA project in this realm—nor, in this regard, is the NSA unique amongst federal entities. Many of these operations capture U.S. persons in their remit—outside the contours of either the Fourth amendment or FISA.[361] One critical difference between them and the programs uncovered by the Church Committee is that the amount of information that can now be amassed far exceeds that of the mid-20th century—at a fraction of the effort previously required (if such data could have been obtained at all).

Perhaps one of the most significant developments in this area is the increasing involvement of the Department of Defense in domestic surveillance. This section briefly discusses DOD's Counterintelligence Field Activity. It also touches on Echelon, a relic of the cold war that NSA continues to run, and Carnivore/DCS 1000, and Magic Lantern, projects initiated by the FBI. It concludes with a short examination of federal watch lists and, despite congressional objection, continued executive branch development of informer systems.

1. Counterintelligence Field Activity

In June 2004, ten activists went to Halliburton to protest the firm's "war profiteering"—charging too much for food distributed to U.S. troops in Iraq.[362] The protesters wore papier-mâché masks and handed out peanut butter and jelly sandwiches to employees.[363] Just over a year previously, the Deputy Secretary of Defense, Paul Wolfowitz, had authorized the creation of the Threat and Local Observation Notice ("TALON") program—"to capture non-validated domestic threat information, flow that information to analysts, and incorporate it into the DOD terrorism threat

---

[361] One suit working its way through the courts, for instance, alleges that the NSA intercepted client-attorney discussions between two citizens in Washington and the director of a Muslim charity, who at the time was in Saudi Arabia. *See* Carol D. Leonnig & Mary Beth Sheridan, *Saudi Group Alleges Wiretapping by U.S.: Defunct Charity's Suit Details Eavesdropping*, WASH. POST, Mar. 2, 2006, at A1; s*ee also NSA III: Wartime Executive Powers and the FISA Court: Hearings Before the S. Judiciary Comm.*, 109th Cong. (2006); Charles Babington & Dan Eggen, *Gonzales Seeks to Clarify Testimony on Spying: Extent of Eavesdropping May Go Beyond NSA Work*, WASH. POST, Mar. 1, 2006, at A8, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/02/28/AR2006022801587.html.

[362] Michael Isikoff, *The Other Big Brother*, NEWSWEEK.COM, Jan. 30, 2006, http://www.msnbc.msn.com/id/10965509/site/newsweek/.

[363] *Id.*

warning process."[364] The peanut butter incident made its way into a TALON report. And like all TALON reports, the information was forwarded to Counterintelligence Field Activity ("CIFA")—a post-9/11 Pentagon creation charged with putting such data in a central database and sharing it with the Defense Intelligence Agency ("DIA"), the Joint Intelligence Task Force Combating Terrorism, and others.[365]

TALON, which grew out of Operation Eagle Eyes (a sort of military neighborhood-watch program discussed below), gathers information from "concerned citizens and military members regarding suspicious incidents."[366] The reports are not validated and "may or may not be related to an actual threat."[367] They focus on non-specific threats to DOD interests: suspected surveillance of DOD facilities and personnel, tests of security, unusual repetitive activity, bomb threats, or any other suspicious activity or incident "reasonably believed to be related to terrorist activity directed against DoD personnel, property, and activities within the United States."[368] In his May 2003 Memo establishing the program, Wolfowitz made it clear that rapid reporting mattered more than careful detail. He supplied a list of the types of information to be included—amongst other items, the date, location, criteria for inclusion, classification level, source and assessment of credibility, and details of the act in question—who, what, when, where, why, and how.[369]

TALON and CIFA illustrate the military's movement into the domestic surveillance realm. But they are not the only such initiatives, and they stem from a broader, more far-reaching re-orientation of the military to domestic affairs. Following 9/11, the Bush Administration pronounced the continental United States a military theater.[370] The Pentagon created

---

[364] Memorandum from Paul Wolfowitz, Deputy Sec'y of Def., to the Secretaries of the Military Dep'ts, Chairman of the Joint Chiefs of Staff, Under Sec'ys of Def., Assistant Sec'ys of Def., Gen. Counsel of the Dep't of Def., Inspector Gen. of the Dep't of Def., Assistants to the Sec'y of Def., Dirs. of the Def. Agencies, and Dirs. of the Dep't of Def. Field Activities, Collection, Reporting, and Analysis of Terrorist Threats to DOD within the United States (May 2, 2003), *available at* http://blogs.washingtonpost.com/earlywarning/files/depsecdef_memo_on_talon_terrorist_reporting_may_2003p.pdf [hereinafter Wolfowitz Memo].

[365] *Id.* The name of the database is CORNERSTONE. Letter from Robert W. Rogalski, Deputy Under Secretary of Def. (Counterintelligence and Sec.) to the Hon. John Warner, Chairman, Comm. on Armed Serv., Jan. 27, 2006, *available at* http://www.sldn.org/binary-data/SLDN_ARTICLES/pdf_file/2859.pdf.

[366] Wolfowitz Memo, *supra* note 364, at 1.

[367] *Id.*

[368] *Id.* at 2.

[369] *Id.* at 3.

[370] Robert Block & Jay Solomon, *Neighborhood Watch; Pentagon Steps Up Intelligence Efforts Inside U.S. Borders*, WALL ST. J. ONLINE, Apr. 27, 2006,

Northern Command ("Northcom").[371] Based in Colorado Springs, Northcom maintains intelligence centers in Colorado and Texas—where the military analyzes data from CIFA, the FBI, and other domestic agencies.[372] The 290 intelligence agents that staff these centers outnumber both the number of people at the State Department's Bureau of Intelligence and Research, and the number of intelligence agents at the Department of Homeland Security ("DHS")[373]—whose job it is to protect the homeland.

According to the Deputy Chief of Staff for Intelligence, Robert W. Noonan, military intelligence agents not only are allowed to collect information about U.S. persons, but can "receive" any information "from anyone, anytime." Noonan wrote in his November 2001 memo that the enemy moves in "a shadowy underworld operating globally with supporters and allies in many countries, including, unfortunately our own."[374] Military intelligence would "play a pivotal role in helping to defeat" the terrorist threat. He continued, "[c]ontrary to popular belief, there is no absolute ban on intelligence components collecting U.S. person information."[375] Noonan expressed concern about reports that had reached his staff, where military intelligence ("MI") personnel had declined "to receive reports from local law enforcement authorities, solely because" they contained such information. He hastened to reassure the agents, noting that not only could they receive the data—"[r]emember, merely receiving information does not constitute 'collection' . . . collection entails receiving 'for use'"—and retain it where it related to foreign intelligence and counterintelligence, but MI could transmit or deliver the information to others.[376]

In January 2002, an official from the Army Inspector General's office, Michael Varhola, again raised the issue in a professional circular. He complained, "unfortunately some individuals find it easier or safer to avoid the issue altogether by simply not collecting the data on citizens they may need to do their complete jobs."[377] By February 2002, Wolfowitz had created CIFA to coordinate military intelligence.[378]

---

http://www.nps.edu/News/ReadNews.aspx?id=2487&role=pao&area=media.

[371] Walter Pincus, *Pentagon Expanding its Domestic Surveillance Activity: Fears of Post-9/11 Terrorism Spur Proposals for New Powers*, WASH. POST, Nov. 27, 2005, at A6.

[372] *Id.*

[373] *Id.*

[374] Memorandum from Robert W. Noonan, Jr., Lieutenant Gen., GS, Deputy Chief of Staff for Intelligence, Dep't of the Army, on Collecting Information on U.S. persons (Nov. 5, 2001), *available at* http://www.fas.org/irp/agency/army/uspersons.html.

[375] *Id.*

[376] *Id.*

[377] Block & Solomon, *supra* note 370.

[378] *Id.*

Military domestic surveillance initiatives did not stop there.[379] CIFA, intended as a clearinghouse for information from other organizations, took on a broader role.[380] It is said now to have more than one thousand employees (although its capacity and budget remain classified).[381] CIFA's mission has become to "transform" counterintelligence by "fully utilizing 21st century tools and resources."[382] The Pentagon boasts that the program uses "leading edge information technologies and data harvesting," and exploits "commercial data"—this means contracting with White Oak Technologies, MZM, and other companies to collect information. CIFA, considers counterintelligence to include not just data collection, but also activities that "protect DoD and the nation against espionage, other intelligence activities, sabotage, assassinations, and terrorist activities . . . ."[383] Their motto is reported to be "Counterintelligence 'to the Edge.'"[384]

While the full extent of information being gathered remains cloaked from the public eye, in late 2005 and early 2006 some details emerged. In Florida, for instance, a TALON report was filed when fewer than two dozen people protested outside a military recruiting office at the local mall.[385] The librarian who organized the event seemed surprised that the gathering, at which a "Bush Lied" sign was displayed, presented a national security threat.[386]

A Freedom of Information Act request submitted by Service members Legal Defense Network also yielded documents in April 2006 showing TALON reports filed on lesbian, gay, bisexual, and transvestite ("LGBT") student groups opposed to the military's "Don't Ask, Don't Tell" policy.[387]

---

[379] In 2004, for instance, the Marine Corps expanded its domestic intelligence gathering; it now oversees the "collection, retention and dissemination of information concerning U.S. persons" (as stated in the April 2004 order approving the program). Pincus, *supra* note 371. The order suggests that Marine Intelligence will be "increasingly required to perform domestic missions . . . as a result, there will be increased instances whereby Marine intelligence activities may come across information regarding U.S. persons." *Id.* (quoting the April 2004 order).

[380] Mark Hosenball, *America's Secret Police? Intelligence Experts Warn that a Proposal to Merge Two Pentagon Units Could Create an Ominous New Agency*, NEWSWEEK.COM, Apr. 14, 2006, http://www.msnbc.msn.com/id/12290187/site/newsweek/.

[381] Pincus, *supra* note 371, at A6; *see also* Walter Pincus, *Defense Facilities Pass Along Reports of Suspicious Activity*, WASH. POST, Dec. 11, 2005, at A12 (discussing CIFA's expanded remit).

[382] Pincus, *supra* note 371, at A6 (quoting CIFA brochure).

[383] *Id.*

[384] Isikoff, *supra* note 362.

[385] *Id.*

[386] *Id.*

[387] TALON Report 902-03-02-05-071_full_text, Feb. 3, 2005, at 1, *available at* http://www.sldn.org/binary-data/SLDN_ARTICLES/pdf_file/2859.pdf.

One group, New York University's OUTlaw—a decades-old student organization found at law schools throughout the United States—attracted attention in part because of the nomenclature.[388] The agent filing the TALON report, unaware that the name referred to the intersection between coming out and legal issues, wrote, "the term 'outlaw' is not defined in the posting . . . the term 'outlaw' is a backhanded way of saying it's all right to commit possible violence and serve as vigilantes during the symposium. Therefore, it is possible that physical harm or vandalism could occur at this event."[389] A later update to the file noted that the term might "refer to members of the gay community that are now 'out' in the open that are studying at law schools." It continued, "[h]owever, per the original source there is almost nothing about the term 'outlaws' available with conventional Internet search engine . . . the source believes there is still a potential for confrontation at NYU."[390] This claim appears somewhat extraordinary: at the time of writing, a Google search for "outlaw law schools" yields more than 1.5 million hits in 0.53 seconds. Admittedly, fourteen months have elapsed since the original TALON report—and some portion of the hits are not directly on point for Outlaw groups at law schools. But it seems at least unlikely that enough references did not grace the Internet at the time for an intelligence officer to ascertain the nature of the NYU student group's activities.

These are not the only activities that are rather far afield from terrorist threats to make their way to CIFA. NBC reported on December 13, 2005, that of approximately fifteen hundred "suspicious incidents" included in a sample of TALON database entries from July 2004 to May 2005, some four dozen focused on anti-war meetings and protests, and opposition to military recruiting. [391]

In January 2006, Paul Wolfowitz acknowledged in a memo that DOD may have obtained and retained information on U.S. citizens that it ought not to have.[392] Stephen A. Cambone, the Undersecretary of Defense,

---

[388] *Id.* at 11-12.

[389] *Id.*

[390] *Id.* at 13 ; *see also* TALON Report 902-22-04-05-358_full_text.txt, Apr. 21, 2005, at 2, *available at* http://www.sldn.org/binary-data/SLDN_ARTICLES/pdf_file/2859.pdf. In February, the ACLU filed a FOIA on behalf of the American Friends Service Committee, Greenpeace, United for Peace and Justice, and Veterans for Peace. *See* National Pentagon Freedom of Information Act Request by the ACLU (Feb. 1, 2006), *available at* http://www.aclu.org/safefree/spyfiles/24021lgl20060201.html.

[391] Walter Pincus, *Pentagon Will Review Database on U.S. Citizens: Protests Among Acts Labeled 'Suspicious'*, WASH. POST, Dec. 15, 2005, at A1.

[392] Isikoff, *supra* note 362.

ordered a formal review.[393] The assessment determined CIFA did indeed have data that violated regulations—specifically, a ban on retaining information on U.S. citizens more than ninety days, unless it was "reasonably believed" to be linked to terrorism, criminal wrongdoing, or foreign intelligence.[394] In January 2006, Deputy Defense Secretary Gordon England issued a memo, ordering that CIFA "purge such information from its files" and recommending refresher training courses on the regulations.[395]

Yet, efforts to expand CIFA's purview continue. CIFA has allegedly contracted with Computer Sciences Corporation to buy "identity masking" software, enabling it to create false web sites.[396] Towards the end of 2005, a Presidential commission on intelligence suggested that CIFA be empowered to conduct domestic criminal investigations as well as clandestine operations.[397] Its law enforcement authorities would extend to crimes such as treason, espionage, and terrorism.[398] The commission found that such an expansion would not require any congressional approval; rather, a Presidential order and Pentagon directive would be sufficient to provide the requisite authority.[399] The 2006 Intelligence Authorization Bill included a provision that would allow the FBI, with the approval of the Director of National Intelligence, to share information with the Pentagon and CIA.[400] (The Pentagon, for now, must report such information exchanges to Congress.[401]) And now rumors are circulating about the possible merger of CIFA and the Defense Security Service, an entity that holds the data generated by background checks on defense contractors and their employees.[402]

An important aspect of these programs, and the military's movement to this realm, is the relative lack of attention paid to it: while the NSA's apparently more limited domestic surveillance program has been the subject of at least four congressional hearings, neither the Senate nor the House has conducted an inquiry into DOD's changing domestic surveillance role.[403]

---

[393] Pincus, *supra* note 391, at A1.

[394] Isikoff, *supra* note 362.

[395] *Id.*

[396] *Id.*

[397] Pincus, *supra* note 371, at A6.

[398] *Id.*

[399] *Id.*

[400] *Id.*

[401] *Id.*

[402] Hosenball, *supra* note 380.

[403] Pincus, *supra* note 391, at A1. For hearings on the NSA program see, e.g., *An Examination of the Call to Censure the President: Hearing Before the S. Judiciary Comm.*, 109th Cong. (2006); *NSA III*, *supra* note 361; *Wartime Executive Power and the NSA's*

The full extent of the program has yet to be made public: setting aside the content for the moment, even the *number* of annual TALON reports is classified.[404] Yet the intrusion on individual privacy may be significant: according to the inspector general's newsletter, for instance, just one military service taking part in this program—the Air Force—generated 1,200 reports during the fourteen months that ended September 2003.[405]

2. Echelon

The NSA's domestic surveillance effort that has attracted so much attention of late is not the only NSA project underway. Echelon, a relic of the Cold War, scans telecommunications traffic for key words and phrases, recording the content of related conversations. The project began with a 1947 agreement between the United States and United Kingdom. Its existence finally reached the public domain in the 1980s, when Margaret Newsham, having overheard United States Senator Strom Thurmond while listening to his conversations at the Menwith Hill facility in England, appeared before Congress.[406] The countries party to the agreement continued to deny Echelon's existence until the late 20th and early 21st century.[407] Around this time, the European Union Parliament's Scientific and Technical Options Assessment Program Office issued two reports: *An Appraisal of Technologies of Political Control* and *Interception Capabilities 2000*.[408] Both referred to Echelon and raised the somewhat awkward issue of economic espionage.[409] The program now includes

---

Surveillance Authority II: Hearing Before the S. Judiciary Comm., 109th Cong. (2006); *Wartime Executive Power and the NSA's Surveillance Authority: Hearing Before the S. Judiciary Comm.*, 109th Cong. (2006).

[404] Pincus, *supra* note 391, at A1.

[405] Pincus, *supra* note 381, at A12.

[406] Duncan Campbell, *Somebody's Listening*, NEW STATESMAN, Aug. 12, 1988, at 10-12, *available at* http://cryptome.sabotage.org/echelon-dc.htm; *see also* David Wood, The Hidden Geography of Transnational Surveillance: Social and Technological Networks Around Signals Intelligence Sites (Dec. 21, 2000) (unpublished Ph.D. dissertation, University of Newcastle), *available at* http://www.staff.ncl.ac.uk/d.f.j.wood/thesis.htm.

[407] Jeffrey Richelson, *Desperately Seeking Signals: "Echelon" May Be Worrisome, But It's not the All-absorbing Big Ear that Some People Think*, BULL. OF THE ATOMIC SCIENTISTS, Mar./Apr. 2000, at 47, *available at* http://www.thebulletin.org/article.php?art_ofn=ma00richelson.

[408] *See* DUNCAN CAMPBELL, IPTV LTD., INTERCEPTION CAPABILITIES 2000 (1999) *available at* http://www.cyber-rights.org/interception/stoa/ic2kreport.htm; STEVE WRIGHT, OMEGA FOUND., EUROPEAN PARLIAMENT, AN APPRAISAL OF TECHNOLOGIES OF POLITICAL CONTROL (Dick Holdsworth ed. 1998), *available at* http://www.statewatch.org/news/2005/may/steve-wright-stoa-rep.pdf.

[409] Richard Barry, *ECHELON: The Evidence*, ZDNET (U.K.), June 29, 2000, http://news.zdnet.co.uk/story/0,,s2079850,00.html.

GCHQ in the United Kingdom, the Communications Security Establishment ("CSE") in Canada, the Defence Signals Directorate ("DSD") in Australia, and Government Communications Headquarters ("GCSB") in New Zealand.[410]

Twenty-four hours a day, seven days a week, Echelon monitors non-military communications from, to, and within the United States. This means that Internet activity, email, faxes, and telephone transmissions run through its filters. It analyzes more than two million messages per hour and redistributes them to member states for decryption, filtering, and codification.[411] With listening stations around the world, the five member countries submit "dictionaries": lists of key words that flag the system to automatically transcribe the message, give it a code, and forward the intercept to the country that is interested in that subject matter. Officials then further examine the information. "Often, the messages that are red-flagged are nothing more than innocent conversations and do not have substantial merit as threats to national security"—such as a mother relating that her son had "bombed" in a play at school.[412]

The same reluctance that marked Congress' willingness to question NSA between 1973 and 1976 characterizes congressional attitudes towards Echelon. In April 2000, Representative Bob Barr finally managed to hold hearings to find out if American citizens had come under surveillance. Met by NSA stonewalling, the House of Representatives subsequently passed a measure requiring full disclosure. However, the Senate stepped in and amended it, requiring only a confidential report from NSA to the Select Committees on Intelligence.[413] Partly because of this lack of public oversight, the legal framework for Echelon remains less than clear. When Porter Goss, the Republican Chair of the House Permanent Select Committee on Intelligence, asked NSA to provide legal standards, the agency refused.[414] The Intelligence Authorization Act for Fiscal Year 2000

---

[410] Sarah Ferguson, *Overloading Big Brother: 'Hactivists' Try to Short-Circuit the Spooks*, VILL. VOICE, Oct. 20-26, 1999, *available at* http://www.villagevoice.com/issues/9942/ferguson.php; *see also* Richelson, *supra* note 407; Patrick S. Poole, ECHELON: America's Secret Global Surveillance Network, http://home.hiwaay.net/~pspoole/echelon.html (last visited June 9, 2006).

[411] Erin Zimmerman & Dale Hurd, Surveillance Society: Exposing Echelon, Techno Warfare/MACRO-USGOV, Dec. 14, 1999, http://members.tripod.com/~ellis_smith/vwars3.html (last visited June 9, 2006).

[412] Erin L. Brown, Comment, *Echelon: The National Security Agency's Compliance with Applicable Legal Guidelines in Light of the Need for Tighter National Security*, 11 COMMLAW CONSPECTUS 185, 189 n.48 (2003).

[413] H.R. 1555, 106th Cong. (2000).

[414] Richelson, *supra* note 407

required NSA, CIA, and the Attorney General to address the legal standards for the interception of communications when such interception may result in intentional targeting of communications involving U.S. persons.[415]

3. Carnivore/DCS 1000

In July 2000, Neil King of the *Wall Street Journal* revealed another secret, wiretapping operation.[416] Carnivore, introduced in 1999 by the FBI without DOJ approval (or knowledge), monitors ISPs to intercept digital information. The Bureau activates the system "when other implementations (e.g., having an ISP provide the requested data) do not meet the needs of the investigators or the restrictions placed by the court."[417] Carnivore uses hardware, known as a "black box," and software, attached to the ISP's system, to collect email, instant messaging, chat-room discussions, financial transactions, and websites visited.[418] Carnivore/DCS 1000 "chews all the data on the network"—while ostensibly only eating the particular information indicated in a court order.[419] Law enforcement can program it to collect all information to and from specified receivers and senders.

As news of Carnivore hit the proverbial fan, the FBI renamed the system the more innocuous-sounding "DCS 1000."[420] The House and the Senate immediately held hearings to look into the matter, at which the FBI revealed that by September 2000 it had used the system twenty-five to

---

[415] Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, § 309, 113, Stat. 1606, § 1613 (1999). Ostensibly, the legal framework would include the Fourth Amendment requirement of reasonableness and probable cause for search and seizure. If the interceptions fall under FISA, then those structures would apply. Of additional relevance would be Executive Order 12,333, established by President Ronald Reagan in 1981 and dealing with the use of surveillance for national defense. 46 Fed. Reg. 59,941 (1981).

[416] Neil King, Jr., *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3.

[417] STEPHEN P. SMITH ET AL., ILL. INST. OF TECH., CHI.-KENT COLL. OF LAW, INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT viii (2000) (marked DOJ Sensitive; obtained by EPIC in 2004 FOIA request).

[418] Graham B. Smith, Notes and Comments, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L. REV. 481, 492 (2001). Full content communications is collected under 18 U.S.C. §§ 2510-22 (2000) and 50 U.S.C. §§ 1801-29; address information is taken under 18 U.S.C. §§ 3121-27 and 50 U.S.C. §§ 1841-46. The filter works at a rate of forty million megabits per second or faster. *Id.*

[419] Robert Graham, Carnivore FAQ, http://corz.org/public/docs/privacy/carnivore-faq.html (last visited June 9, 2006).

[420] FED. BUREAU OF INVESTIGATION, CARNIVORE/DCS-1000 REPORT TO CONGRESS 1 (2003) [hereinafter FBI CARNIVORE REPORT] (submitted to Judiciary Committees of the United States House of Representatives and United States Senate on Feb. 24, 2003).

thirty-five times.[421] Twenty-eight members of Congress followed with letters to Attorney General Janet Reno, demanding that the program be terminated.[422] Instead, the DOJ suspended it, pending an independent, technical review.[423] When the report concluded that the system was sound, the DOJ reengaged Carnivore.[424] Importantly, though, while the review noted that the information being gathered may exceed the court order initiating the surveillance, it did not address the constitutional issues raised by the operation of the program.

The agency's refusal to disclose more information led to the introduction of Section 305 of the 21st Century Department of Justice Appropriation Authorization Act, which required a report at the end of Fiscal Year 2002 and Fiscal Year 2003 on the operation of the program. In these documents, the FBI announced that it had used DCS 1000 zero times from 2002 to 2003. Instead, the Bureau made use of commercially-available software to undertake surveillance thirteen times during that period.[425] (This number does not include the number of times ISPs used their own software to intercept communications, such as those requested under NSLs.[426])

An Electronic Privacy Information Center ("EPIC") FOIA request in October 2000 yielded 729 pages of information on the system—of which two hundred pages were blank, and another four hundred partially redacted.[427] The FBI, which justifies the system on claims of national security, asserted that it could only be programmed to get specific information. However, as noted by Senator Patrick Leahy and the formal review report, the system lacks procedural safeguards. The FBI determines which emails to obtain, according to classified FBI procedures.

---

[421] *See Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000), *available at* http://commdocs.house.gov/committee/judiciary/hju67305.000/hju67305_0.htm; *Digital Privacy and the FBI's Carnivore Internet Surveillance Program: Hearing Before the S. Comm. on the Judiciary*, 106th Cong. (2000).

[422] Smith, *supra* note 418, at 495.

[423] SMITH ET AL., *supra* note 417.

[424] Smith, *supra* note 418, at 496.

[425] *See* FBI CARNIVORE REPORT, *supra* note 420, at 1.

[426] *See* Kevin Poulsen, *FBI Retires Its Carnivore*, SECURITY FOCUS, Jan. 14, 2005, http://www.securityfocus.com/news/10307.

[427] Peter J. Young, Note, *The Case Against Carnivore: Preventing Law Enforcement from Devouring Privacy*, 35 IND. L. REV. 303, 306 (2001).

4. Magic Lantern

Magic Lantern is an FBI keystroke logging program that does not require physical access to conduct surveillance of an individual's computer use.[428] The software targets a user's system through an email message, with the sender posing as a friend or family member. It is unclear whether the recipient needs to open the attachment or not.[429] The FBI also has the option of hacking a user's computer and placing the program directly on the hard drive. Magic Lantern captures keystrokes and, when the computer hooks up to the Internet, automatically sends the information back to the FBI. Although Magic Lantern might be caught by virus scans, the FBI approached companies that program against viruses and requested that they not target the surveillance device. Some agreed.[430] This program provides the FBI with a way to break the use of encryption by identifying pass phrases used to access information. It also can recreate emails and word documents never printed or sent, as well as other information that was never meant to move beyond the immediate computer. Its primary use is in an intelligence function.

The courts have already addressed the constitutionality of keystroke programs: they determined that a key-logging device, *with a search warrant*, is not a violation of the Fourth Amendment.[431] The court wrote, "we must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes."[432] The government argued in *Scarfo* that the Key Logger System ("KLS") used met Title III requirements: it did not record the user's entry while any modem on the computer was in operation. Similarly, the program did not actively seek out

---

[428] *See* Elinor M. Abreu, *FBI Confirms Magic Lantern Exists*, REUTERS, Dec. 12, 2001, *originally published at* http://www.msnbc.com/news/671981.asp?0si, *currently available at* http://www.commondreams.org/headlines01/1212-07.htm; Alex Salkever, *A Dark Side to the FBI's Magic Lantern*, BUS. WEEK ONLINE, Nov. 27, 2001, http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; Bob Sullivan, *FBI Software Cracks Encryption Wall*, MSNBC, Nov. 20, 2001, http://www.msnbc.com/news/660096.asp?cp1=1; Robert Vamosi, *Commentary, Warning: the FBI Knows What You're Typing*, ZDNET (U.K.), Dec. 4, 2001, http://zdnet.com.com/2100-1107-504142.html; *see also* Christopher Woo & Miranda So, Note, *The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, 15 HARV. J.L. & TECH. 521, 521 (2002).

[429] *See* Sullivan, *supra* note 428.

[430] Woo & So, *supra* note 428, at 524 (citing Carrie Kirby, *Network Associates Mired in Security Debate*, S.F. CHRON., Nov. 28, 2001, at B1).

[431] United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001).

[432] *Id.* at 583.

data already held on the computer. The court denied defense counsel access to the manner in which KLS operated as well as the precise data gained, saying instead that the program "obtained the passphrase to the [suspect] file and retrieved information."[433]

5. Terrorism Information and Prevention System (TIPS)

In January 2002, the DOJ announced plans for the Terrorism Information and Prevention System ("TIPS"). "A national system for concerned workers to report suspicious activity,"[434] the aim was to recruit "millions of American truckers, letter carriers, train conductors, ship captains, utility employees and others" as informers.[435] The pilot program would have required one in every twenty-four Americans living in the largest ten cities to report anything perceived as "unusual or suspicious." For seven months after the announcement, little happened. Then, just weeks before the DOJ was set to launch TIPS, Ritt Goldstein wrote an article in the *Sydney Morning Herald* pointing out that implementation would mean "the US will have a higher percentage of citizen informants than the former East Germany through the infamous Stasi secret police."[436] Some four percent of Americans would report "suspicious activity."[437] The Associated Press picked up the story, and an immediate backlash followed.

A *Boston Globe* editorial led off: "OPERATION TIPS . . . is a scheme that Joseph Stalin would have appreciated."[438] Opposition spanned the ideological divide: in the House of Representatives, Republican majority leader Dick Armey and Representative Bob Barr condemned the program, their resistance matched in the Senate by Democratic Senators Patrick J.

---

[433] *Id.* at 574; *see also* JAMES A. ADAMS, NAT'L INST. FOR TRIAL ADVOCACY, OVERVIEW OF CHAPTER 121. STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS Commentary (2004).

[434] STANLEY, *supra* note 289, at 3.

[435] Operation TIPS web pages have since been removed from the internet, although the original pages from July 16 and Aug. 8, 2002, are available at http://www.thememoryhole.org/policestate/tips-changes.htm (last visited June 9, 2006).

[436] Ritt Goldstein, *U.S. Planning to Recruit One in 24 Americans as Citizen Spies*, SYDNEY MORNING HERALD, July 15, 2002, at 2, *available at* http://www.smh.com.au/articles/2002/07/14/1026185141232.html?oneclick=true.

[437] *Id.*

[438] Editorial, *Ashcroft vs. Americans*, BOSTON GLOBE, July 17, 2002, at 22, *available at* http://http://www.commondreams.org/views02/0717-01.htm; *see also* Editorial, *What is Operation TIPS?*, WASH. POST, July 14, 2002, at B6; Ellen Sorokin, *Planned Volunteer-Informant Corps Elicits '1984' Fears; Accessing Private Homes is Objective of 'Operation TIPS,'* WASH. TIMES, July 16, 2002, at A3, *available at* http://www.commondreams.org/headlines02/0716-01.htm.

Leahy, Edward M. Kennedy, and Charles E. Schumer.[439] The deliberate inclusion of professions with access to private homes, and the apparent intention to use TIPS to build a central data base, caused particular affront. On July 25, Attorney General Ashcroft told the Senate Judiciary Committee that although the FBI and agencies would retain the information, he was not aware of any plans to build a central data base.[440]

Congress, unconvinced, shut down the program: "Any and all activities of the Federal Government to implement the proposed component program of the Citizen Corps known as Operation TIPS (Terrorism Information and Prevention System) are hereby prohibited."[441]

Congress' ban on TIPS turned out to be wishful thinking: although the website disappeared from cyberspace, a plethora of watch programs followed. Marine Watch sprung up in Maine, Ohio, and Michigan.[442] President Bush declared "Coastal Beacon," which coordinated reports of suspicious activity along the shores of Maine, to be "[o]ne of the most innovative TIP [*sic*] programs in the country."[443] DHS, which funded Highway Watch, embraced the more than three million truck drivers integrated into the program as "a potential army of eyes and ears to monitor for security threats," claiming they are "naturally very aware of suspicious activity and behavior." The department added, "truck drivers are everywhere—ports, airports, malls, bridges, tunnels—thus giving greater range to homeland security observation efforts."[444] On March 15, 2004, the Transportation Security Administration ("TSA") announced that another $19.3 million would assist the TSA and American Trucking Associations to expand the operations. The press release stated, "[t]his innovative program combines the training of highway professionals in safety and security awareness with information sharing and analysis networks, to assist in

---

[439] Adam Clymer, *Ashcroft Defends Plan for National Hotline on Terrorism*, N.Y. TIMES, July 25, 2002, *available at* http://www.nytimes.com/2002/07/25/politics/25CND-PRIV.html.

[440] *See, e.g.*, William Matthews, *Ashcroft: No Central Database for Citizen Tips*, FCW.COM, July 29, 2002, http://www.fcw.com/fcw/articles/2002/0729/news-tips-07-29-02.asp.

[441] *See* H.R. REP. 108-2555, §880 (2003) (Conf. Rep.) *available at* http://www.ala.org/ala/oif/ifissues/terrorisminformationprevention.htm.

[442] STANLEY, *supra* note 289, at 5.

[443] Press Release, The White House, President Promotes Citizen Corps for Safer Communities (Apr. 8, 2002), *available at* http://www.whitehouse.gov/news/releases/2002/04/ 20020408-4.html.

[444] Highway Watch Fact Sheet, http://www.highwaywatch.com/press_room/fact_sheets.html (last visited June 9, 2005); *see also* http://www.tmta.com/Resources/News/HighwayWatch.asp (last visited June 9, 2006).

national security and road safety."[445] What makes the expansion—indeed, the very existence—of the Highway Watch system surprising is that the "Operation TIPS Fact Sheet" initially listed it as a TIPS system, making its continuance a violation of Congress' express prohibition.[446]

Proponents of these programs argue that the state has limited resources. Enlisting the help of law-abiding citizens—many of whom are eager to help in some way—would dramatically increase law enforcement's ability to interdict crime. And past successes readily present themselves. For instance, the "Neighborhood Watch" concept has proven effective in stemming ordinary crime.[447] Terrorism, in particular, depends upon surreptitious operations—planning that may easily slip beneath the radar of law enforcement that must focus on a range of different threats. The approach counters the impersonalization created by social mobility and urbanization, returning society to an environment more like the small communities that characterize rural areas.[448] By preventing terrorists from blending into their surroundings, they lose the anonymity critical to their ability to mount attacks. With the potential devastation created by technological advances, it becomes all the more important to try to prevent terrorist attacks.

Those opposed to these programs note the potential for prejudice and abuse imbedded in the requirement that "suspicious activity" be reported. According to Eagle Eyes, for instance, potential terrorists include, "[p]eople who don't seem to belong in the workplace, neighborhood, business establishment or anywhere else . . . people know what looks right and what doesn't look right in their neighborhoods, office spaces, commutes, etc., and if a person just doesn't seem like he or she belongs, there's probably a reason for that."[449] As the *Pentiti* trials in Italy or the Supergrass system in

---

[445] Highway Watch, Transportation Security Administration and the American Trucking Associations Team up to Prevent and Respond to Possible Terrorist Threats, http://www.highwaywatch.com/announcements/tsa.html (last visited June 9, 2006).

[446] STANLEY, *supra* note 289, at 5 n.11.

[447] *See, e.g.*, Neighborhood Crime Watch, Anchorage Police Dep't, http://www.muni.org/apd2/ncw.cfm (last visited June 9, 2006) (extolling the virtues of the Anchorage neighborhood watch program); Neighborhood Watch, City of San Diego, http://www.sandiego.gov/police/prevention/neighwatch.shtml (last visited June 9, 2006) (underscoring the value of the San Diego neighborhood watch program); Neighborhood Watch, Lane County, Or., http://www.co.lane.or.us/NeighborhoodWatch/default.htm (last visited June 9, 2006) (referring to Neighborhood Watch as "a proven crime-reduction program.").

[448] As of 1977, three out of every four Americans lived in cities or surrounding suburbs. *See* PRIVACY PROT. STUDY COMM'N, REPORT: PERSONAL PRIVACY IN AN INFORMATION SOCIETY 1 (1977), *available at* http://www.epic.org/privacy/ppsc1977report/ c1.htm.

[449] U.S. Air Force Office of Special Investigations, Eagle Eyes Program,

Northern Ireland attest, such programs become a way for people to settle old scores—which bear no relation to terrorism.[450] And the lack of controls over what happens to the information—how it is stored, whether and to what extent it is verified, who sees it, how long it is kept, and to what ends it is directed—creates a system that is vulnerable to political abuse.

Even once ordered destroyed, such information may nevertheless haunt those to whom it relates. In the mid-1970s, the Church Committee hearings led to the order to destroy thousands of files held by the Los Angeles Police Department.[451] In 1983, however, it emerged that an LAPD detective had stolen the files and kept them in his garage, making the information available to the Western Goals Foundation.[452] This anti-Communist, Cold War organization circulated the data to local police departments, the Secret Service, FBI, State Department, and CIA.[453] Such systems may quickly take on racial overtones. Moreover, they increase fear and mistrust in society and may have a debilitating affect on social interactions. And free speech bears the burden: the ease with which issues may be discussed both publicly and privately may alter, with a debilitating affect on the democratic process.

TIPS is only one part of the Citizen Corps program handed down by Executive Order in the aftermath of 9/11. The Corps' self-stated goal is "to harness the power of every individual through education, training, and volunteer service to make communities safer, stronger, and better prepared for terrorism . . . ."[454] The Citizens' Preparedness Guide, issued by the USA Freedom Corps, (with a foreword by Ashcroft noting the need to change social behavior in the aftermath of 9/11) urges citizens to "[c]onsider incorporating your place of worship into your Neighborhood Watch programs."[455]

At one extreme, such recommendations contribute to increased suspicion throughout the fabric of social life. At the other, many recommendations appear to have little real impact on terrorism. The guide also recommends, for example, that Americans keep their yards clean and

---

http://public.afosi.amc.af.mil/eagle/index.asp (last visited June 9, 2006).

[450] *See, e.g.*, STEVEN GREER, SUPERGRASSES: A STUDY IN ANTI-TERRORIST LAW ENFORCEMENT IN NORTHERN IRELAND (1995)**.**

[451] STANLEY, *supra* note 288, at 8.

[452] *Id.*

[453] *Id.* at 8-9.

[454] *Id.* at 27.

[455] NAT'L CRIME PREVENTION COUNCIL, UNITED FOR A STRONGER AMERICA: CITIZENS' PREPAREDNESS GUIDE 12 (2002), *available at* http://www.citizencorps.gov/pdf/cpg.pdf.

"[p]rune shrubbery."[456] Citizens are directed to contact law enforcement whenever they see "someone unfamiliar . . . loitering in a parking lot."[457] The guide further urges that, "[w]hen traveling" Americans should "dress conservatively."[458]

6. Watch Lists

As was previously discussed, in the mid-20th century the CIA, FBI, IRS, and NSA all had "watch lists" that carried consequences for American citizens.[459] It was not clear exactly how names got onto each of these lists. The directors of the organizations did not review each name personally. The head of the NSA, Admiral Gaylor, did not even know about the existence of the tabulations until a year after taking office. Instead, the lists were administered at a lower level and agencies circulated names to each other, which the NSA and others simply accepted on the assurance that their inclusion was somehow appropriate.[460]

Once again, the executive branch has begun to construct lists with minimal procedural safeguards. At least twelve exist at a federal level.[461] One of these, what has colloquially come to be considered the "No Fly List," merits brief discussion.

As of September 11, 2001, the federal government maintained sixteen people on a secret "No Transport List"—a total number that, even if names correlated, would have been insufficient to prevent all nineteen hijackers from boarding the planes. By December 2001, this list evolved into two sets of records: the "No Fly List" and the "Selectee List." The first completely barred individuals from flying; the second merely subjected certain people to further security measures. By the following year, these

---

[456] *Id.* at 6.

[457] *Id.* at 18.

[458] *Id.* at 15.

[459] *Church Committee Vol. 5*, *supra* note 98.

[460] *Id.* at 30-33.

[461] U.S. GEN. ACCOUNTING OFFICE, INFORMATION TECHNOLOGY: TERRORIST WATCH LISTS SHOULD BE CONSOLIDATED TO PROMOTE BETTER INTEGRATION AND SHARING 12 (2003), *available at* http://www.gao.gov/new.items/d03322.pdf; *see also Progress in Consolidating Terrorist Watchlists—The Terrorist Screening Center (TSC): Joint Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary and the Subcomm. on Intelligence and Counterterrorism of the H. Select Comm. on Homeland Security*, 108th Cong. 8-13 (2004) (statement of Donna A. Bucella, Dir., Terrorist Screening Ctr., Fed. Bureau of Investigation) (discussing Terrorist Screening Center watchlist derived from Terrorist Threat Integration Center's main database); *Review: 'No-fly list' Lacks Rules, Procedures: Watch List Meant to Stop Terrorists from Flying Is Under Scrutiny*, CNN.com, Oct. 10, 2004, http://www.cnn.com/2004/US/10/10/terror.watch.list/ [hereinafter *Review: 'No-Fly list'*].

two lists combined encompassed more than one thousand names, and by April 2005, some 70,000 names graced the two catalogs.[462] For the program's first two-and-a-half years, however, the FBI and TSA denied its existence.[463]

It was not until prominent anti-war activists, such as Jan Adams and Rebecca Gordon, and political opponents of the Bush Administration, such as Senator Edward Kennedy and civil rights attorney David Cole, found themselves on the list that it began to attract broader public attention.[464] Various prominent Muslim-Americans, such as singer Cat Stevens and Army chaplain James Yee, similarly found themselves singled out, as did two dozen students, chaperoned by a priest and a nun, on their way to a peace teach-in.[465] Documents obtained through an ACLU FOIA request in 2004 demonstrated that even those entering names and administering the list had no idea how everyone had been added.[466] One particularly telling email suggested that the author would not risk flying commercial, because of the haphazard manner in which the list had been assembled and the lack of procedural safeguards or mechanisms to facilitate getting off of it.

Beyond the 70,000 people actually on the lists, anecdotal evidence shows that individuals who share exact or similar names to those on the list also have become caught in the system. In Portland, Oregon, two comedians wrote a song about the plight of anyone named David Nelson:

> They call me David Nelson and my name has been besmirched
>
> When I fly across my country, I will always be strip-searched
>
> Somewhere a David Nelson is allegedly quite mean
>
> And the TSA ain't able to declare my person clean . . .
>
> I missed my flight from Texas and I missed my flight to Spain
>
> You'd think my second cousin was a Tikrit named Hussein

---

[462] *Morning Edition* (Nat'l Pub. Radio radio broadcast, Apr. 26, 2005).

[463] Telephone interview with Thomas R. Burke, Partner, Davis Wright Tremaine LLP, in Palo Alto, Cal. (May 5, 2005).

[464] BOB CUDDY & ANGILEE SHAH, *Jan Adams & Rebecca Gordon*, *in* AM. CIVIL LIBERTIES UNION OF N. CAL., CAUGHT IN THE BACKLASH: STORIES FROM NORTHERN CALIFORNIA (2002), *available at* http://www.aclunc.org/911/backlash/; Sara Kehaulani Goo, *Sen. Kennedy Flagged by No-Fly List*, WASH. POST, Aug. 20, 2004, at A01; Interview with David Cole, Professor of Law, Georgetown Univ. Law Ctr., in Palo Alto, Cal. (Sept. 17, 2005) [hereinafter Interview with Cole].

[465] James Bovard, *The Surveillance State*, AM. CONSERVATIVE, May 19, 2003, at 10; Interview with Cole, *supra* note 464.

[466] *See Review: 'No-fly list,' supra* note 461.

I'm scrutinized and sanitized by security and then

The next time that I fly, they have to do it all again.[467]

In response to a class-action lawsuit filed by people caught in the name game, the TSA created an ombudsperson process. Individuals now can download and print out a Passenger Identity Verification Form and mail it, along with certain notarized documents, to TSA. The organization then decides whether clearance procedures may help to expedite your travel, but it is not required to do anything, nor is any criterion available as to how the decision is made. The process does not remove your name. Rather, it differentiates you from others who may be on the list and saves your personal information, which is then forwarded to the airlines, in another, specially-cleared list.

The No Fly List list overlaps with the Computer Assisted Passenger Screening ("CAPS"), which draws information from a database to determine which individuals ought to be placed under further scrutiny.[468] The idea behind CAPS was to create a "vast air security screening system designed to instantly pull together every passenger's travel history and living arrangements, plus a wealth of other personal and demographic information" in order to "profile passenger activity and intuit obscure clues about potential threats."[469] Airlines would collect and provide the full name, address, phone number, and date of birth of people flying. The broader system would then use "data-mining and predictive software" to determine the degree of risk posed by the individual.[470]

The companies initially signed up to develop prototypes collected the information themselves, which ranged from land records and car ownership to projected income, magazine subscriptions, and telephone numbers.[471] When interviewed on the system, the former acting administrator of the Federal Aviation Administration (and security consultant for the CAPS project) said, "[t]his is not fantasy stuff . . . . This technology, based on

---

[467] ACLU of Northern California, No-Fly Lawsuit Client Biography: David C. Nelson, http://aclunc.org/911/nelson.html (last visited June 9, 2006).

[468] The Federal Aviation Reauthorization Act of 1996 required the FAA to help airlines to develop CAPS as part of its overall security effort. Pub. L. No. 104-264, § 307, 110 Stat. 3213, 3253 (1996).

[469] Robert O'Harrow, Jr., *Intricate Screening of Fliers in Works*, WASH. POST, Feb. 1, 2002, at A1.

[470] *Id.*

[471] *See id.* To accommodate the accumulation of this information, the *Washington Post* reported, "[i]ndustry officials have already discussed with lawmakers the possible need to roll back some privacy protections in the Fair Credit Reporting Act and Driver's Privacy Protection Act to enable them to use more of the credit and driver's-license data." *Id.*

transaction analysis, behavior analysis, gives us a pretty good idea of what's going on in a person's mind."[472] In July 2004, Homeland Security Secretary Tom Ridge announced that CAPS II would be terminated, but other DHS officials said only the name had been retired.[473] Indeed, Secure Flight, the FAA's latest project, bears a striking similarity to the previous project.[474]

The problems with the No Fly List generally, and Secure Flight in particular, loom large. It is not at all clear who runs the lists, how the information gets entered, who verifies it, what the criteria are for inclusion, and how the information subsequently is used. Passengers are not given the opportunity to challenge the relevant data or to confront those accusing them of being associated with terrorist activity. In July 2005, government auditors alleged that Secure Flight held information on 43,000 people who were not suspected of terrorism—in violation of existing privacy laws.[475] Because TSA refuses to comment on the criteria used, it also cannot reveal whether First Amendment activities are being used as a basis for inclusion. The existence of the lists shifts the burden of proof onto anyone wishing to travel. She first has to prove that she is not the individual sought by the state. It also is not clear where the information goes. The Departments of Defense, State, Justice, Transport, and Treasury all run similar watch lists, some of which include biometric and other personal data. Furthermore, much of the information is currently in the hands of private industry.

The combination of these programs and the proliferation of surveillance operations, such as TALON, Echelon and Carnivore, the use of programs such as Magic Lantern, and the operation of widespread informer systems raise concerns about the broader impact of post-9/11 surveillance on the country. The next section discusses how technology has changed the nature of this surveillance, moving the United States from a position of physical or data surveillance into the psychological realm.

F. DATA MINING

Data mining is a technique used to extract information from large amounts of information. The United States operates hundreds of data

---

[472] *Id.* (emphasis added).

[473] Cynthia L. Webb, *Uncle Sam Mothballs Screening Program*, WASH. POST.COM, July 16, 2004, http://www.washingtonpost.com/wp-dyn/articles/A54487-2004Jul16.html.

[474] *Compare* Secure Flight Program: Test Phase: Privacy Impact Assessment, 69 Fed. Reg. 57,352 (Sept. 24, 2004), *with* Privacy Act of 1974: System of Records; Secure Flight Test Records, 69 Fed. Reg. 57,345 (Sept. 24, 2004).

[475] Mark Clayton, *U.S. Plans Massive Data Sweep*, CHRISTIAN SCI. MONITOR, Feb. 9, 2006, *available at* http://www.csmonitor.com/2006/0209/p01s02-uspo.html.

mining operations, more than a dozen of which relate to counterterrorism. The material included in these efforts is not limited to what is gathered through surveillance. On the contrary, it may come from any number of private and public sources. The aim is to use technology to construct a detailed picture of individuals, organizations, and regions.

Such efforts are not new. In 1961, for instance, Santa Clara County developed an alphabetical person index, called LOGIC: Local Government Information Control.[476] The database included citizens' names, any aliases they used, their social security number, their address, birth date, and driver's license number, any vehicles they drove, where they were employed, what their voter and jury status was, and property they owned.[477]

Programs currently in existence, though, are considerably more sophisticated than earlier prototypes. The information revolution means that different, and intensely personal, information can be recorded and traced. Digital technology allows massive amounts of information to be stored—and shared. And new systems process information faster and allow for more complex analysis.

Data mining tools are not singular to counterterrorism. In the private sector, companies use them to manage their customer relationships, conduct market research, and increase supply chain efficiency.[478] The United States government initially wielded them to prevent financial fraud. But after 9/11, data mining emerged as one of the principal tools for the Departments of Defense and Homeland Security to counter the terrorist threat. This section briefly touches on advances in technology and the commodification of information that affect data mining capabilities; it then turns to a discussion of Total Information Awareness and other post-9/11 data mining operations.

1. Advances in Technology and the Commodification of Information

Digitization allows vast amounts of information to be recorded, transferred, analyzed, and stored. The type and extent of the material now available eclipse that obtained in more traditional surveillance operations. Some forty-four percent of American Internet users, for instance, contribute their thoughts to the online world.[479] Sixty-four percent, nearly eighty two

---

[476] See WESTIN, *supra* note 16, at 311.

[477] *Id.*

[478] *See* U.S. GEN. ACCOUNTING OFFICE, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 4 (2004), *available at* http://www.gao.gov/new.items/d04548.pdf; James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004).

[479] AMANDA LENHART ET AL., THE PEW INTERNET & AM. LIFE PROJECT, CONTENT

million Americans, go online for spiritual or religious purposes.[480] The most popular uses reflect the most personal of matters, such as financial records, access to medical information, letters to friends and family, and gift purchases.[481]

It is not just Internet use that leaves a trail; medical, educational, financial, and other records can be digitally recorded and shared. And the evolution in telephony from copper to optical fiber means that not just voice, but data and images, can be transferred at the speed of light: just one of Cisco Systems's CRS-1 routers can move the entire Library of Congress in 4.6 seconds.[482] From circuit-switched networks, technology has morphed to allow for packet-switched designs, making the movement of data even more efficient.[483] And satellites break physical constraints. These and other technologies have dramatically increased the number of people using electronic communications. By 2007, the number of people using just mobile phones—not computers or land lines—is expected to hit two billion.[484]

CREATION ONLINE: 44% OF U.S. INTERNET USERS HAVE CONTRIBUTED THEIR THOUGHTS AND THEIR FILES TO THE ONLINE WORLD (2004), *available at* http://www.pewinternet.org/pdfs/PIP_Content_Creation_Report.pdf.

[480] STEWART HOOVER ET AL., THE PEW INTERNET & AM. LIFE PROJECT, FAITH ONLINE: 64% OF WIRED AMERICANS HAVE USED THE INTERNET FOR SPIRITUAL OR RELIGIOUS PURPOSES (2004), *available at* http://www.pewinternet.org/pdfs/PIP_Faith_Online_2004.pdf.

[481] *See* SUSANNAH FOX, THE PEW INTERNET & AM. LIFE PROJECT, TRUST AND PRIVACY ONLINE: WHY AMERICANS WANT TO REWRITE THE RULES 4 (2000), *available at* http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf; SUSANNAH FOX & DEBORAH FALLOWS, THE PEW INTERNET & AM. LIFE PROJECT, INTERNET HEALTH RESOURCES: HEALTH SEARCHES AND EMAIL HAVE BECOME MORE COMMONPLACE, BUT THERE IS ROOM FOR IMPROVEMENT IN SEARCHES AND OVERALL INTERNET ACCESS (2003), *available at* http://www.pewinternet.org/pdfs/PIP_Health_Report_July_2003.pdf; LEE RAINIE & JOHN HORRIGAN, THE PEW INTERNET & AM. LIFE PROJECT, HOLIDAYS ONLINE – 2002: EMAIL GROWS AS A SEASONAL FIXTURE AND E-SHOPPING ADVANCES (2003), *available at* http://www.pewinternet.org/pdfs/PIP_Holidays_Online_2002.pdf. The proliferation of computing technology further assisted the telecommunications explosion and the greater use made by people of Internet technologies. In 1981, for example, only three hundred computers were linked to the Internet. But by 1993, approximately one million computers had joined it. As of Jan. 2000, some 72.4 million were connected. *See* Young, *supra* note 427, at 303 n.4 (citing Randall L. Sarosdy, *The Internet Revolution Continues: Responding to the Chaos*, METROPOLITAN CORP. COUNS., Sept. 2000, at 15).

[482] Press Release, Cisco Sys., CRS-1 Heralds New Era for Modern Communications (May 24, 2004), *available at* http://newsroom.cisco.com/dlls/2004/hd_052504d.html.

[483] *See* Susan Landau, National Security on the Line 17 (July 1, 2005) (unpublished manuscript, on file with author).

[484] *Number of Mobile Phone Users Worldwide to Increase to 2 Billion by 2007*, GEEKZONE, Aug. 8, 2003, http://www.geekzone.co.nz/content.asp?contentid=1245.

Traveling through time and space to obtain information, share ideas or beliefs, and communicate with others are all activities that leave a trail—one on which private industry, quite outside state demands, has capitalized. Acxiom, Choicepoint, LexisNexis, and other firms now comprise a multi-billion dollar information industry. Infobase, just one of Acxiom.com's products, provides "[o]ver 50 demographic variables . . . including age, income, real property data, children's data and others."[485] It contains material on education levels, occupation, height, weight, political affiliation, ethnicity, race, hobbies, and net worth.[486] For a fee, Docussearch.com will provide any customer with the target's social security number, previous addresses, date of birth, neighbors, driver records, current address and phone number, current employer, driver's license number, driver histories, license plates/vehicle VIN numbers, unlisted numbers, beepers, cell phone numbers, fax numbers, bankruptcy and debtor filings, employment records, bank account balances and activity, stock purchases, corporate bank account, and credit card activity.[487]

Not only does private industry trade in this digital market, but the state buys access to it as well. Choicepoint, one of the industry's leaders, claims that it contracts with at least thirty-five American government agencies. These include a number of organizations that deal in counterterrorism, such as the DOJ, the FBI, the DEA, the US Marshals, the IRS, the Immigration and Naturalization Service ("INS"), and the Bureau of Alcohol, Tobacco and Firearms.[488]

The development of public identification, search, and tracking systems adds yet another dimension to the type of information that can be recorded, shared, and analyzed. Aerial and satellite reconnaissance aside, video surveillance systems make it possible to follow a person as she moves through public and, where closed circuit television ("CCTV") is provided by nonpublic actors, private space.[489] Combined with biometric

---

[485] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 3-4 (2004).

[486] *Id.*

[487] *The Privacy Commission: A Complete Examination of Privacy Protection: Hearing Before the Subcomm. on Gov't Mgmt., Info., and Tech. of the H. Comm. on Gov't Reform*, 106th Cong. 28-42 (2nd Sess. 2000).

[488] *See* STANLEY, *supra* note 289, at 26 n.107 (citing William Matthews, *Commercial Database Use Flagged*, FED. COMPUTER WEEK.COM, Jan. 16, 2002, http://www.fcw.com/fcw/articles/2002/0114/web-epic-01-16-02.asp); Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001 at A1; Electronic Privacy Information Center, EPIC Choicepoint Page, http://www.epic.org/privacy/choicepoint/default.html (last visited June 9, 2006).

[489] *See* Kevin Flynn, *Fighting Crime with Ingenuity, 007 Style: Gee Whiz Police Gadgets*

technologies, such as voice, gait, iris, and signature recognition, and hand or face vein mapping, cameras can identify members of the public without their knowledge.[490]

Individuals can be searched without being aware that it is being done: millimeter wave technology, infrared heat emission, back-scattered X-ray imaging, and radar skin scanning cut through barriers to reveal the human form and any objects located beneath garments.[491] Some of these systems already have been deployed at airports and other public places. And technology can go even further. For instance, thermal polygraphy may reveal whether a subject is telling the truth, without the person even knowing that they are under observation.[492] Tracking systems too have become ever more sophisticated. RFID tags, which emit short-range radio signals, or cell phone locator chips, take advantage of global positioning systems and allow for objects—or individuals—to be tracked. Both RFID and GPS chips are built to be implanted under the skin.

Get A Trial Run in New York, N.Y. TIMES, Mar. 7, 2000, at B1. For discussion of video technology, see Robert D. Bickel et al., *Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?* 33 STETSON L. REV. 299 (2003); Roberto Iraola, *Lights, Camera, Action!—Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 LOY. L. REV. 773 (2003); Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISCIP. L.J. 295 (1999); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213 (2002); Kent Greenfield, Comment, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U. CHI. L. REV. 1045 (1991); Robert H. Thornburg, Comment: *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses under the Fourth Amendment*, 20 J. MARSHALL J. COMPUTER & INFO. L. 321 (2002).

[490] *See, e.g.*, *Pentagon Aims to Track People*, OREGONIAN (Portland), May 20, 2003, *available at* http://foi.missouri.edu/terrorandcivillib/paimstotrack.html.

[491] Aerial reconnaissance and satellite imaging, for their part, provide views from the air, or space, of people and objects below. Senate Armed Services Committee Chair, John Warner, wants to deploy drones within the United States. For a discussion of Fourth Amendment and issues raised by aerial surveillances, see California v. Ciraolo, 476 U.S. 207 (1986); Eric D. Bender, Note, *The Fourth Amendment in the Age of Aerial Surveillance: Curtains for the Curtilage?* 60 N.Y.U. L. REV. 725 (1985); Krysten C. Kelly, Note, *Warrantless Satellite Surveillance: Will Our 4th Amendment Privacy Rights Be Lost in Space?*, 13 J. MARSHALL J. COMPUTER & INFO. L. 729 (1995); John R. Dixon, Note, *Criminal Procedure/Constitutional Law—Warrantless Aerial Surveillance and the Open View Doctrine*—Florida v. Riley, 109 S. Ct. 393 (1989), 17 FLA. ST. U. L. REV. 157 (1989).

[492] Henry T. Greely, *Prediction, Litigation, Privacy, and Property: Some Possible Legal and Social Implications of Advances in Neuroscience, in* NEUROSCIENCE AND THE LAW: BRAIN, MIND AND THE SCALES OF JUSTICE 114, 129-130 (Brent Garland ed., 2004).

These technologies and trends mean many things. But critically, for privacy and surveillance, they mean that a digital copy of our selves exists and can be refined. None of the underlying activities that we perform—birth, education, seeking medical care, buying food, reading, or writing letters—is new. But the recording of this information, its integration, and its swift recall—by private or public entities—is unprecedented. Access to such data gives others insight into who we are, who we have been, and who we are becoming. It allows people to get inside our minds and to learn about how we react, what our emotional states are, what issues we care about, and what drives us. A critical point here is that the information is individualized. It relates specifically to us and can be recalled in relation to ourselves.

Whatever the arguments may be for and against the accumulation and retention of this information, it represents something different in kind, not degree, from what has come before.[493] What makes this relevant to the current discussion is that national security claims generally, and counterterrorism in particular, dramatically increase the state's access to this information. Perhaps nowhere is this more obvious than in the realm of data mining, where the elimination of anonymity and entrenchment of broad psychological surveillance is the stated aim of those responding to the terrorist threat.

2. Data Mining Operations

In 2004, the GAO conducted a survey of 128 departments and agencies to determine the extent of federal data mining activities.[494] GAO uncovered 199 operations.[495] These served a broad range of purposes, such as improving services, managing human resources, and detecting terrorist activity.[496] The Department of Defense maintained the largest number of projects, with the most frequent users of data mining efforts being the Departments of Justice, Homeland Security, and Education.[497] One hundred and twenty-two of the 199 projects included personal information.

---

[493] These and other advances have devices led Sun Microsystems experts Whitfield Diffie and Susan Landau to write, "the impact of technology is so weighted on the side of law enforcement as to make it remarkable that crime has survived at all." DIFFIE & LANDAU, *supra* note 215, at 121.

[494] U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE RANKING MINORITY MEMBER, SUBCOMMITTEE ON FINANCIAL MANAGEMENT, THE BUDGET, AND INTERNATIONAL SECURITY, COMMITTEE ON GOVERNMENTAL AFFAIRS, U.S. SENATE: DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2 (2004) [hereinafter DATA MINING REPORT].

[495] *Id.*

[496] *Id.* at 2-3.

[497] *Id.* at 3.

Fifty-four purchased data from the private sector. Seventy-seven mined data from other federal agencies.[498]

Most importantly for our purposes, fourteen of the 199 programs addressed counterterrorist activity.[499] The CIA, for instance, runs "Octopus" and "Quantum Leap."[500] DIA operates "Insight Smart Discovery," and "Pathfinder." The Department of Education maintains Project Strikeback, which compares FBI and Department of Education files to find anomalies. The Department of Homeland Security's Notebook I2 links people and events to specific data points. The DOJ has a Secure Collaborative Operational Prototype Environment to enable investigators to analyze multiple digital sources to find hidden patterns and relationships. Some rely in considerable measure on personal information. For example, DIA's Verity K2 Enterprise trawls the intelligence community and the Internet to identify foreign terrorists or Americans connected to foreign terrorism. Eight of the fourteen counterterrorist initiatives drew on privately-held information to profile potential operatives.[501] Twelve obtained information from other agencies.[502]

Non-terrorist government databases also can be used for mining operations. The Department of the Treasury collects financial information from banks and financial institutions. The FBI maintains a criminal database with records, fingerprints, and DNA material. The Department of Health and Human Services has a "new hires" database that includes the name, address, social security number, and quarterly wages of every working person in the U.S. The Department of Education maintains primary school through higher education records (which, post-9/11, the FBI can search without probable cause). And the Departments of Motor Vehicles have photographs of virtually every American over the age of sixteen.[503] As for the terrorism-specific data mining efforts, while it would border on tedium to go through each one of these programs, a short discussion of a few will illustrate the extent to which the state is actively

---

[498] *Id.*

[499] *Id.* at 7.

[500] Bill Powell, *How George Tenet Brought the CIA Back From the Dead*, FORTUNE, Sept. 29, 2003, at 129, 134; Michael J. Sniffen, *Controversial Terror Research Lives On*, WASH. POST., Feb. 23, 2004, *available at* http://www.washingtonpost.com/wp-dyn/articles/A63582-2004Feb23.html.

[501] DATA MINING REPORT, *supra* note 494, at 11.

[502] *Id.* at 12.

[503] JAY STANLEY & BARRY STEINHARDT, AM. CIVIL LIBERTIES UNION, BIGGER MONSTER, WEAKER CHAINS: THE GROWTH OF AN AMERICAN SURVEILLANCE SOCIETY, 8 (2003), *available at* http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf.

seeking to develop psychological profiles, and highlight impact of these on privacy.

In 2002, John Poindexter launched Total Information Awareness—a program designed to link *all* government and commercial databases available worldwide.[504] The leviathan would trawl through multiple petabytes of data, uncovering hidden patterns and giving advance warning of a terrorist attack.[505] The logo of Poindexter's new agency neatly captured his vision: an eye from the top of the Illuminati pyramid spread its gaze over the world. Encircled with the words "Information Awareness Office," a Latin phrase at the bottom, *Scientia est Potentia*, proclaimed "Knowledge is Power."

The public balked at the flagrant disregard for privacy. On the Internet, web sites immediately appeared, dedicated to collecting information on Poindexter: his telephone number, where he lived, where he shopped, what he bought, what his family did, and where he last had been spotted.[506] Poindexter changed his telephone number. And in May 2003, he renamed the program "Terrorism Information Awareness."[507]

---

[504] John Markoff, *Pentagon Plans A Computer System that Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12; Robert O'Harrow, Jr., *U.S. Hopes to Check Computers Globally*, WASH. POST, Nov 12, 2002, at A4; s*ee also* INFO. AWARENESS OFFICE, DEF. ADVANCED RESEARCH PROJECT AGENCY, REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM: DETAILED INFORMATION 1 (2003), *available at* http://www.globalsecurity.org/security/library/report/2003/tia-di_report_20may2003.pdf [hereinafter TIA REPORT]. For a thoughtful discussion of the privacy issues raised by TIA and subsequent data mining efforts, see Dempsey & Flint, *supra* note 478.

[505] *See* THE INTENSIFICATION OF SURVEILLANCE: CRIME, TERRORISM AND WARFARE IN THE INFORMATION AGE 3 (Kirstie Ball & Frank Webster, eds., 2003). One petabyte would fill the Library of Congress' space for 18 million books more than 50 times. Some intelligence data sources "'grow at the rate of four petabytes per month.' Experts said those are probably files with satellite surveillance images and electronic eavesdropping results." Sniffen*, supra* note 500 (quoting the Office of Advanced Research and Development Activity). Deviance from social norms was to serve as an early indicator of terrorism:

> From human activity models, the ARM Program will develop scenario-specific models that will enable operatives to differentiate among normal activities in a given area or situation and activities that should be considered suspicious. The program aims to develop technologies to analyze, model, and understand human movements, individual behavior in a scene, and crowd behavior. The approach will be multisensor and include video, agile sensors, low power radar, infrared, and radio frequency tags.

TIA REPORT, *supra* note 504, at 11.

[506] *See, e.g.*, Warblogging.com, Who is John Poindexter?, http://www.warblogging.com/tia/poindexter.php (last visited June 9, 2006); Peter Barnes, *Tracking John Poindexter*, TECH LIVE WASH., D.C., Dec. 20, 2002, http://www.g4tv.com/techtvvault/features/41146/Tracking_John_Poindexter.html.

[507] A report submitted to Congress on the operation of the program bragged that TIA had already been used to analyze data obtained from detainees in Afghanistan, and to assess

As it became clear that the new TIA shared much in common with the old TIA, on September 30, 2003, Congress cut off funding.[508] But many of the projects simply transferred to other intelligence agencies.[509] Two of the most important have moved to the Advanced Research and Development Activity ("ARDA"), located at NSA headquarters.[510]

In 2002, DOD awarded a $19 million contract to Hicks & Associates to build an Information Awareness Prototype System—the architecture underlying TIA.[511] An email from Brian Sharkey, an executive at the firm, to subcontractors, said that the congressional decision "caused a significant amount of uncertainty for all of us about the future of our work." "Fortunately," he added, "a new sponsor has come forward that will enable us to continue much of our previous work."[512] According to the National Journal, the new source was ARDA.[513] Sharkey wrote that the new effort would be referred to as "Basketball"—a program later described by the Defense Department, after Congress shut down TIA—in the same language used for the TIA Information Awareness Prototype System first awarded to Hicks & Associates.[514]

Another central TIA project, Genoa II, sought to develop the technology to help to anticipate and preempt terrorism.[515] Intelligence sources confirmed to *National Journal* that this project had been re-named "Topsail" and moved to ARDA.[516] In October 2005, a government press release announced that it had granted SAIC a $3.7 million contract under

---

"weapons of mass destruction in the Iraqi situation." *See* TIA REPORT, *supra* note 504, at 16. These examples give pause: many detainees were tortured for information, making subsequent analysis somewhat suspect. Furthermore, the Bush Administration later admitted that there had been no weapons of mass destruction in Iraq. The nine organizations already using TIA included the U.S. Army Intelligence and Security Command ("INSCOM"); NSA, DIA, CIA, DOD's Counterintelligence Field Activity ("CIFA"), U.S. Strategic Command ("STRATCOM"), Special Operations Command ("SOCOM"), Joint Forces Command ("JFCOM"), and Joint Warfare Analysis Center ("JWAC"). *Id.* at 16-17. The report was required by the Consolidated Appropriations Resolution. Pub. L. No. 108-7, 117 Stat. 11 (2003).

[508] Department of Defense Appropriations Act, Pub. L. No. 108-87, 117 Stat. 1054 (2004).

[509] Sniffen, *supra* note 500.

[510] Shane Harris, *TIA Lives On*, NAT'L J., Feb. 23, 2006, *available at* http://nationaljournal.com/scripts/printpage.cgi?/about/njweekly/stories/2006/0223nj1.htm.

[511] *Id.*

[512] *Id.*

[513] *Id.*

[514] *Id.*

[515] *Id.*

[516] *Id.*

Topsail—with language describing the project virtually the same as previous descriptions of Genoa II.[517] In February 2006, when Senator Ron Wyden asked the Director of National Intelligence John Negroponte whether it was "correct that when [TIA] was closed, that several . . . projects were moved to various intelligence agencies,"[518] Negroponte's deputy, General Michael V. Hayden, the former director of the NSA, responded, "I'd like to answer in closed session."[519]

The Technology and Privacy Advisory Committee ("TAPAC"), appointed by Secretary of Defense Donald Rumsfeld to analyze the use of "advanced information technologies to identify terrorists before they act,"[520] admitted in March 2004 that TIA-like activities "may be continuing."[521] It

---

[517] *Id.*

[518] *Id.*

[519] *Id.* In a classified annex to its legislation halting funding to TIA, Congress created an exception, allowing funds to be used for "[p]rocessing, analysis, and collaboration tools for counterterrorism foreign intelligence . . . ." Department of Defense Appropriations Act, Pub. L. No. 108-87, § 8131, 117 Stat. 1054 (2004). The condition attached was that such tools could only be used where connected to "lawful military operations of the United States conducted outside the United States" or "lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens." *Id.* § 8131 (b)(1)-(2).

[520] DEP'T OF DEF., TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE CHARTER (2003), *available at* http://faca.disa.mil/pdf/165969.pdf.

[521] TECH. & PRIVACY ADVISORY COMM., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM: REPORT OF THE TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE viii (2004), *available at* http://www.cdt.org/security/usapatriot/20040300tapac.pdf [hereinafter TAPAC 2004 REPORT]. Evidence exists to support this. After Congress directed TIA to be dismantled, SRS Technologies, the primary support contractor for DARPA's Information Awareness Office, subcontracted with Torch Concepts to develop a data mining prototype. Ryan Singel & Noah Shachtman, *Army Admits Using JetBlue Data*, WIRED NEWS, Sept. 23, 2003, http://www.wired.com/news/privacy/0,1848,60540,00.html. The aim was to identify "abnormal events or activities that may include rebel actions before damaging events occur" by applying "intelligent pattern recognition in identifying latent relationships and behaviors that may help point to potential terrorist threats." *Id.* (quoting Press Release, Torch Concepts (May 8, 2002)). Singel and Shachtman pointed out, "[t]o privacy advocates, that sounds a lot like TIA's mission of researching 'data search and pattern recognition technologies . . . based on the idea that terrorist planning activities or a likely terrorist attack could be uncovered by searching for indications of terrorist activities in vast quantities of transaction data.'" *Id.* To help in constructing the prototype, JetBlue gave Torch Concepts five million passenger records. Ryan Singel, *JetBlue Shared Passenger Data*, WIRED NEWS, Sept. 18, 2003, http://www.wired.com/news/privacy/0,1848,60489,00.html. Torch Concepts then combined them with social security numbers, income levels, and other personal information. *Id.* The Transportation Security Administration facilitated the transfer of information. *Id.* Although other airlines immediately tried to distance themselves from the incident and claimed that, unlike JetBlue, their passenger records remained solely in the possession of the airline, this turned out to be false. *Id.* Immediately following 9/11, airlines turned over millions of records to the FBI. Sara K. Goo, *Northwest Gave U.S. Data on Passengers*, WASH. POST, Jan. 18, 2004, at A1; John Schwartz et al., *Airlines Gave F.B.I.*

added, TIA is "not unique in its potential for data mining. TAPAC is aware of many other programs in use or under development both within DOD and elsewhere in the government that make similar uses of personal information concerning U.S. persons to detect and deter terrorist activities."[522]

Indeed, the Homeland Security Act requires DHS's Directorate for Information Analysis and Infrastructure Protection:

> To access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies (including law enforcement agencies), and private sector entities, and to integrate such information in order to—(A) identify and assess the nature and scope of terrorist threats to the homeland; (B) detect and identify threats of terrorism against the United States; and (C) understand such threats in light of actual and potential vulnerabilities of the homeland.[523]

The legislature authorized $500 million for the Homeland Security Advanced Research Projects Agency to develop "data mining and other advanced analytical tools."[524]

Many of the systems being developed remain screened from the public eye. Hints of the scope of some of the projects, however, occasionally surface. One little-known DHS project, for instance, is Analysis, Dissemination, Visualization, Insight and Semantic Enhancement ("ADVISE").[525] According to the National Laboratories, this project "is a

---

Millions of Records on Travelers After 9/11, N.Y. TIMES, May 1, 2004, at A10. Later, Northwest Airlines provided millions more to NASA. Electronic Privacy Information Center, Northwest Airlines' Disclosure of Passenger Data to Federal Agencies, http://www.epic.org/privacy/airtravel/nasa/ (last visited June 9, 2006). And American Airlines admitted it had given 1.2 million passenger records to TSA. *American Released Passenger Data*, ASSOCIATED PRESS, Apr 10, 2004, http://www.wired.com/news/privacy/0,1848,63018,00.html.

[522] TAPAC 2004 REPORT, *supra* note 521, at viii. The report recognized that although data mining may be a "vital tool in the fight against terrorism . . . when used in connection with personal data concerning U.S. persons, data mining can present significant privacy issues." *Id.* Magnitude of privacy concerns depends upon,

> the sensitivity of the data being mined, the expectation of privacy reasonably associated with the data, the consequences of an individual being identified by an inquiry, and the number (or percentage) of U.S. persons identified in response to an inquiry who have not otherwise done anything to warrant government suspicion.

Id. at ix.

[523] Homeland Security Act of 2002, Pub. L. No. 107-296, § 201(d)(1), 116 Stat. 2135, 2146 (codified as amended at 6 U.S.C. § 121 (Supp. 2002)).

[524] GINA M. STEVENS, PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS, RL 31730, at 20 (2003) (citing Homeland Security Act, § 201(d)(14), 116 Stat. at 2147 (codified as amended at 6 U.S.C. § 121)).

[525] Clayton, *supra* note 475; *see Hearing Before H. Comm. on Science*, 109th Cong.

thrust area that has been developed to support the full range of information fusion needs of the DHS." The past tense here matters: it is under "spiral development," meaning that DHS implements it as the system evolves.[526]

ADVISE collects a broad range of information, such as financial records, blog postings, and news stories.[527] But it does not stop there. The model, as discussed by the National Laboratories, also includes multimedia, inferences, metadata, and history as types of information to be integrated into the system.[528] ADVISE then cross-references this data against intelligence and law-enforcement records.[529] The system stores each cross-reference as an "entity." A report summarizing a 2004 DHS conference in Virginia said that the system would be able to retain information on approximately one quadrillion entities.[530] According to Joseph Kielman, who manages DHS' Threat and Vulnerability, Testing and Assessment portfolio (which oversees ADVISE), the aim is not just to identify terrorists, but to find new patterns that reveal their intentions: to generate new knowledge.[531]

In addition to the federal efforts that continue apace, multi-state initiatives mirror TIA aims. Immediately following 9/11, Seisint Corp., a database firm located in Boca Raton, Florida, offered to work with the Florida Department of Law Enforcement ("FDLE") to create a statewide TIA program. According to their website, "Seisint is a global information management and technology company whose platforms enable organizations to unleash the power of massive data stores."[532] Their Data Supercomputer "enables data fusion and analysis of tens of billions of records in seconds and minutes instead of hours, days, or even weeks."[533] The company owns more than seven billion public records "from thousands

---

(2005) (statement of Dr. Charles McQueary, Under Sec'y for Sci. and Tech., Dep't of Homeland Sec.) (referencing ADVISE knowledge-generating architecture and highlighting plans to use it to "Create a National Homeland Security Support System (NH3S)"), *available at* http://www.house.gov/science/hearings/full05/feb16/McQueary.pdf

[526] SANDIA NAT'L LABS. & LAWRENCE LIVERMORE NAT'L LAB., DATA SCIENCES TECHNOLOGY FOR HOMELAND SECURITY INFORMATION MANAGEMENT AND KNOWLEDGE DISCOVERY 4, 6 (2004), *available at* http://csmr.ca.sandia.gov/~tgkolda/pubs/DSW2004_LoRes.pdf [hereinafter DATA SCIENCES].

[527] Clayton, *supra* note 475.

[528] DATA SCIENCES, *supra* note 526, at 6-11.

[529] Clayton, *supra* note 475.

[530] *Id.*

[531] *Id.*

[532] Line56.com, E-Business Company Profiles, http://www.line56.com/directory/company.asp?CompanyID=3349 (last visited June 9, 2006).

[533] SEISINT INC., SEISINT'S FACTS FOR THE MATRIX PROJECT 8 (2003), *available at* http://www.aclu.org/FilesPDFs/seisint_facts_83.pdf.

of locations" containing information on U.S. individuals and businesses.[534] The company announced, "[t]he associative links, historical residential information, and other information, such as an individual's possible relatives and associates, are deeper and more comprehensive than other commercially available database systems presently on the market."[535]

Seisint's offer almost immediately resulted in a working group with the FBI, U.S. Secret Service, INS, and the U.S. Attorney's Office, (plus FDLE and Seisint).[536] Although the working group ceased after six months, Seisint continued to work on a model system with FDLE. They combined "billions of public and commercial records with five of Florida's existing data files: Criminal Histories, Drivers' Licenses, Motor Vehicle Registrations, Department of Corrections records and Sexual and Violent Offender lists."[537] The Florida Crime Information Center Plus (FCIC+) has been in operation since March 2002. As this program got off the ground, the Office of Justice Programs, DOJ, initiated funding for MATRIX—"a proof-of-concept, state initiated and state governed project."[538] By August 2004, DHS and DOJ had provided more than $9.2 million to develop a counterterrorism system.[539] Georgia, New York, Oregon, and Pennsylvania joined ranks, and by mid-2003, some thirteen states participated, covering roughly fifty percent of the population in the US. A public relations nightmare, however, ensued, as political and civic leaders began to realize what was happening. By August 2004, eight of the thirteen had dropped out, leaving only Connecticut, Florida, Michigan, Ohio and Pennsylvania.[540] In September 2004, LexisNexis acquired Seisint.[541]

MATRIX combined criminal records, driver's license data, motor vehicle registration records, and individual-specific public information.[542] At one point, the program's web site claimed to marshal more than twenty

---

[534] *Id.* at 6.

[535] *Id.* at 10.

[536] *Id.*

[537] *Id.*

[538] *Id.*

[539] *Id.*; STANLEY, *supra* note 289, at 26 n.108 (citing INST. FOR INTERGOVERNMENTAL RESEARCH, APPLICATION FOR FEDERAL ASSISTANCE TO THE OFFICE OF JUSTICE PROGRAMS BUREAU OF JUSTICE ASSISTANCE (2002)).

[540] Brian Robinson, *Reenter the Matrix*, FED. COMP. WEEK.COM, Aug. 30, 2004, http://www.fcw.com/supplements/homeland/2004/sup3/hom-matrix-08-30-04.asp.

[541] Press Release, LexisNexis Completes Acquisition of Seisint, Inc.: Acquisition Enhances Ability to Provide Customers with Powerful, Fast and Easy-to-Use Risk Management Products and Services (Sept. 1, 2004), http://www.accurint.com /news/news_9_1_2004.html (last visited June 9, 2006).

[542] Anita Ramasastry, *Why We Should Fear the Matrix*, FIND LAW, Nov. 5, 2003, *available at* http://writ.news.findlaw.com/ramasastry/20031105.html.

billion records from hundreds of sources.[543] The system included social network visualization—a diagram that presents relationships among individuals, addresses, vehicles, and corporations. MATRIX also generated geographic mapping visualization, photomontage, and photo lineups. In October 2003, the ACLU filed FOIA requests with Connecticut, Michigan, New York, Ohio and Pennsylvania to find out more about the program.[544] In April 2006, the MATRIX web site indicated that the project had been completed, and the web site was discontinued.[545]

TIA, ADVISE, MATRIX, and the other data mining efforts demonstrate that the United States has an interest in, and is attempting to develop, a centralized clearinghouse for information. In July 2002, the National Strategy for Homeland Security recognized that instead of a central computer network, information exists in a variety of federal, state, and local databases. The strategy stated, "[i]t is crucial to link the vast amounts of knowledge resident within each agency at all levels of government."[546] The document declared its intent:

> We will build a national environment that enables the sharing of essential homeland security information. We must build a 'system of systems' that can provide the right information to the right people at all times. Information will be shared 'horizontally' across each level of government and 'vertically' among federal, state and local governments, private industry, and citizens . . . . We will leverage America's leading-edge information technology to develop an information architecture that will effectively secure the homeland.[547]

This goal raises important concerns related to privacy and the role it plays in democratic states—issues that include but expand beyond the state's effectiveness in countering terrorist threat. I return to these in Part III.

II. SURVEILLANCE AND THE LAW IN THE UNITED KINGDOM

The English constitution differs from its American counterpart in that it embraces the principle of parliamentary supremacy. This means that the constitution combines common law, statutory law, and custom. Unlike in the United States, no single document takes precedence. While some

---

[543] Briefing by Seisent, Inc., MATRIX Michigan Briefing, slide "Seisint's Core Capabilities" (May 8, 2003), *available at* http://www.aclu.org/privacy/spying/14950res20040121.html.

[544] Ramasastry, *supra* note 542.

[545] Multistate Anti-Terrorism Information Exchange, http://www.matrix-at.org/ (last visited June 9, 2006).

[546] OFFICE OF HOMELAND SEC., NATIONAL STRATEGY FOR HOMELAND SECURITY 55 (2002), *available at* http://www.whitehouse.gov/homeland/book/ nat_strat_hls.pdf (emphasis added).

[547] *Id.* at 56.

statutes may be considered particularly important, all acts technically have the same status. In 1998, an important nuance emerged: Westminster, through the Human Rights Act, incorporated the European Convention of Human Rights into domestic law. The statute requires that acts of Parliament be read *as far as possible* in a manner consistent with the Convention. However, should courts find a divergence, the legislation requires only that a declaration of incompatibility be made. No other domestic legal consequences follow.

Until the incorporation of this Convention, the English constitution did not admit of a right to privacy writ large. Instead, specific statutes protected different aspects of the country's unique culture of privacy. The 1361 Justices of the Peace Act, for instance, outlawed eavesdroppers and peeping toms.[548] *Semayne's Case* later underscored the status of the home.[549] Just over a century later, in *Entick v. Carrington*, Lord Camden dismissed the doctrine of state necessity without statutory basis, requiring the Crown to obtain proper authorization to cross the threshold of the home.[550] This case formed part of a series of civil actions in which English courts grappled with the contours of privacy.[551] These cases, however, and such laws as did exist, addressed particular situations that gave rise to privacy claims.[552]

---

[548] Justices of the Peace Act, 1361, 34 Edw. 3, c. 1 (Eng.).

[549] Semayne's Case, (1603) 77 Eng. Rep. 194, 195 (K. B.).

[550] Entick v. Carrington, (1765) 19 St. Tr. 1030 (K.B.). Security forces, searching for John Wilkes' pamphlets, had entered into Entick's dwelling, broken into locked desks, and retrieved his papers. Lord Camden warned against a state of affairs where, "the secret cabinets and bureaus of every subject in this kingdom will be thrown open to the search and inspection of a messenger, whenever the secretary of state shall think fit to charge, or even to suspect, a person to be the author, printer or publisher of a seditious libel." *Id.* at 1063.

[551] *See also* Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (C.P.); Huckle v. Money, (1763) 95 Eng. Rep. 768 (K.B.), *aff'd*, Money v. Leach (1765), 19 Howell's State Trials 1002, 1028, 97 Eng. Rep. 1075 (K.B.). The United States Supreme Court later looked to them as a guide of what the Framers intended in the Fourth Amendment. *See, e.g.*, Boyd v. United States, 116 U.S. 616, 626 (1886).

[552] *See also* Data Protection Act, 1984, c. 35 (U.K.), *repealed by* Data Protection Act, 1998, c. 29 (U.K.), *available at* http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm; Rehabilitation of Offenders Act, 1974, c. 53 (U.K.); Protection from Harassment Act, 1997, c. 40 (U.K.); Unsolicited Goods & Services Act, 1971, c. 30, § 4 (U.K.). Common law protection in the realm of nuisance also existed. *See, e.g.*, Victoria Park Racing & Recreation Grounds Co. Ltd. v. Taylor (1937) 58 C.L.R. 479 (Austl.); Khorasandjian v. Bush, (1993) Q.B. 727 (U.K.); Bernstein v. Skyviews & Gen. Ltd., (1978) Q.B. 479 (U.K.); Jolliffe v. Willmett & Co., (1971) 1 All E.R. 478 (U.K.); Hickman v. Maisey, (1900) 1 Q.B. 752 (A.C.) (Eng.). *But see* Hunter v. Canary Wharf Ltd., [1997] A.C. 655 (H.L.) (appeal taken from Eng.) (U.K.). Breach of confidence also was widened at common law. *See, e.g.*, Francome v. Mirror Group Newspapers Ltd., (1984) 2 All E.R. 408 (A.C.) (U.K.).

Part of the reason for the lack of a blanket protection revolved around the complexity of the right and its intimate relationship with other rights and freedoms. In some measure, it also related to the difficulty of definition. In the late 19th century, Judge Thomas Cooley provided one of the earliest: the right to be left alone. Although initially a negative claim, as in the United States, British popular understanding gradually moved towards a more positive right—the ability to control information and to choose whether and in what manner to communicate personal details. However, the definitional problem remained. In 1972, the Younger Committee declared that privacy escaped satisfactory definition.[553] Nearly two decades later, the Calcutt Committee echoed the earlier findings, stating, "nowhere have we found a wholly satisfactory statutory definition of privacy."[554] Undeterred, the Committee nevertheless suggested one: "The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information."[555] The possibility of creating a more general right to individual privacy attracted attention.

In 1993, a follow-up report called for the government to introduce legislation to protect the private sphere.[556] And other documents followed. The Lord Chancellor's Department issued *Infringement of Privacy*, which attacked the absence of such protections in English law. The report called for the creation of a tort to address situations where substantial distress might be caused by the invasion of privacy. Soon thereafter, the U.K. government's *Response to the National Heritage Select Committee* asserted "[e]very individual has a right to privacy comprising: (a) a right to be free from harassment and molestation; and (b) a right to privacy of personal information, communications, and documents."[557] But the government still determinedly dodged the creation of a broader right.

It was not until the 1998 incorporation of the European Convention of Human Rights ("ECHR") into domestic law that Westminster embraced a general right to privacy. Article 8(1) of the Convention ensures that all

---

[553] HER MAJESTY'S STATIONERY OFFICE, 1972: REPORT OF THE COMMITTEE ON PRIVACY, 1972, Cm. 5012 (U.K.) [hereinafter YOUNGER COMMITTEE REPORT].

[554] HER MAJESTY'S STATIONERY OFFICE, REPORT OF THE COMMITTEE ON PRIVACY AND RELATED MATTERS, 1990, Cm. 1102 (U.K.) [hereinafter CALCUTT COMMITTEE REPORT].

[555] *Id.*

[556] HER MAJESTY'S STATIONERY OFFICE, CALCUTT (NO.2) REPORT, 1993, Cm. 2135 (U.K.).

[557] HER MAJESTY'S STATIONERY OFFICE, GOVERNMENT RESPONSE TO THE NATIONAL HERITAGE SELECT COMMITTEE, PRIVACY AND MEDIA INTRUSION, 1995, Cm. 2918 (U.K.).

persons have the right to respect for their private and family life, their home, and their correspondence.[558]

Article 8(2), however, goes on to provide that the public authority can interfere with this right when it "is in accordance with the law and is necessary in a democratic society *in the interests of national security, public safety* or the economic well being of the country, *for the prevention of disorder or crime,* for the protection of health or morals, or *for the protection of the rights and freedoms of others*."[559]

When placed against counterterrorist claims, this exception provides a loophole that can be exploited by the state. Exactly what constitutes a national security concern can be molded to fit the moment. Moreover, the Human Rights Act, which incorporated the ECHR, requires only that legislation be read *as far as possible* in a manner compatible with the convention. In the event that surveillance statutes contravene it, the judiciary only is required to make a declaration of incompatibility. And question still exists about the extent of European law. Three years after incorporation of the ECHR, the House of Lords questioned whether any *actionable* right to privacy exists in the United Kingdom.[560]

Part II posits that despite the recent protections offered by the European Convention of Human Rights, and the British government's repeated claim to be meeting the European Court's objections through the introduction of a statutory framework, it appears as though the state has

---

[558] Under the European Convention, respect for the privacy of the home extends to the place of business. Halford v. United Kingdom, 24 Eur. Ct. H.R. 523, 523-24 (1997) ("It is made clear from the Court's case law that telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8(1)."); *see also* Niemietz v. Germany, 16 Eur. Ct. H.R. 97, 97-98 (1992); Chappell v. United Kingdom, 12 Eur. Ct. H.R. 1 (1990). However, in public places, no legitimate expectation of (illegitimate) businesses is provided. *Compare* Khan v. United Kingdom, 31 Eur. Ct. H.R. 1016, 1023 (2001) (finding that there was no legal authority for proper judicial regulation of police placing microphone on outside of a building), *with* Ludi v. Switzerland, 15 Eur. Ct. H.R. 173 (1992); *see also* Kruslin v. France, 12 Eur. Ct. H.R. 547 (1990).

[559] European Convention on Human Rights, art. 8(2), Nov. 4, 1950, 213 U.N.T.S. 221 (emphasis added), *available at* http://www.hri.org/docs/ECHR50.html.

[560] Douglas v. Hello! Ltd, [2001] Q.B. 967, 1012 (A.C.) (U.K.) (maintaining that it was "unlikely that *Kaye v. Robertson*, which held that there was no actionable right of privacy in English law, would be decided in the same way on that aspect today").

> Consequently, if the present case concerned a truly private occasion, where the persons involved made it clear that they intended it to remain private and undisclosed to the world, then I might have concluded that in the current state of English law the claimants were likely to succeed at any eventual trial.

FELDMAN, supra note 17, at 550 (quoting Kaye v. Robertson, (1992) F.S.R. 62 (A.C.) (U.K.)).

used European objections as an opportunity to legitimize existing practices and extend the scope of state surveillance. Unlike the United States, warrants for surveillance remain within the executive domain. Outside the judicial domain, the standard applied is that of reasonable suspicion, which sets the bar lower than the probable cause requirements for Title III searches across the Atlantic.

A. THE EVOLUTION OF INFORMATION-GATHERING AUTHORITY

This section begins with the evolution of information-gathering authority in British law. It focuses on property interference, the interception of communications, covert surveillance, the use of covert human intelligence sources, and encrypted data. The main bodies exercising these powers for counterterrorist purposes include the Security Service ("MI5"), Secret Intelligence Service ("MI6"), Government Communications Headquarters ("GCHQ"), and law enforcement.[561] While oversight mechanisms within the executive branch exist, their effectiveness is not at all clear. The United States is not alone in taking advantage of technology to expand its surveillance capabilities. Part II concludes with a brief discussion of CCTV, the realm in which the U.K. leads the world for concentration of cameras in the public sphere.

1. Property Interference

The first observation to be made about British surveillance law is that, as in the United States, a distinction between regular law enforcement and counterterrorist authorities can be drawn. The English Constitution long ago addressed the conditions under which the police had to obtain a warrant physically to interfere with property. More recently, the 1984 Police and Criminal Evidence Act provided the relevant standard.[562] The 1997 Police

---

[561] The United Kingdom has three agencies that perform its principal counterterrorist intelligence functions: The Secret Intelligence Service, Government Communications Headquarters, and the Security Service. MI6, run under the authority of the Secretary of State, provides information relating to events, individuals, and networks *outside* domestic bounds. Its powers are exercisable only in relation to national security (particularly defense and foreign policy), safeguarding the economy, and preventing or detecting serious crime. GCHQ, of Bletchley Park fame, focuses on signals intelligence, monitoring electromagnetic, acoustic, and electronic communications. Its functions must be carried out in the interests of national security, the economic well-being of the UK, and the prevention or detection of serious crime. MI5 covers *domestic* national security threats. SIS and GCHQ report to the Foreign Secretary, and MI5 to the Home Secretary. Intelligence-gathering authority for counterterrorism also extends to agencies located at the Ministry of Defence, the Cabinet, and law enforcement.

[562] Police and Criminal Evidence Act, 1984, § 8, ¶ 1 (U.K.), *available at*

Act subsequently expanded the number of law enforcement bodies who could obtain permission to gain entry to include the police, the National Criminal Intelligence Service ("NCIS"), the National Crime Squad, and HM Customs and Excise.[563] In the event that a dwelling, hotel bedroom, or office, is to be inspected, or where confidential information is likely to be acquired, prior approval must be granted by a Commissioner.[564] The statute empowers the Commissioner to quash the warrant where reasonable grounds exist for believing the authority sought does not meet statutory requirements. In all cases, the officer authorizing the intrusion must notify the Commission.

Unlike law enforcement, MI6 which addressed threats outside domestic bounds had, until 1994, no statutory authority to interfere with property inside state borders.[565]

Perhaps more spectacularly, for nearly four decades the MI5, which *did* focus on domestic matters, operated without any statute sanctioning its existence or powers.[566] This meant that, technically, MI5 operatives had the same search and arrest authorities extended to all British subjects.[567]

---

http://www.opsi.gov.uk/si/si1988/Uksi_19881200_en_1.htm.

[563] SECURITY SERVICE COMMISSIONER, ANNUAL REPORT FOR 1999, ¶ 22 (U.K.), *available at* http://www.archive.official-documents.co.uk/document/cm47/4779/4779-01.htm. Formal implementation of these measures began in February 1999. The officer must be satisfied that the action will be "of substantial value in the prevention or detection of serious crime, and that what the action seeks to achieve cannot reasonably be achieved by other means." Police Act 1997, c. 50, § 93(2) (U.K.), *available at* http://www.opsi.gov.uk/acts/acts1997/97050—j.htm#91. The legislation defines serious crime as violent acts, events that result in substantial financial gain, or conduct by a large number of people in pursuit of a common purpose. It also includes *any* offense for which a person above the age of twenty-one with no previous convictions, would likely receive at least three years' imprisonment. *Id.* § 93(4).

[564] If, however, it is not reasonably practicable for a Commissioner to grant prior approval, an urgent, seventy-two-hour approval can be authorized by designated officers within the law enforcement bodies, for later approval by a Commissioner. *Id.* §§ 94-95.

[565] *See* Intelligence Services Act, 1994, §5(3) (U.K.), *available at* http://www.opsi.gov.uk/ACTS/acts1994/Ukpga_19940013_en_1.htm. In 1909, MI6 began as the foreign section of the Secret Service Bureau. By 1922 it had evolved into a separate agency, called the Special Intelligence Service/MI6. MICHAEL COUSENS, SURVEILLANCE LAW 91 (2004).

[566] In 1952, Sir David Maxwell Fife issued a Directive to the Director General of the Security Service, indicating that MI5 would report directly to the Home Secretary. The organization was to be considered separate from the Home Office and part of the United Kingdom's Defence Forces. Its purpose would be to defend the realm "from external and internal dangers arising from attempts at espionage and sabotage or from actions of persons and organizations whether directed from within or without the country which may be judged to be subversive of the state." Directive to the Director General of the Security Services, issued by Home Secretary Sir David Maxwell Fife, 24 Sept. 1952 (U.K.), *reprinted in* COUSENS, *supra* note 565.

[567] LORD DENNING'S REPORT, 1963, Cmnd. 2152, c. XVII (U.K.).

Nevertheless, just five years after the creation of the agency, a special Committee of Privy Councillors determined that MI5 routinely intercepted domestic communications.[568]

Towards the end of the 20th century, public concern mounted about MI5's general role. The media reported, for instance, that the agency screened potential employees of the British Broadcasting System.[569] The secretive nature of the organization and lack of redress afforded to British subjects for perceived violations of individual rights came under increasing scrutiny. A prominent case raising these concerns reached the European Commission ("EC").[570] The applicants, both members of the National Council for Civil Liberties, claimed to have been the object of MI5 surveillance. The EC found that the 1952 Directive that created the Security Service did not count as a legally enforceable rule. It did not give British subjects a sufficient idea of the powers of the state; nor was there an effective remedy under English law. This brought the UK into violation of articles 8 and 13 of the ECHR.

In 1989 the government responded by placing MI5 on a statutory basis.[571] Section 5 of the Security Services Act empowered the Secretary of State to issue warrants for physical interference with property. The application includes a description of the case, the name of the person or organization targeted, the property involved, the operational plan, and an assessment risk. The Secretary of State must be satisfied that the search is necessary, "of substantial value" to MI5 in discharging its duties, and "cannot reasonably be obtained by other means."[572] The warrant is valid for

---

[568] REPORT OF THE COMMITTEE OF PRIVY COUNCILLORS APPOINTED TO INQUIRE INTO THE INTERCEPTION OF COMMUNICATIONS (1957) (U.K.), *available at* http://fipr.org/rip/Birkett.htm [hereafter BIRKETT REPORT].

[569] COUSENS, *supra* note 565, at 85.

[570] Hewitt & Harman v. United Kingdom, 14 Eur. Ct. H.R. 657 (1992).

[571] Updated in 1996, the Security Services Act requires MI5 to protect national security "against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means." The statute leaves "national security" undefined. Security Service Act, 1989, c. 5 (U.K.), *available at* http://www.archive.official-documents.co.uk/document/cm47/4779/4779.htm. This statute replaced a 1952 Directive that read, in part, "[t]he Security Service is part of the Defence Forces of the country. Its task is the Defence of the Realm as a whole, from external and internal dangers arising from attempts at espionage and sabotage, or from actions of persons and organisations whether directed from within or without the country, which may be judged to be subversive of the State." LORD DENNING'S REPORT, *supra* note 567, at 80.

[572] SECURITY SERVICE COMMISSIONER, *supra* note 563, ¶ 7-8.

a period of up to six months from issue, but can be renewed for another six month period if considered necessary by the Secretary of State.[573]

What makes this mechanism extraordinary is that, even as it allows the Security Services to move into ordinary policing, the device for preventing misuse of the powers remains in the control of the Executive—not the Judiciary. This appears to violate the basic principle laid down in *Entick v. Carrington*: allowing the state to cross the threshold of the home without appropriate oversight risked abuse. Yet MI5 can now enter and search property without a judicial warrant.

To bring the powers into line with the European Convention, Parliament provided for formal review by an Independent Commissioner, whose annual report is laid before each House of Parliament. These reports, however, contain little information of value. They do not even reveal the number of warrants obtained by the Intelligence Services. In the First Report, the Rt. Hon. Lord Justice Stuart Smith considered it "not in the public interest" to provide such information, adding that, compared to the 1985 Interception of Communications Act, there were only a "comparatively small number of warrants issued under the 1989" legislation. Despite further statutes, however, reviews have consistently resisted providing such information, concerned that it would "assist the operation of those hostile to the state."[574] For the most part, the annual reports simply restate the legal authority under which the Intelligence Services operate. The legislation also included the creation of a Tribunal for investigating complaints. Between 1989 and 1999, the Tribunal considered some 338 complaints, with three left outstanding.[575] In none of these cases did the Tribunal find in favor of a complainant.[576] I will return to these considerations in Part III.

2. Interception of Communications

Legal scholarship sharply divides over the origin of Executive authority to intercept communications. But speculation over whether the

---

[573] Security Service Act 1989, c. 5, §§ 3(4)-(5) (U.K.). The procedure on renewal is much the same as on initial application, except that the request states whether or not the operation has produced intelligence of value since its inception, and has to show that it remains necessary for the warrant to continue to have effect for the purpose for which it was issued. In 1994, the Intelligence Service Act brought the warrant requirements of MI6, MI5, and GCHQ into line. Application for all is made to the Secretary of State.

[574] INTELLIGENCE SERVICES COMMISSIONER, REPORT, 2005, H.C. 548, ¶ 31 (U.K.), *available at* http://www.official-documents.co.uk/document/hc0506/hc05/0548/0548.pdf.

[575] SECURITY SERVICE. COMMISSIONER, *supra* note 563, ¶ 37.

[576] *Id.* ¶ 38.

power finds its locus in Royal Prerogative, statutes governing preservation of the state and public order, common law, or custom derived from a monopoly on the posts, remain just that.[577] Indeed, two secret committees (one each in the House of Lords and House of Commons), designated in 1844 with the task of determining the state of the law with respect to opening letters, dodged consideration of the origins of this power by simply recognizing its existence.[578]

Written documents and letters became the first kind of communications to be intercepted. The ordinance *establishing* the first Post Office referred to the office as "the best Means to discover and prevent any dangerous and wicked Designs against the Commonwealth."[579] An Act of Parliament in 1660 agreed *mutatis mutandis* with the content of the Ordinance.[580] Three years later, the Crown issued a Royal Proclamation, announcing that only the Principal Secretary of State could open packages and letters.[581] Similar language marked the 1710 statute "for establishing a General Post Office for all Her Majesty's Dominions," 1837 Post Office (Offences) Act, 1908 Post Office Act, and, more recently, the 1953 Post Office Act. Under this last statute, only an express warrant issued by a Secretary of State could authorize the interception and opening of any letter, postcard, newspaper, parcel, or telegram.[582]

This history led a special review body to conclude in 1957 that:

> (a) The power to intercept letters and postal packets and to disclose their contents and otherwise to make use of them had been used and frequently used through many centuries
>
> (b) Such a power existed and was exercised widely and publicly known . . . .
>
> (c) At no time had it been suggested with any authority that the exercise of the power was unlawful.[583]

The power to intercept telephone communications presents a similar history.

---

[577] *See* BIRKETT REPORT, supra note 568, at Part I.

[578] The House of Lords commented, "the Power appears . . . to have been exercised from the earliest Period, and to have been recognized by several Acts of Parliament. This appears to the committee to be the State of the Law in respect to the detaining and opening of Letters at the Post Office and they do not find any other Authority for such detaining or opening." *Id.* ¶ 15.

[579] *Id.*

[580] *Id.*

[581] *Id.* ¶ 32.

[582] Post Office Act 1953, 1 & 2 Eliz. II, c. 36, §87(1) (U.K.).

[583] BIRKETT REPORT, *supra* note 568, ¶ 39.

From the origins of the telephone until 1937, the Post Office and others assumed that any entity operating the telecommunication network had the authority to intercept messages.[584] Such surveillance did not, therefore, require any warrants from the Secretary of State; rather, the intelligence services and law enforcement contacted the Director-General of the Post Office to obtain information.[585] In 1937, the policy changed to reflect the Home Secretary's view that the powers granted to the Secretary of State in regard to the post and, later telegrams, logically extended to telecommunications.[586] For nearly fifty years, however, no explicit, statutory authority followed.

Throughout this time, the Secretary of State required that the requesting body provide the name, address, and telephone number of the targets of the interception. Occasionally, one warrant would include multiple people.[587] The standard practice was for the Secretary to ascertain whether such intercepts would be necessary for either the prevention or detection of serious crime or to protect national security.[588] What constituted a "serious crime," though, changed over time: during the war years, efforts to get around rationing constituted a serious offence. Participating in lotteries, a severe crime in 1909, by 1953 had become a way to pass the time. And the standards for obscenity gradually relaxed.[589]

The Metropolitan Police and HM Customs and Excise submitted the majority of the warrant requests.[590] From time to time the Home Office admonished these and other agencies for making too many requests: In September 1951, the Home Office issued letters saying the interception was an "inherently objectionable" practice, and suggested that "the power to stop letters and intercept telephone calls must be used with great caution."[591] The Secretary laid down three conditions for law enforcement to meet: the offence had to be really serious—meaning an individual with no previous record could reasonably expect at least three years' sentence, or the offence, of lesser gravity, involved a significant number of people. For Customs and Excise, the Secretary of State narrowed "serious crime" to cases involving "a substantial and continuing fraud which would seriously damage the revenue or the economy of the country if it went unchecked."

---

[584] *Id.* ¶ 40.
[585] *Id*.
[586] *Id.* ¶ 41.
[587] *Id.* ¶ 56.
[588] *Id.* ¶ 57.
[589] *Id.* ¶¶ 58-59.
[590] *Id*. ¶ 66.
[591] *Id.* ¶ 64.

Finally, the requesting agency had to have tried normal methods of investigation, and failed. Alternatively, other methods had to be unlikely to succeed. The Home Office also declared that good reason must exist to believe that interception would result in conviction.[592]

The Home Office maintained separate arrangements for warrants granted to the Security Service.[593] For this organization, the Secretary of State required that the investigation relate to a major subversive or espionage activity likely to hurt national security, and that the material thus yielded would be of use to MI5 in carrying out its duties. While the Secretary of State preferred that more conservative means of gathering the information be first attempted, or be unlikely to succeed, the Home Office gave greater weight to the collection of information than to the need to secure convictions.[594] All warrants issued by the Secretary of State authorized interception for an indefinite period.

Although not regulated by statute, the procedure for requesting warrants involved many layers; the Metropolitan Police, Customs and Excise, and MI5 created internal structures to vet applications.[595] The first two organizations then forwarded these to the Home Office Criminal Department for approval, after which the application went to the Permanent Under-Secretary of State. (MI5 forwarded the application directly to the Permanent Under-Secretary of State). If satisfied that the requirements had been met, the under-secretary then forwarded the request to the Secretary of State for final approval. The net result of this process was that the Secretary of State ended up rejecting very few applications[596]—a claim reflected in the American Department of Justice's defense of the almost nonexistent refusal by the FISA courts to grant a warrant. Additional procedures within the Home Office, law enforcement, and intelligence agencies assisted in vetting applications: as of 1957, the Permanent Under-Secretary undertook quarterly reviews of outstanding warrants.[597] The Metropolitan Police (from 1956) undertook their own weekly review; Customs and Excise considered theirs quarterly; and MI5 analyzed outstanding warrants twice a year. The Home Office strictly followed a policy that, except in extraordinary circumstances, any information gleaned

---

[592] *Id.* ¶¶ 64-67.
[593] *Id.* ¶ 67.
[594] *Id.* ¶ 68.
[595] *Id.* ¶ 69.
[596] *Id*. ¶ 70.
[597] *Id.* ¶ 71.

from interception would be excluded from judicial proceedings or as evidence in any other formal Inquiry.[598]

While cautioning against the use of intercept material in the course of investigations, consecutive Secretaries of State recognized the importance of such surveillance in undermining criminal and subversive activities. Successes ranged from disrupting a £9 million illicit diamond market and recapturing escaped convicts to detecting Communist spies located in the Civil Service.[599]

As telecommunications grew in social importance, the trend moved away from postal intercepts and towards telephone conversations. In 1937, the total number of warrants for mail openings issued by the Home Secretary in England and Wales, eclipsed the number issued for telephone wiretaps: 556 warrants approved of postal intercepts, while a mere seventeen applied to telephones. In 1955, the numbers reversed, with wiretaps exceeding mail openings. And the number of taps steadily expanded: from 299 in 1965, by 1975 the number had grown to 468. In 1995 the Home Secretary authorized 910 taps. By 2000, this number had increased to 1,559.[600]

Throughout this period, no law sanctioned the interception regime or provided a remedy for violations. It technically remained legal to place phone taps even in the absence of an authorizing warrant. This caused the Birkett Committee to suggest as early as 1957 that Parliament "consider whether legislation should be passed to render the unauthorised tapping of a telephone line an offence."[601] It was not until the United Kingdom fell afoul of European law, however, nearly three decades later, that Westminster took up the gauntlet.

---

[598] *Id.* ¶ 90.

[599] *Id*. ¶¶ 104-07.

[600] These numbers do not reflect the total number of wiretaps issued in the UK. They omit warrants issued in Scotland, although a similar pattern existed there. *See* Regulation of Investigatory Powers Act, 2000, c. 23 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts2000/20000023.htm; INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2001, H.C. 1243 (U.K.), *available at* http://www.archive2.official-documents.co.uk/document/deps/hc/hc1243/1243.pdf. The numbers also neglect those issued by the Secretary of State for Northern Ireland, which have never been published, as well as the Foreign Secretary, which have been withheld from public scrutiny since 1984. Equally absent is the number of wiretaps placed, but not specifically authorized or penalized, by domestic law. *See* Statewatch News Online, Telephone Tapping and Mail-opening Figures 1937-2000, http://www.statewatch.org/news/DOCS/Teltap1.htm (last visited June 9, 2006) (providing a table indicating number of telephone tapping, mail opening, and total surveillance warrants issued in England and Wales by year).

[601] BIRKETT REPORT, *supra* note 568, ch. 5 ¶ 131.

a. *Malone v. United Kingdom*[602] and its aftermath

In the mid-1970s, the London Metropolitan Police requested and obtained a warrant from the Secretary of State to tap the phone lines of an antique dealer suspected of handling stolen property. Mr. Malone, the target of the intercept, responded to charges brought against him with a suit against the police claiming relief under both English law and the European Convention of Human Rights.

In regard to the first, Malone argued that it was unlawful for anyone, including the state, to intercept communications without the consent of those involved. This claim arose from the right of property, the right of privacy, and the right of confidentiality. The state countered, saying that no statute made government wiretapping illegal; in fact, broad recognition in the statutory instruments that such tapping occurred suggested no right to immunity existed.

Sir Robert Megarry responded to Malone's claims by announcing that he was unconvinced that the electronic impulses transmitted over the wires constituted property. On the right to privacy, the oft-repeated recognition that no blanket right to privacy existed in English law—not least in the recently published Halsbury's Laws of England—rather defeated any claim to an express right. The claim to an implicit right also failed. Like the American court in *Olmstead*, Megarry asserted that interception outside the bounds of ones premises did not constitute trespass. Nor could the intercept be understood as eavesdropping: Described in 1809 by Blackstone as the act of listening under walls or windows or the eaves of a house and framing slanderous and mischievous tales, the offence had once earned punishment of "immersion in the trebucket or ducking stool."[603] The 1967 Criminal Law Act, however, abolished this offense.[604] The right of confidentiality, still in its infant stages, also did not apply, as extension lines, private switchboards and crossed lines meant that no realistic person would expect not to be overheard when speaking on a telephone.

The plaintiff's second claim relied on Article 8 of the ECHR, which safeguarded family and private life, and Article 13: "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

---

[602] Malone v. United Kingdom, 1985 Eur. Ct. H.R. 5 (Article 50) of Apr. 26, 1985 (ser. A no. 95).

[603] Malone v. Comm'r for the Metro. Police (no. 2), (1979) 2 All E.R. 620 (Ch.) (Eng.) (Sir Robert Megarry).

[604] Criminal Law Act, 1967, c. 58, § 13 (Eng.).

Here the English court recognized a case directly on point. In *Klass v. Federal Republic of Germany*, the European Court had found that although the Federal Republic of Germany had not actually placed wiretaps on the five German citizens claiming relief, the legal structure of the German surveillance system could be addressed.[605] German law required the state to inform the citizens after the fact, where it would not jeopardize the purpose of the surveillance, that their communications had been intercepted. It also required, *inter alia*, that there be an imminent danger to state security, that other methods of obtaining the information be unavailable, and that the surveillance cease as soon as the requisite conditions cease. These safeguards meant that the statute, which fell afoul of Article 8(1), nevertheless met the criteria for exception laid out in Article 8(2). The court also required that an effective remedy before a national authority existed, bringing such measures into line with Article 13.

In contrast to the German case, English surveillance provisions, as previously noted, did not exist on a statutory basis, and so no legal remedy for violations that may occur were available. This suggested that the measures fell afoul of the ECHR. The English court, however, bristled at the suggestion that European law carried any weight in the domestic realm: "Any regulation of so complex a matter as telephone tapping is essentially a matter for Parliament, not the courts; and neither the Convention nor the *Klass* case can, I think, play any proper part in deciding the issue before me."[606] While, then, wiretapping may be "a subject which cries out for legislation," the court's hands were tied. Malone appealed to the Continent.[607]

In 1984, the European Court of Human Rights found for Malone. Justice Pettiti wrote in his concurring judgment that "the mission of the Council of Europe and its organs is to prevent the establishment of systems and methods that would allow 'Big Brother' to become master of the citizen's private life."[608] He noted the continuing "temptation facing public authorities to 'see into' the life of the citizen."[609] The United Kingdom responded with new statutes to satisfy the ECHR.

---

[605] Klass v. Fed. Republic of Germany, 2 Eur. H.R. Rep. 214 (Ser. A, no. 28) (1979).

[606] *Malone*, 2 All E.R. 620.

[607] Malone v. United Kingdom, 7 Eur. Ct. H.R. 14 (1985).

[608] Malone v. United Kingdom, App. No. 8691/79 (judgement of Aug. 2, 1984) (Pettiti, J., concurring) (translated), *available at* http://www.mannrettindi.is/the-human-rights-rpoject/humanrightscasesandmaterials/cases/regionalcases/Undirflokkureuropeancourtofhumanrights/nr/576.

[609] Malone, 7 Eur. Ct. H.R. 14.

The 1985 Interception of Communications Act made it a crime to obtain communications en route, other than as specified under statute.[610] It also established a complaints body. Any citizen, suspecting interception of their mail or telephone conversations, could file a complaint with a special tribunal, which was empowered to use judicial review mechanisms to ascertain whether the individual was, in fact, under surveillance and, if so, whether proper procedures were followed. Where an individual was not under surveillance, however, the tribunal could only confirm to the applicant that no violations had occurred. In the event of surveillance and actual violations, the tribunal informed the applicant and Prime Minister, quashed the warrant, destroyed any information intercepted, and compensated the applicant. A senior member of the judiciary served as Commissioner and generated an annual report, which, after the deletion of national security concerns, was laid before Parliament.

In the first six years of the statute's enactment, the tribunal uncovered a number of what it considered to be minor mistakes (such as the wrong phone tapped), but no blatant violations. On the whole, the number of warrants issued steadily increased.[611]

Soon after the adoption of the 1985 legislation, Westminster introduced measures to place the intelligence agencies on more secure legal footing. The 1989 and 1996 Security Services Acts and 1994 Intelligence Service Act empowered these agencies to apply through the secretary of state for telegraphic intercepts. By the mid-1990s, however, with momentum gaining ground for the incorporation of the European Convention of Human Rights into domestic law, gaps in British law remained. A landmark case reached the European Court directly on point, vividly highlighting what still needed to be done in domestic law to bring it into line with the Convention.

b. *Halford v. United Kingdom* and the Regulation of Investigatory Powers Act 2000

The Assistant Chief Constable for Merseyside, the most senior female police officer in the United Kingdom, failed eight times in seven years to obtain a promotion to Deputy Chief Constable either in Merseyside or elsewhere.[612] In 1990, she initiated proceedings in the Industrial Tribunal, claiming gender discrimination. Two years later, she finally obtained a

---

[610] Interception of Communications Act 1985, c. 56, § 1 (Scot.).

[611] *See id.*; INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 1988, Cm. 652, ¶ 8 (U.K.); *see also* HOME OFFICE, INTERCEPTION OF COMMUNICATIONS IN THE UNITED KINGDOM, 1985, Cm. 9438 at annex 2 (U.K.).

[612] Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).

hearing. To prepare for the case, the Chief of Police for Merseyside placed secret wiretaps on Ms. Halford's home and work telephones.[613]

The European court held that the interception of communications over *private* telecommunications systems fell outside the scope of the 1985 Interception of Communications Act.[614] But no remedy at either common law or within domestic statutory law existed. The European Court found therefore a violation of Article 8(1) saying phone calls made from work or home could be considered "private life" and "correspondence."[615] As it was a public authority interfering with private life and correspondence, such actions had to be taken in accordance with the law. But the domestic statutes did not provide adequate protection. The court also found that the practice violated Article 13 and awarded £10,000 in damages plus £25,000 for costs and default interest at eight percent per year.[616] The case drew attention to two problems: the codes of practice under which the police operated and the remedy such as was provided for under the law. With the 1998 Human Rights Act looming large, the case forced the Labour Government to bring forward new legislation.

In June 1999, the Home Office issued a consultation paper on the interception of communications. Although the aim, purportedly, was to establish the safeguards required by the Convention, the state used the occasion as an opportunity to update the powers claimed by the state to respond to (and take advantage of) new technologies: the Government noted in particular issues associated with the increase in the number of companies offering fixed line services, the mass distribution of mobile phones, the evolution of satellite technology, the growth of Internet communications, and the diversification of the postal network to include non-state-run companies.[617] A number of changes followed.

The state proposed to expand the interception of communications sent via post or public telecommunication systems to *all* communications by telecoms operators or mail delivery systems, and to relax warrant applications, tying them not to addresses, but to individuals, with a list of addresses and numbers attached and easily amendable by lower officials.[618]

---

[613] *Id.*

[614] *Id*.

[615] *Id.*

[616] *Id.*

[617] Regulation of Investigatory Powers Bill, 2000, H.C. Bill [64] (U.K.), *available at* http://www.publications.parliament.uk/pa/cm199900/cmbills/064/2000064.htm2.

[618] INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2001, *supra* note 600, at 9. The purpose of this was to allow for what the United States referred to at the time as "roving wiretaps," giving the state flexibility to handle situations where suspects used and discarded or frequently switched telephones.

For urgent situations, Labour would expand those granted the authority to request wiretaps from the Senior Civil Service to the Head of the Agency involved. The Labour Government wanted to expand the length of time for which a warrant operated: previously taps only stayed in place for a two month period, with monthly renewals in cases of serious crime, and on a six month basis for matters of national security or economic well-being. The state proposed to change the length of time to three months, renewed every three months for serious crime, and six months, renewed every six months for matters of national security and economic well-being.[619] The state also proposed to expand intercept authority to include private networks. The aim was to make it legal for businesses to record communications to create a paper trail of commercial transactions and business communications in the public and private sector. Where previously communications data could be turned over voluntarily, the state wanted to *compel* them to do so. The new legislation ultimately forced Internet Service Providers ("ISPs") to attach devices to their systems to enable communications to be intercepted while in-route.[620] This move reversed the principle of innocent until proven guilty, with ISPs automatically re-routing all Internet traffic—from email to click streams—to the Government Technical Assistance Centre at MI5's London headquarters.[621] No effort was made to insert any form of *prior* judicial sanction into the process. Again, it should be noted that none of these alterations addressed concerns raised by the European Court. Rather, they represented expansions in existing powers. The Regulation of Investigatory Powers Act ("RIPA") became the primary legislation for surveillance and the interception of communications.[622]

c. Effectiveness of Safeguards

While RIPA served to *expand* the authorities claimed by the state to intercept communications, it should be remembered that the original impetus was actually to introduce *safeguards* on privacy to bring British law into line with the Convention. The legislation did create judicial and administrative oversight functions and established a complaints tribunal to

---

[619] This brought the interception of communications into the same timeframe as intrusive surveillance device provisions, discussed in the subsequent text.

[620] *See* Young, *supra* note 427, at 313.

[621] *Your Privacy Ends Here*, OBSERVER (U.K.), June 4, 2000, *available at* http://observer.guardian.co.uk/ focus/story/0,6903,328071,00.html.

[622] Regulation of Investigatory Powers Act, 2000, c. 23 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts2000/20000023.htm. While Halford helped to stimulate this piece of legislation, other factors also played a role. *See* Yaman Akdeniz et al., *Bigbrother.gov.uk*: *State Surveillance in the Age of Information and Rights*, CRIM. L. R. (U.K.), Feb. 2001, at 73.

protect, in particular, private information.[623] However, significant questions can be raised about the effectiveness of these safeguards.

First, consider the annual reports. Like those generated under the 1985 Interception of Communications Act, reports on the use of the powers by law enforcement issued by the Interception of Communications Commissioner ("ICC") post-RIPA refer to a "significant number of errors" in the operation of the intercepts.[624] These center on human error or technical problems, which resulted in the destruction of the information intercepted. But they do not address substantive violations. The portions of the reports that might have sensitive information remain classified. As for the annual report generated on the intelligence services by the Intelligence Services Commissioner, this document stands out in its use of the cut-and-paste function, simply repeating from year to year the legal authorities under which the intelligence services conduct surveillance. The handful of paragraphs addressing errors made by the intelligence services (which, each year, can be counted on one hand) carry language to the effect, "[a]s it is not possible for me to explain any details of these breaches without revealing information of a sensitive nature, I have referred to them in more detail in the confidential annex."[625] The reviewers frequently assure the public, however, that what errors exist are solely due to administrative hiccups and were conducted in good faith. The law requires the

---

[623] In addition to the oversight function provided by the Commissioners, which I address in the following text, RIPA created a nine-member Investigatory Powers Tribunal, which replaced the Interception of Communications Tribunal, Security Service Tribunal, and Intelligence Services Tribunal, as well as complaints function under Police Act 1997 Commissioner and Human Rights Act claims. This body has not found any violations of RIPA or the 1998 HRA. *See, e.g.*, INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2003, H.C. 883, at 6-7 (U.K.), *available at* http://www.archive2.official-documents.co.uk/document/deps/hc/hc883/883.pdf.

[624] Regulation of Investigatory Powers Act; INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2000, H.C. 1047, at 5-6 (U.K.), *available at* http://www.archive2.official-documents.co.uk/document/deps/hc/hc1047/1047.pdf. As of the present time, under RIPA 2000, there are four commissioners: the Interception Commissioner (replacing the Commissioner under IOCA 1985; previously a High Court judge: Lord Lloyd, 1986-91; Lord Bingham. 1992-93, Lord Nolan, 1994-2000, and Lord Justice Swinton-Thomas, 2001-06), the Intelligence Services Commissioner (replacing two different commissioners under the Security Services Act 1989 and ISA 1994), the Investigatory Powers Commissioner for Northern Ireland, and a Chief Surveillance Commissioner (who has functions under the Police Act 1997, now Parts II and III of RIPA). They have not been combined into one Commission, which would ensure clear lines of accountability.

[625] INTELLIGENCE SERVICES COMMISSIONER, REPORT, 2002, H.C. 1048 at 8 (U.K.), *available at* http://www.archive2.official-documents.co.uk/document/deps/hc/hc1048/1048.pdf; *see also* INTELLIGENCE SERVICES. COMMISSIONER, REPORT, 2003, H.C. 884 at 8 (U.K.), *available at* http://www.archive2.official-documents.co.uk/document/deps/hc/hc884/884.pdf.

Investigatory Powers Commissioner for Northern Ireland, who focuses on the operation of the security services in the province, to lay annual reviews of the surveillance powers before the Northern Ireland Assembly. However, the legislation specifies that the commissioner may exclude any information that may be prejudicial to the prevention or detection of serious crime or the continued discharge of the functions of any public authority.[626] This appears to be a rather large chunk of material, as precious little information is made public. Annexes to the Chief Surveillance Commissioner's annual review, the Interception of Communications Commissioner's annual review, and the Parliamentary Intelligence and Security Committee, which performs oversight of MI5, MI6, and GCHQ, are confidential.

Second, the broader information made public tells us little about the powers specifically as related to terrorism and national security—the rather large loophole provided by Article 8(2) of the ECHR. The ICC, for instance, does not disclose the number of warrants issued by either the Foreign Secretary or the Secretary of State for Northern Ireland—the two secretaries most likely to be dealing with terrorism. The rationale, as laid out by the Birkett Committee, is that "[i]t would greatly aid the operation of agencies hostile to the state if they were able to estimate even approximately the extent of the interceptions of communications for security purposes."[627] The government does not consider a similar risk, however, to accompany the release of information related to warrants issued by the Home Secretary or the First Minister for Scotland, nor does it consider the release of information related to property warrants, and broken down into offences that include drug crimes, terrorism, and the like, to compromise the state.

Third, while the ICC and Intelligence Services Commissioner inspect the agencies engaged in the interception of communications, the results of their inspections remain secret.[628]

---

[626] Regulation of Investigatory Powers Act §§ 57-61.

[627] BIRKETT REPORT, *supra* note 568, ¶ 121.

[628] The legislation also creates the position of Interception of Communications Commissioner ("ICC"), to review the exercise and performance of the Secretary of State. Twice a year the ICC visits the Security Service, Secret Intelligence Service, GCHQ, NCIS, Special Branch of Metropolitan Police, Strathclyde Police, Police Service for Northern Ireland, HM Customs and Excise, Foreign and Commonwealth Office, Home Office, Scottish Executive and MoD. These organizations forward a complete list of warrants issued since the last visit; the Commissioner then selects which cases he would like to inspect—sometimes at random, sometimes for specific reasons. The ICC reviews the files, supporting documents, and the product of the interception to ensure that the procedure complies with RIPA. He also speaks to the Home Secretary, Secretary of State for Northern Ireland,

Fourth, while RIPA also provided for a tribunal to function as a complaints body and to oversee remedies for violation of the statute, its effectiveness also can be questioned. Under RIPA, the new Investigatory Powers Tribunal assumed jurisdiction over the areas previously addressed by the Interception of Communications Tribunal, the Security Service Tribunal, and the Intelligence Services Tribunal. It also took over the complaints function assigned to the Commissioner under the 1997 Police Act, as well as complaints lodged under the Human Rights Act. On no occasion did the tribunal find in favor of an applicant.[629] The net result is that the previous breakdown in information regarding the cases forwarded to the court has become obfuscated, with only the total number of complaints made available.[630]

Against the above concerns is the fact that some aspects of the legislation *did* formalize what before had been general guidelines adopted, exercised, and modified by the Secretary of State. To this extent, the changes offered increased procedural protections. Part I of RIPA reiterated from the 1985 legislation, for instance, that it was a criminal offence for any person, without lawful authority, to intercept any communication sent via public post or telecommunication in the course of their transmission.[631] To be lawful, interception must be undertaken in accordance with a warrant issued by the Secretary of State. The grounds for granting the warrant collapsed national security, preventing or detecting serious crime,

---

Secretary of State for Defence, and First Minister for Scotland. In 2003, the Commissioner also visited communications service providers (such as the Post Office and major telephone companies), which are the entities responsible for executing the warrants. Critics look at this, and the Home Secretary's refusal to state publicly the average amount of time spent examining warrant requests, as evidence that the Secretary simply rubber stamps applications. *See, e.g.*, Letter from Mr. Simon Davies, Dir., Privacy Int'l, to the Rt. Hon. Sir Swinton Thomas, Interception of Commc'ns Comm'r (July 31, 2002) (U.K.), *available at* http://www.privacyinternational.org/countries/uk/surveillance/pi-letter-swinton2.html.

[629] *See, e.g.*, Regulation of Investigatory Powers Act; INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2001, *supra* note 600, at 4; INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 2000, REPORT ¶ 32 (U.K.), *available at* http://www.archive.official-documents.co.uk/document/ cm47/4778/4778.htm.

[630] *See* INTELLIGENCE SERVICES. COMMISSIONER, REPORT, 2003, *supra* note 625, at 7-8; INTELLIGENCE SERVICES COMMISSIONER, REPORT, 2001, H.C. 1244, at 7, *available at* www.ipt-uk.com/docs/rep_intel_ser_comm.pdf. INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT, 2001, *supra* note 600, at 2-3; INTERCEPTION OF COMMUNICATIONS COMMISSIONER, REPORT: REGULATION OF INVESTIGATORY POWERS ACT, 2000, Cm. 5296, at 10 (U.K.), *available at* http://www.privacyinternational.org/countries/uk/surveillance/inter-comm-report-2000.pdf.

[631] Regulation of Investigatory Powers Act § 1; *see* Interception of Communications Act 1985, c. 56, §§ 1(1), 1(2)(s), 2(2) (U.K.), *available at* http://www.archive.official-documents.co.uk/ document/cm47/4778/4778.htm.

safeguarding the economic well-being of the United Kingdom (in relation to persons outside the British Islands), or giving effect to any international mutual assistance agreement in relation to serious crime, into one category.

The statute requires the Secretary of State to be satisfied that no other reasonable means exists for obtaining the same information. The conduct authorized must be proportionate to that sought to be achieved. The warrant must specify the conduct that will be undertaken, how related communications data will be obtained, and the individuals who must assist in giving effect to the warrant. Those authorized to request interception warrants include the Director-General of MI5, the Chief of MI6, the Director of GCHQ, the Director General of the National Criminal Intelligence Service, the Commissioner of the Police of the Metropolis, the Chief Constables of the Northern Ireland and Scottish police forces, the Commissioners of Customs and Excises, the Chief of Defence Intelligence, and, for cases involving mutual assistance, any competent authority of countries outside the United Kingdom.[632] It is up to the Secretary of State to examine and approve the number of persons to whom the material is made available and the extent to which the information is released or copied, as well as the number of copies made.[633] Overall, the new legislation did force the agencies conducting intercept activities to conform to and ensure their practices were in accord with the legal authorities.

It is not clear whether other elements carried over from the Home Office guidelines offer greater or less protection for British subjects. What is important, however, about these is that their codification in law does not offer *greater* protection to the targets of surveillance than existed prior to the European Court's findings. For example, the statute excludes any information gathered—or the information that it had been gathered—from being used as evidence in court.[634] Anyone revealing it becomes subject to criminal penalties.[635]

Arguments can be made both ways as to whether the exclusion of intercepts benefits or hurts targets of surveillance. On the one hand the state can use the information to find a place and time where further information could be obtained. The fruits of such surveillance remain admissible. On the other hand, private aspects of an individual's life, even those not at all related to the crime suspected, may enter the surveillance record. This provision thus prevents such information from surfacing

---

[632] Regulation of Investigatory Powers Act § 6.

[633] *Id.* § 15.

[634] *Id.* § 17. The legislation exempted proceedings before the Tribunal, the Special Immigration Appeals Commission, or the Proscribed Organisations Appeal Commission.

[635] *Id.* § 19.

directly in a court of law. But, back to the first hand, keeping the surveillance out of court means that the means of surveillance writ largely remains cloaked—which is, of course, the primary argument put forward for preventing it from entering official records. The state is reluctant to provide information about the authorities' capabilities, which would give an advantage to those engaged in terrorism and other serious crime.[636] The inclusion of this limitation has proven to be highly controversial, with multiple reviews arguing for its repeal, but the state has held its course.[637]

3. Covert Surveillance: Intrusive, Directed, Covert Human Intelligence Sources

Covert surveillance, or electronic bugging, occurs when the target of the surveillance is unaware of its existence. Like the relationship of the intelligence agencies to the interception of communications, Home Office guidelines, not statutes, governed law enforcement's use of electronic surveillance throughout most of the 20th century. Part III of the 1997 Police Act introduced the first statutory controls, including a Code of Practice on Intrusive Surveillance, which entered into force in February 1999.[638] Similarly, until 1994, no law regulated MI5's use of covert surveillance. That year the Intelligence Services Act required authorization by the Secretary of State.[639] RIPA amended and expanded these statutes. Before delving into the details of the current authorities, however, it is helpful to first look at a case considered by the European Court of Human Rights, which demonstrates where the authorities introduced between 1989 and 1997 fell short of Convention demands.

---

[636] *See* 400 PARL. DEB., H.C. (6th Ser.) (2003) 588 (U.K.).

[637] *See e.g.,* PRIVY COUNSELLOR REVIEW COMMITTEE, REPORT: ANTI-TERRORISM, CRIME AND SECURITY ACT REVIEW, 2005, H.C. 100, at 9, (U.K.) *available at* http://www.statewatch.org/news/2003/dec/atcsReport.pdf; HOME AFFAIRS SELECT COMMITTEE, MINUTES OF EVIDENCE (2003) (U.K.) (testimony of Lord Carlile of Berriew QC on Mar. 11, 2003), *available at* http://www.publications.parliament.uk/pa/cm200203/cmselect/cmhaff/515/3031101.htm; *see also* 614 PARL. DEB., H.L. (5th Ser.) (2000) 111 (U.K.); LORD LLOYD, INQUIRY INTO LEGISLATION AGAINST TERRORISM, 1996, Cm. 3420, c. 7 (U.K.).

[638] R v. Khan (Sultan), [1997] A.C. 558 (1996) (appeal taken from Eng. A.C.); *see also*, R v. Khan (Sultan), 2 CHRLD 125, n.4 (1996). Various non-statutory codes of practice also were developed at this time by the Association of Chief Police Officers in England and Wales, the Association of Chief Police Officers in Scotland, and HM Customs and Excise. The Code has been replaced by the Covert Surveillance Code of Practice (Surveillance Code) issued under the Regulation of Investigatory Powers Act, 2000, c. 23, § 71(5) (U.K.), *available at* http://www.opsi.gov.uk/acts/acts2000/20000023.htm.

[639] Intelligence Services Act 1994, c. 13, § 5(2) (U.K.), *available at* http://www.opsi.gov.uk/ACTS/acts1994/Ukpga_19940013_en_1.htm.

a. *Khan v. United Kingdom*

On March 14, 1994, English courts sentenced Sultan Khan, a British national, to three years in prison for dealing drugs. The case relied heavily on information obtained from an electronic bug that the police placed in his home.[640] The Appeal Courts dismissed his appeal but raised the issue as a point of law whether the product of covert surveillance could be introduced as evidence in a criminal trial. Although the House of Lords again dismissed the appeal, it addressed the question at hand. The Lords asserted that English law admitted of no right to privacy writ large—and that, even if such a right did exist, common law required that improperly obtained evidence be admitted at trial, according to judicial discretion. Lord Nolan, writing for the majority, added, "[t]he sole cause of this case coming to the House of Lords is the lack of a statutory system regulating the use of surveillance devices by the police." He continued, "[t]he absence of such a system seems astonishing, the more so in view of the statutory framework which has governed the use of such devices by the Security Service since 1989, and the interception of communications by the police as well as by other agencies since 1985."[641]

In January 1997, Kahn lodged a complaint with the European Commission of Human Rights, claiming, *inter alia,* a violation of Article 8, focusing on the right to respect for private life, and Article 13, requiring an effective domestic remedy. In April 1999, the European Court agreed to hear the case. The Court held that the surveillance in question clearly violated Article 8(1).[642] The question was whether it fell sufficiently within Article 8(2)—namely, whether it was "in accordance with the law" and "necessary in a democratic society" for one of the purposes specified in that section. Drawing on *Halford*, the court noted that "in accordance with the law" required both compliance and attention to whether it reflected the rule of law. The court recognized that this meant, amongst other things, that the law had to be sufficiently clear as to inform the public of the authorities claimed by the state. But no statutory scheme existed. The Home Office guidelines that governed covert surveillance neither carried the force of law, nor could the public directly access them. The Court unanimously ruled that the practice violated Article 8. The Court also found in the applicant's favor with respect to the claim under Article 13: while the English judiciary could have excluded the evidence under the Police and Criminal Evidence

---

[640] R v. Khan (Sultan), 2 CHRLD 125 (1996).

[641] *Id.*

[642] Khan v. United Kingdom, 31 Eur. H.R. Rep. 45 (2001); *see also* Hewitson v. United Kingdom, 37 Eur. Ct. H.R. 31 (2003).

Act, the only redress to violations of that statute was to file a complaint with the Police Complaints Authority—hardly an impartial body.[643] On May 12, 2000, the Court awarded Khan £311,500.[644]

b. 2000 Regulation of Investigatory Powers Act

Khan dealt with the state of law prior to the RIPA and revealed in stark contours the difference between British practice and European standards. In the interim, RIPA addressed this disparity by creating a new regime to address electronic bugging. As with the interception of communications, however, the Government did not just address the issues raised by the European court; instead, it used the occasion as an opportunity to expand on the existing guidelines to allow for broader surveillance authority.

Part II of the legislation focuses on the three categories of covert surveillance established in the 1997 Police Act: intrusive surveillance, directed surveillance, and covert human intelligence sources. The levels of authorization that must be obtained, and the circumstances under which public authorities can authorize information gathering, vary depending on the category, and the entity undertaking the surveillance. The legislation covers operations undertaken by MI5, MI6, and GCHQ, as well "public authorities," which encompasses more than 950 entities. These entities range from local authorities and health trusts, to the National Crime Squad and the Metropolitan Police. In 2004, the Government further expanded the number of public authorities to which the legislation applied, bringing such varied bodies as the Postal Services Commission and Office of Fair Trading under its remit.[645]

The first area, intrusive surveillance, covers any covert search conducted on residential property or in private vehicles, in which either an individual or device collects the information. Gadgets not physically located on the property or in the car, which deliver the same quality of information as though the instrument were physically present, count as intrusive. The authorizing officer must be assured that the surveillance is necessary on the grounds of national security, or to prevent or detect serious crime. The statute also requires that the officer be satisfied that the

---

[643] *See* Police and Criminal Evidence Act, 1984, § 78 (U.K.), *available at* http://www.opsi.gov.uk/si/si1988/Uksi_19881200_en_1.htm.

[644] The court also awarded VAT for costs and expenses, minus any funds obtained from legal aid. *See* Khan v. United Kingdom, http://www.chiark.greenend.org.uk/pipermail/ukcrypto/2000-May/010446.html

[645] Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order, 2003, S.I. 2003/3171, art. 2 ¶ 17 (U.K.), *available at* http://www.opsi.gov.uk/si/si2005/20051084.htm.

operation is proportionate to its aim. Outside of emergency situations, the approval of a Commissioner is required prior to implementation.[646]

Although the legislation established Commissioners to oversee the process, once again question can be raised as to how much of an impact they have. In the first year of the statute's operation, for instance, the Commissioners only refused prior approval in one case (out of 371 authorizations for property interference and 258 authorizations of intrusive surveillance).[647] The Commissioners did not overturn any of the forty-six emergency authorizations. Outside of prior approval, the commissioners also have the ability to terminate an authorization or renewal where either no reasonable grounds exist for believing that the authorization meets the required criteria, or where an emergency authorization is found to be wanting. In the first year of the statute's operation, the Commission refrained from overturning any intrusive surveillance warrants. In his annual review of these powers, Andrew Leggatt interpreted these numbers as indicating "that applications continue to be properly considered by the agencies before they are authorized."[648] This trend continued.[649]

The second category, directed surveillance, focuses on information sought in the course of an investigation or operation where private data is likely to be gathered. Electronic bugs placed in work areas or non-private

---

[646] Subsequent guidelines constructed by the Commissioners' office state that it is not necessary to obtain authorization through the Secretary of State when hostages are involved; the suspects in such circumstances are considered to be engaged in crime, thus stripping them of any claim to privacy. The victims, in turn, would be unlikely to object to any invasion of their privacy if it meant being freed from captivity. CHIEF SURVEILLANCE COMMISSIONER, REPORT TO THE PRIME MINISTER AND TO SCOTTISH MINISTERS, 2002-2003, H.C. 1062, at 4 (U.K.), *available at* http://www.archive2.official-documents.co.uk/document/ deps/ hc/hc1062/1062.pdf.

[647] The reason for refusal centered on timing: the public authority initiated the surveillance *prior* to obtaining commission approval, as required by law.

[648] Police Act 1997, ch. 50 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts1997/1997050.htm; CHIEF SURVEILLANCE COMMISSIONER, *supra* note 646. The 2002-03 report states, "I am satisfied that such authorizations continue to be treated seriously by the authorities concerned." *Id.*

[649] CHIEF SURVEILLANCE COMMISSIONER, *supra* note 646; *see also* CHIEF SURVEILLANCE COMMISSIONER, ANNUAL REPORT TO THE PRIME MINISTER AND TO SCOTTISH MINISTERS, 2003-2004, H.C. 668, at 11 (U.K.), *available at* http://www.surveillancecommissioners.gov.uk/docs1/annualreport2003-04.pdf. These numbers do not include renewals, which, at least in regard to the Police Act, are increasing: 437 in 2001-2002, 543 in 2002-2003. CHIEF SURVEILLANCE COMMISSIONER, *supra* note 646, at 3. The total renewals are decreasing, however, in intrusive surveillance: from 102 in 2001-2002, the total dropped to eighty in 2002-2003. *Id.* at 4. In his annual review of these powers, the Chief Commissioner, Andrew Leggatt, attributed this decline and the drop in urgent requests to "improved knowledge and efficiency as well as to an increasing familiarity with the requirements of authorization." *Id.* at 3.

vehicles fall into this category. The process for obtaining warrants duplicates intrusive surveillance requirements. But there are two critical differences in the criteria considered in this process: First, unlike intrusive surveillance, the senior authorizing officer, or (for intelligence services) Secretary of State, does not need to take into account whether the information could reasonably be obtained by other means; second, the number of entities who can request a directed warrant is significantly broader than those who can request an intrusive one. This links to the broader number of aims such warrants can seek. Where intrusive warrants are limited to issues of serious crime, national security, and the economic well-being of the United Kingdom, directed warrants may, in addition to these, be directed towards public safety, the protection of public health, the assessment or collection of taxes or duties, and any other purpose specified under order by the Secretary of State. Accordingly, orders of magnitude *more* authorizations are made for directed surveillance than for intrusive. In 2001, for instance, public authorities and intelligence agencies obtained some 28,000 directed authorizations, as opposed to 493 intrusive ones.[650]

The third category, covert human intelligence sources (CHIS), addresses the process via which public authorities develop relationships with individuals in order to facilitate the secret transfer of information. As with intrusive surveillance, proportionality is required. The statute requires that the public authority establish a manager for day-to-day contact with the CHIS, a handler for general oversight, and a registrar to maintain records on the source, and that access to the records be limited to a need-to-know basis. CHIS authorizations include the broader aims of directed surveillance, extending the utilization of such information-gathering powers to public safety, public health, the collection of taxes, and other purposes as may be issued under order by the Secretary of State. On average, public authorities and the intelligence services recruit between five and six thousand new sources annually. For all three of these categories, authorization lasts for three months, with three-month renewals possible. In an emergency, authorization can be granted for a seventy-two-hour period.

The role of the Commissioners here again draws attention. Arguments could be made that the oversight conducted by the office is significant: Records of all surveillance must be kept by the public authority for review by the Commissioners. But, again, in the rare instance that the Commission does quash an authorization (only a handful of instances in the five years

---

[650] In 2004, the state narrowed this requirement for local authorities to only allow them to conduct direct surveillance or use CHIS for preventing crime or disorder. Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003 (U.K.), *available at* http://www.opsi.gov.uk/si/si2003/draft/20037759.htm.

that have elapsed since RIPA), law enforcement and public authorities can appeal to the Chief Surveillance Commissioner. And the standard of review here is remarkably weak: where the Chief Surveillance Commissioner is satisfied that reasonable grounds exist for believing that the requirements had been satisfied, he can modify the Commissioner's decision. There is, though, some oversight of this: the Chief Surveillance Commissioner then reports his findings directly to the Prime Minister.[651]

In addition to the reporting of statistics and review of applications for authorization, the Commissioners also conduct general inspections of law enforcement and public authorities making use of the powers. Again, an argument could be made that this is an effective function: the Surveillance Commissioners annually inspect approximately 60 law enforcement entities and 270 public authorities. With this rigorous schedule, as of the time of writing, all 442 local authorities in Great Britain have undergone at least one inspection. However, the results of these inspections are not made public. Rather, the Commission forwards a report to the Chief Officer and, where necessary, requests that the entity develop an action plan to address any issues raised. Some flavor of these reviews comes through in the Commissioner's annual report. Here he has highlighted a number of bad practices, such as "insufficiently specific applications and authorizations, exceeding the terms of the authorization, delegation of reviews by authorizing officers, codes of practice not readily available to practitioners and inadequate RIPA training and education."[652] The inspections also revealed a significant number of basic errors, such as the entry of wrong addresses, mistakes in the vehicle identification numbers specified in the authorization, and the use of the procedures for intrusive surveillance when the situation warranted only directed surveillance authority.

The importance of these reviews is not to be underestimated; it is likely that the presence of "inspectors" external to these agencies creates a certain relationship within which errors in the application of these powers can be addressed. This is something. But the insistence that reports on these agencies be made available only to the entity being inspected somewhat detracts from our ability to judge its effectiveness.

4. Encrypted Data

Section III of the Regulation of Investigatory Powers Act appears somewhat at odds with Labour's stated goal of making Britain "the most e-

---

[651] Regulation of Investigatory Powers Act, 2000, c. 23, § 38-38 (U.K.), *available at* http://www.opsi.gov.uk/acts/acts2000/20000023.htm.

[652] CHIEF SURVEILLANCE COMMISSIONER, *supra* note 649, at 11.

friendly country in the world" by 2002.[653] With virtually no public discussion prior to its introduction, this portion of the legislation addresses the issue of encrypted electronic data. The statute creates a duty on individuals possessing the key to disclose the information where necessary for reasons of national security, preventing or detecting crime, or in the interests of the economic well-being of the United Kingdom. It may also be required where the information sought is central to the exercise of public authority, statutory power, or statutory duty. In either case, the duty of disclosure must be proportionate to what is sought to be achieved by its imposition, and it must be the only reasonable way in which the information can be obtained.[654] Criminal penalties with up to two years imprisonment and a fine follow violations of the statute. The legislation makes it illegal to tip off others that the state is seeking the information.[655] This is treated as even more serious of an offence than not providing the keys, carrying up to five years imprisonment and a fine as a penalty. The Act creates a duty on law enforcement and public authorities to use the keys only for the purpose for which they are sought, as well as to store them in a secure manner. The records of the keys must be destroyed as soon as the key is not longer needed to decrypt the information.[656]

Although the powers were supposed to begin in 2004, the Home Office deferred implementation of Part III. Leggat writes,

> [t]he use of information security and encryption products by terrorist and criminal suspects is . . . not yet as widespread as had been expected when the legislation was approved by Parliament four years ago. Meanwhile the National Technical Assistance Centre (a facility managed by the Home Office to undertake complex data processing) is enabling law enforcement agencies to understand protected electronic data, so far as necessary. I am assured that the need to implement Part III of RIPA is being kept under review.[657]

As of the time of writing, Part III of RIPA remained in abeyance.

The upshot of this section is that while MI5 would still need a warrant to read the content of the information obtained from ISPs, such authorization is *not* necessary for the agency to monitor patterns, such as web sites visited, to and from whom email is sent, which pages are downloaded, of which discussion groups a user is a member, and which

---

[653] *Your Privacy Ends Here*, *supra* note 621.

[654] Regulation of Investigatory Powers Act § 49.

[655] *Id.* § 54.

[656] *Id.* § 55.

[657] CHIEF SURVEILLANCE COMMISSIONER, *supra* note 649, at 3 (statement by the Rt. Hon. Sir Andrew Leggatt), *available at* http://www.spy.org.uk/spyblog/2004/07/annual_report_of_the_chief_sur.html.

chat rooms an individual visits. It is too early to gauge how these powers will measure up against the ECHR. Nor is it clear how the European Court will respond to the gag orders included in the legislation. Their practical effect is that if an individual is approached for an encryption key, and she has forgotten the code, she cannot even inform her family of why she is being taken away by the police and charged.

What makes the section of particular note is the transferred burden of proof: it is not the state that must prove that an individual has the key, but the accused that must prove that they have forgotten it. The statute assumes the accused's guilt. Both business and civil liberties groups object to the legislation, which the Government presented with little public discussion and no evidence about the level of threat posed over the Internet by terrorists, pedophiles, and other criminals. Nor did the Government present evidence that would suggest that the need for these measures outweighs their impact on privacy.

B. POST-9/11: THE 2001 ANTI-TERRORISM, CRIME AND SECURITY ACT

After formal inquiry and extensive public debate, in 2000 the United Kingdom introduced permanent counter terrorist legislation. Prior to that time (albeit since the 19th century) counterterrorist measures existed on a temporary basis.[658] Despite the recent comprehensive terrorism package, following 9/11, pressure to expand state power resulted in further legislation. The 2001 Anti-terrorism, Crime, and Security Act ("ATCSA") had the feel of stale leftovers; powers that the security and intelligence forces had attempted to acquire previously but which they had been unable to obtain.[659] While much of the statute has very little to do with terrorism, some sections are directly relevant to our current discussion. I will here briefly address Part III, which allows for the exchange of information between government entities, and Part XI, which augments the surveillance powers contained in RIPA.

RIPA, it will be recalled, prevents information collected via covert surveillance from being used in court. Part III of the ATCSA does not repeal this, but it allows public bodies to disclose information to *assist* in criminal investigations or proceedings either in the United Kingdom or abroad (including inquiries into whether charges ought to be initiated or investigations brought to an end).[660] The legislation also allows Inland

---

[658] *See* LAURA K. DONOHUE, COUNTERTERRORIST LAW AND EMERGENCY POWERS IN THE UNITED KINGDOM 1922-2000 (2000).

[659] Anti-terrorism, Crime and Security Act, 2001, c. 24 (U.K.).

[660] *Id.* §§ 17-20. While the Secretary of State may prevent disclosure of information under the ATCSA to overseas jurisdictions that do not offer an "adequate" level of

Revenue and Customs and Excise to disclose information to the intelligence and security agencies. This means that the information gathered for counterterrorist purposes can be distributed to organizations with a considerably different remit than those gathering the data.[661]

As reflected in the catch-all nature of the statute itself, many of the information exchanges that have already occurred have little to do with terrorism. Between January 2002 and September 2003, for instance, only four percent of the disclosures made by Inland Revenue to police and intelligence services under Part 3, Section 19 of the ATCSA related to terrorism.[662] In contrast, forty-six percent (9,157 disclosures) related to sex offences, and twenty-four percent (4,848 disclosures) related to drug offences.[663] This phenomenon is not singular to Inland Revenue: during the same period, only twenty-one percent of the disclosures made by Customs and Excise related to terrorism.[664] Observing the use of these powers, the Privy Counsellor Review Committee concluded, "these provisions are, in our view, a significant extension of the Government's power to use information obtained for one purpose, in some cases under compulsory powers, for a completely different purpose."[665]

Part XI of the 2001 ATCSA augmented the surveillance powers in the 2000 RIPA. It requires that communication service providers retain data for a specified period, in order to ensure that requests made under 2000 RIPA can be fulfilled. Some scholars attribute the inclusion of this passage to lobbying done by NCIS on behalf of the police, Customs and Excise, the Security Service, SIS, and GCHQ, which called for a minimum twelve-month retention by the CSP, followed by six-year storage, either in-house or by a Trusted Third Party.[666] What is fascinating about the expansion is the rationale offered by NCIS:

> Communications data is crucial to the business of the Agencies. It is pivotal to reactive investigations into serious crime and the development of proactive

---

protection, the exact parameters that would require this finding remain less than clear.

[661] PRIVY COUNSELLOR REVIEW, *supra* note 637, at 43-44. As the parliamentary body reviewing the measure notes, "information obtained by public authorities under statutory powers conferred for one purpose may be disclosed to the police and intelligence and security agencies to be used for completely different legitimate purposes . . . ." *Id.* at 43.

[662] *Id.* at 44.

[663] *Id.*

[664] *Id.* at 44.

[665] *Id.* at 45.

[666] Clive Walker & Yaman Akdeniz, *Anti-terrorism Laws and Data Retention: War is Over?*, 54 N. IRELAND LEGAL Q. 159, 162 n.21 (2003) (citing ROGER GASPAR, NCIS SUBMISSION TO THE HOME OFFICE; LOOKING TO THE FUTURE: CLARITY ON COMMUNICATIONS DATA RETENTION LAW 9 (2000), *available at* http://cryptome.org/ncis-carnivore.htm).

> intelligence on matters effecting not only organized criminal activity but also national security. At the lower level, it provides considerable benefit to the detection of volume crime . . . . Short term retention and the deletion of data will have a disastrous impact on the Agencies' intelligence and evidence gathering capabilities.[667]

This language suggested a general data mining approach to the detection of crime—startlingly similar to its U.S. counterpart.[668]

In order to carry out the retention provisions, the ATCSA empowered the Secretary of State to issue a voluntary code of practice, a draft of which the Home Office published in March 2003, to be followed by implementation via statutory instrument. In the event that the code proves inadequate to force communication service providers to turn over information, the legislation empowers the Secretary of State to issue compulsory directions.[669] In the case of a recalcitrant service provider, civil proceedings for an injunction or other relief may be initiated by the Secretary of State.[670]

Like so many information-gathering authorities in the USA PATRIOT Act, the ATCSA does not limit the information retained to terrorism data. A late amendment required that the information "may relate directly or indirectly to national security" for prosecution—however, "may" also suggests "may not."[671] There is some evidence that the purpose may be for entirely different reasons: the Government opposed the amendment at the time.[672] Counsels' advice to the Information Commissioner on the data retention provisions in the ATCSA noted that it is "an inevitable consequence of the scheme envisaged by ATCSA that communications data" retained for an extended period will be "available for production in accordance with a notice issued under [S]ection 22 RIPA for a purpose with no connection whatever to terrorism or national security."[673]

---

[667] Walker & Akdeniz, *supra* note 666, at 163.

[668] While Lord Rooker formally denied this language in the House of Lords, similar claims proliferate. *See* 629 PARL. DEB., H.L. (5th ser.) (2001) 770 (U.K.).

[669] Anti-terrorism Crime and Security Act, 2001, c. 24, §§ 102-04 (U.K.), *available at* http://www.opsi.gov.uk/ACTS/acts2001/20010024.htm**;** *see also* S. A. Mathieson, *The Net's Eyes are Watching*, GUARDIAN ONLINE (U.K.), Nov. 15, 2001, http://www.guardian.co.uk/internetnews/story/0,7369,593920,00.html.

[670] Walker & Akdeniz, *supra* note 666, at 170. While the 1998 Data Protection Act and 1999 Telecommunications (Data Protection and Privacy) (citing THE HOME OFFICE, REGULATORY IMPACT ASSESSMENT: RETENTION OF COMMUNICATIONS DATA ¶¶ 21-23 (2001) (U.K.)).

[671] Walker & Akdeniz, *supra* note 666, at 166.

[672] *Id.*

[673] Anti-terrorism, Crime and Security Act 2001: Retention and Disclosure of Communications Data Summary of Counsels' Advice, ¶ 13 (U.K.), available at http://www.privacyinternational.org/countries/uk/surveillance/ic-terror-opnion.htm.

The requirement that data be retained received a boost the following year when the European Union issued a directive regarding the processing of personal data and the protection of privacy in the electronic communications sector. Echoing Article 8 of the ECHR, Article 15(1) allows for the information to be archived in the interests of national security, defense, or public security, or the prevention or detection of criminal offences.[674]

The ATCSA, however, retains considerably more information than is necessary, while it remains relatively easy for individuals committed to anonymity on the Internet to dodge state grasp. Although traditional email systems include the name of the sender and the receiver, with login and password information, it is entirely possible for other people to access these accounts. Various email systems, such as Earthlink, Hotmail, and Yahoo! allow individuals to obtain accounts under aliases. A user can access these via public terminals, thus remaining anonymous. Individuals surfing the web can use sophisticated browsers that cover their trail. Guardster.com "offers free anonymous internet web surfing to everyone."[675] Other sites, such as Anonnymizer.com, the-cloak.com, and anonymous.com offer similar services. Special programs, such as Anonymity 4 Proxy, allow a user to scan servers and confirm their anonymity.[676] Users can obtain fake IP addresses, block cookies, and change their browsers to masque any personal information. It is unlikely that those engaged in terrorism will forego these relatively accessible tools to ensure that their communications escape state grasp. This introduces concerns about whether the measures introduced are proportionate.

The concern regarding proportionality becomes even more pronounced when examined in light of the ability to introduce statutory instruments under RIPA to expand the number of entities who can demand the stored communications to include non-national-security-related public authorities. Leading and Junior Counsel from Matrix Chambers advised the Information Commissioner, upon being approached for analysis:

> There is, in Counsel's view, no doubt that both the retention of communications data on behalf of a public authority, and the disclosure of such data to a public authority

---

[674] *See* Council Directive 2002/58/EC, 2002 O.J. (L 201) 37-47 (E.C.), *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf (Directive on privacy and electronic communications) (concerning the processing of personal data and the protection of privacy in the electronic communications sector).

[675] Welcome to Guardster, http://www.guardster.com (last visited June 9, 2006).

[676] *See* Anonymity 4 Proxy (A4Proxy)—Web Anonymizing Software for Surfing with Privacy, http://www.inetprivacy.com/a4proxy/ (last visited June 9, 2006).

> constitute an interference with the right to respect for private life and correspondence enshrined in Article 8(1) of the European Convention of Human Rights.[677]

Indeed, the European Court has found that "states do not enjoy unlimited discretion to subject individuals to secret surveillance or a system of secret files. The interest of a State in protecting its national security must be balanced against the seriousness of the interference with an applicant's right to respect for his or her private life." The court continued,

> there has to be at least a reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate. To refer to the more or less indiscriminate storing of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern is . . . evidently problematic.[678]

The European Court also reads the convention to require that the new measures be necessary. However, the 2001 ATCSA, introduced nine months after the 2000 Terrorism Act came into effect, could hardly be said to have addressed a serious gap in the law. There simply wasn't enough time to establish this, and certainly no evidence to this effect has been made public since.[679]

C. ANONYMITY AND SURVEILLANCE IN PUBLIC SPACE: CCTV

Just as the United States, understandably, is taking advantage of new technologies to expand its surveillance powers, so too is the United Kingdom. The country leads the world in the concentration of public surveillance devices.[680] Eight years ago the British government appropriated £153 million to develop a closed circuit television ("CCTV") network.[681] By 2003, two and a half million, or roughly ten percent of the globe's total CCTVs operated on British soil.[682] According to *National*

---

[677] Anti-terrorism, Crime and Security Act 2001: Retention and Disclosure of Communications Data Summary of Counsels' Advice, *supra* note 673, ¶ 15.

[678] Walker & Akdeniz, *supra* note 666, at 174 (citing Rotaru v. Romania, App. No. 28,341/95, 2000 Eur. Ct. H.R. 192 (Wildhaber, J., concurring)).

[679] The only cases made available in an attempt to convince Internet companies to retain records cited instances in which records more than fifteen months old were sought in non-national security-related investigations. *See* Stuart Miller, *Internet Providers Say No to Blunkett*, GUARDIAN (U.K.), Oct. 22, 2002, at 9.

[680] The cameras were first introduced into the U.K. in 1956. Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1080 (1997).

[681] COUSENS, *supra* note 565, at 59-60.

[682] Mark Townsend & Paul Harris, *Security Role for Traffic Cameras*, THE OBSERVER (U.K.), Feb. 9, 2003, at 2.

Geographic, in 2004, this number topped four million.[683] The net effect is substantial: Each person traveling through London is caught on film approximately three hundred times per day.[684] These devices do not just watch and record; some use facial recognition technology to scan the public against a database of persons sought by the state.[685] In East London alone, approximately three hundred cameras incorporate this technology.

The system aims at deterring and detecting ordinary crime—and increasing residents' sense of security. But statistics are not available to evaluate how effective the cameras have been in meeting these goals. Until recently, CCTV had not yielded the capture or conviction of a single terrorist.[686] Following the King's Cross bombing in July 2005, however, police review of CCTV tapes played a significant role in piecing together the events leading up to the attack and helped to identify a suspected handler.

London is not alone in its surveillance efforts. Scotland maintains approximately ten thousand cameras to monitor traffic speed and parking structures.[687] Some seventy-five cities in total have public CCTV systems, with a number of private actors following suit.[688] The cameras have overwhelming support: approximately ninety-five percent of all local governments regard it as a viable means to enforce the law.[689] In Newham, England, for instance, where thirty million dollars went into installing the devices, police claimed an eleven percent drop in assaults, a forty-nine percent drop in burglary, and a forty-four percent drop in criminal damage through the end of 1994.[690] These statistics, however, are not without

---

[683] David Shenk, *Watching You*, NAT'L GEOGRAPHIC MAG. Nov. 2003, at 16.

[684] *Privacy vs. Security: Electronic Surveillance in the Nation's Capital: Hearing before the Subcomm. on the D.C of the Comm. on Government Reform*, 107th Cong. 2 (2002) (statement of Rep. Constance A. Morella, Chairman) [hereinafter *Privacy vs. Security Hearing*].

[685] Facial recognition technology is form of biometric ID. Algorithms map relationships between facial features, can ID from live video or still images, up to a thirty-five degree angle, and compensates for light conditions, glasses, facial expressions, facial hair, skin color, and aging. *Find Criminals, Missing Children, Even Terrorists in a Crowd Using Face Recognition Software Linked to a Database*, PRNEWSWIRE, Nov. 16, 1998.

[686] *Privacy vs. Security Hearing*, *supra* note 684, at 2.

[687] Joyce W. Luk, Note, *Identifying Terrorists: Privacy Rights in the United States and United Kingdom*, 25 HASTINGS INT'L & COMP. L. REV. 223, 229 n.33 (2002) (citing Alastair Dalton, *Controls Urged on Big Brother's All-Seeing Eyes*, SCOTSMAN, July 23, 1998, at 9).

[688] These private cameras have given rise to a voyeuristic industry, with footage from toilet cams, gynocams, and dildocams tending to end up on the Internet. *See* Luk, *supra* note 687, at 229.

[689] *See* Luk, *supra* note 687, at 228 (citing Burrows, *supra* note 680, at 1099).

[690] *See* Luk, *supra* note 687, at 228 (citing John Deane, *CCTV Boost Follows Crime-*

controversy. Some suggest that the drop in crime experienced by these cities could be due to a host of factors, undertaken at the same time, as well as part of a general trend in decreased crime even in areas where cameras are lacking.

The legal regime that governs the use of CCTV centers on the 1998 Data Protection Act. This section briefly considers this statute and the phenomenon of CCTV in the context of the European Convention of Human Rights. It concludes with a brief consideration of the proliferation of these devices in the United States.

1. Data Protection Act 1998

The primary legislation governing CCTV is the 1998 Data Protection Act ("DPA"). The statute incorporates rights of access to information and regulates data controller behavior. It also provides special exceptions, among which is national security.[691]

Data controllers, in this case, those overseeing CCTV, must act in accordance with eight principles: fair and lawful processing, the acquisition of information only for specific and lawful purposes, and the processing of information only in a manner compatible with that purpose. The information gathered must be proportionate to the purpose for which it is processed, and those obtaining the data may not hold the information any longer than necessary for the stated purpose. The legislation grants targets of surveillance particular entitlements—such as the right to know when a controller is processing their personal data, and the ability to prevent the information from being used for direct marketing. The statute requires that no significant decision impacting the information be made solely via automation. The target has the right to require the destruction of inaccurate information. And the legislation allows subjects to go to court to remedy a breach of the measure.

In keeping with RIPA 2000, the Chief Commissioner recommended that where CCTV is to be used at a crime hotspot, if it is likely that private information will be gathered, the police apply for directed surveillance. The Commissioner's assumption is that a judge will go easier on public authorities where they have sought a warrant.[692]

Fighting Success, PRESS ASS'N NEWSFILE, Oct. 13, 1995).

[691] Data Protection Act 1998, c. 29, § 1 (U.K.), *available at* http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm.

[692] CHIEF SURVEILLANCE COMMISSIONER, *supra* note 652 (statement by the Rt. Hon. Sir Andrew Leggatt).

2. European Courts

While the European Court has not adjudicated the general presence of the cameras, it ruled against Britain's use of footage. In *Peck v. United Kingdom*, the facts of which occurred prior to the 1998 Human Rights Act, CCTV caught the applicant wielding a knife in preparation for suicide. The police immediately went to the scene and prevented the applicant from hurting himself. Although the police did not charge the applicant with a criminal offence, the local council later released the tape to the media, which aired footage of him with the knife (but not the actual suicide attempt) on national television. The government also used a photograph of the applicant as part of a public relations exercise to demonstrate the effectiveness of the cameras. The state did not mask the applicant's identity when it released the information to the public.

When the applicant's efforts to seek relief through the domestic judicial system failed, he appealed to the European Court. The British government asserted that because the event occurred in public, the state's action had not compromised the applicant's Article 8 right to a private life. The Court noted that the applicant was not a public figure and not attending a public event. Rather, in a state of considerable distress, he was walking late at night. Although disclosure had a basis in law,[693] was foreseeable, and sought to uphold public safety and the prevention of crime, it failed on the grounds of proportionality. The council could have tried to mask the applicant's identity, or it could have sought his consent. Advertising the effectiveness of the system did not present a compelling enough reason to violate Peck's rights under Article 8. It also determined the lack of domestic remedy to be a violation of Article 13. In 2003, the Court awarded Peck €11,800 for non-pecuniary damages, and €18,705 for expenses.[694]

In handing down its decision, the Court emphasized the importance of recording the information: had the cameras simply been observation devices, the monitoring of public space would not give rise to privacy concerns. The recording of the information, however, even though it was a public arena, mattered, and the dissemination of the material meant that a much broader audience than would otherwise be witness to the action became aware of it.

---

[693] The High Court had held that under the Criminal Justice and Public Order Act 1994, x. 163, the local council could use CCTV to prevent crime; and through the Local Government Act 1972, s. 111, could distribute the footage. *See* COUSENS, *supra* note 565, at 56.

[694] Peck v. United Kingdom (44647/98), 36 Eur. Ct. H.R. (2003); *see also* R v. Brentwood BC [1998] EMLR. 697 (U.K.).

3. CCTV in the United States

Similar CCTV systems are beginning to spring up in the United States, but no legislation even approximating the Data Protection Act exists on this side of the Atlantic. Washington, D.C., for instance, plans to take advantage of more than one thousand video cameras "all linked to central command station accessible to not only the District police but the FBI, the Capitol Police, the Secret Service, and other law enforcement agencies."[695] The public only learned about the placement of these devices, and plans for expanding the system, after the initial group had been put into place. What began as thirteen cameras owned by the Metropolitan Police Department became linked to several hundred cameras in schools and public transportation.[696] The National Park Service, in turn, spent some two to three million dollars to install cameras at major memorial sites on the mall.

In 2002, at the first congressional hearings to be held into the matter, Chief of Police Charles Ramsey said that the department only made use of the cameras twenty-four seven during heightened alert or large scale events.[697] The National Park Service, as of the time of the hearings, had yet to decide how long to keep the recordings. The associate regional director of the National Capital Region, National Service, John Parsons, tied the existence of these cameras to the terrorist threat: "We are convinced by studies and consultants that these icons of democracy are high targets for terrorist activities. And that is the sole reason that have [sic] made the decision to go forward with planning for these cameras."[698]

Chicago presents an even more extreme case. As of the time of writing, police have the ability to monitor some two thousand cameras.[699] By 2006, the city will have added another 250.[700] What makes these numbers even more significant than Washington, D.C. is the technology attached: software programs will cue the cameras, which are trained on sites considered terrorist targets, to alert the police automatically when anyone wanders in circles, lingers outside, pulls a car over onto a highway shoulder, or leaves a package and walks away.[701] The camera immediately highlights the people so identified. The city consciously modeled the

---

[695] *Privacy vs. Security Hearing*, *supra* note 684, 1 (statement of Rep. Constance A. Morella, Chairman).

[696] *Id.* at 1-2.

[697] *Id.* at 21 (statement of Chief of Police Charles Ramsey).

[698] *Id.* at 48.

[699] Stephen Kinzer, *Chicago Moving to 'Smart' Surveillance Cameras*, N.Y. TIMES, Sept. 21, 2004, at A18.

[700] *Id.*

[701] *Id.*

system after London, as well as systems in place in Las Vegas and currently being used by Army combat teams.[702] When implemented, it will be one of the most sophisticated in the world, particularly with respect to its ability to monitor the thousands of cameras in motion. Dispatchers who receive the image will have the ability to magnify the image up to four hundred times. And the total cost to the city? $5.1 million for the cameras, and another $3.5 million for the computer network.[703] Mayor Daley boasted, "[t]his project is a central part of Chicago's response to the threat of terrorism, as well as an effort to reduce the city's crime rate." But he also acknowledged, "[i]t . . . subjects people here to extraordinary levels of surveillance. Anyone walking in public is liable to be almost constantly watched."[704] Discussing plans to place cameras on public vehicles, such as street sweepers, Daley defended the eye of the state: "We're not inside your home or your business. The city owns the sidewalks. We own the streets and we own the alleys."[705]

As of the time of writing, more than sixty urban centers in the United States use CCTV for law enforcement purposes.[706] Baltimore has perhaps the most extensive system.[707] But it is not just large cities that have jumped on the train. Yosemite Airport, for instance, combines CCTV with facial recognition technology to scan for terrorists.[708] These systems make it increasingly difficult for individuals to retain their anonymity as they move through public.

There are legitimate law enforcement interests in such surveillance, such as to prevent and detect crime, reduce citizens' fears, and aid in criminal investigations. Yet even electronic surveillance companies admit that, "[o]verall, it is fair to say that no jurisdiction is currently keeping the kind of statistical data that can be analyzed in such a way to demonstrate the effect of CCTV."[709]

---

[702] *Id.*

[703] *Id.*

[704] *Id.*

[705] *Id.*

[706] Luk, *supra* note 687, at 227 (citing Mark Boal, *SpyCam City*, VILL. VOICE, Oct. 6, 1998, at 38). Some of these have become incorporated into the infotainment industry, with footage appearing on reality programs such as *COPS*. *Id.* at 227.

[707] *See id.* (citing Mark Hansen, *No Place to Hide*, 83 A.B.A.J. 44, 44-45 (1997)).

[708] Pelco News Release, Oct. 26, 2001, *available at* http://www.pelco.com/company/newsreleases/2001/102601.aspx.

[709] *Privacy vs. Security Hearing*, *supra* note 684, at 107 (statement of Richard Chace, Executive Dir., Sec. Indus. Ass'n (SIA), which represents over 400 electronic secuirty manufacturers, distributors, service providers).

III. POLICY CONSIDERATIONS

Having looked at surveillance authorities and programs on both sides of the Atlantic, we turn now to a brief discussion of the risks of doing nothing and, with these in mind, policy options that present themselves.

A. RISKS

Alan Westin, in his seminal work on privacy, predicted that advancing technologies would give the government unprecedented power.[710] Early computer science entrepreneurs shared Westin's concern. In 1961, for instance, Richard Benson warned that when all the data could be collected together, the state could control citizens' lives: "Where information rests is where power lies, and . . . concentration of power is catastrophically dangerous."[711] In 1962, Richard W. Hamming, of Bell Telephone Labs, asked what safeguards could be introduced to prevent information from being used for purposes other than intended.[712]

Articles on privacy began to appear in academic journals, and in 1965, the Gallagher Subcommittee in the House of Representatives announced its intent to look into the issue of data surveillance. (The final report, however, did not look at digital surveillance.) When a 1965 Social Science Research Council ("SSRC") committee report suggested that the federal government create a National Data Center for socio-economic information, the public went ballistic.[713] The issue that the SSRC was trying to address was how to provide services more efficiently. Senator Long responded to the report with a series of hearings. He concluded:

> The files of the Internal Revenue Service, the Social Security Administration, the Veterans' Administration, the Defense Department, the Federal Housing Administration, and the Agriculture Department, to name but a few, already contain about all there is to know on almost every American. To store all this information in a

---

710

> [T]he increased collection and processing of information for diverse public and private purposes, if not carefully controlled, could lead to a sweeping power of surveillance by government over individual lives and organizational activity. As we are forced more and more each day to leave documentary fingerprints and footprints behind us, and as these are increasingly put into storage systems capable of computer retrieval, government may acquire a power-through-data position that armies of government investigators could not create in past eras.

WESTIN, *supra* note 16, at 158.

711 *Id.* at 299, n.1 (citing N.Y. POST, Apr. 16, 1961).

712 *Id.* at 299, n.2 (citing *Man and the Computer*, N.Y. TIMES, Jan. 1, 1962).

713 *Id.* at 317.

> computer where it could be collected and retrieved at a moment's notice gives rise to serious questions relative to privacy.[714]

Senator Long turned out to be wrong: the intervening years have proven that the information then available, far from being "all there is to know on almost every American," turned out to be but a drop in the bucket. The range of information available in digital form eclipses that which could be amassed in the 1970s: voting records, medical information (genetic vulnerabilities, past and current illnesses or disorders, infectious diseases), commercial and consumer data (on-line banking, E-commerce, credit cards, travel, food, entertainment), business records, scholastic achievement, library materials, newspaper and magazine subscriptions, electronic communications, and a host of other types of material can now be collected. The number and extent of projects designed to harvest this data is nothing short of staggering.

It is important to have information on terrorist organizations. However, granting the state the power to collect data beyond individualized suspicion, making a broad range of public and personal information unrelated to criminal charges available to the government, and engaging in data mining, eliminate anonymity and move the state from physical and data surveillance and into the realm of psychological surveillance. This shift, enabled by counterterrorism claims, raises issues that go beyond terrorist threats and are of consequence to conservative and liberal alike.[715] Unfortunately, in calculating such costs, the analysis frequently stops at "security or freedom." A more accurate picture would examine the host of interrelated rights and state mechanisms affected by, and the unintended consequences that follow from, these measures. They raise substantive concerns and have far-reaching effects on the political, legal, social, and economic fabric of the state.

1. Substantive

At a substantive level, perhaps the most important consideration is the possibility of inaccurate information becoming part of an individual's permanent digital record. Here, concerns can be raised about the extent to which systems on either side of the Atlantic include within them adequate safeguards. The lack of openness, absence of public access, and denial of due process mean that individuals on whom information is gathered have

---

[714] *Id.* at 318 (citing *Invasions of Privacy (Government Agencies) Hearings Before Subcomm. on Administrative Practice and Procedure of the S. Judiciary Comm.*, 89th Cong., 1613 (1965) (temporary transcript)).

[715] *Compare, e.g.*, William Safire, *Privacy in Retreat*, N.Y. TIMES, Mar. 10, 2004, at A27, *with* STANLEY & STEINHARDT, *supra* note 503.

little opportunity to confront their digital accusers. The use of multiple sources of information also raises issues related to records matching—a problem that has come out in spades in the operation of the "No Fly" list post-9/11.

Substantive difficulties also arise when one takes into account third party collection points. Systems are only as good as the entity gathering the information. Yet a host of possibilities, from deliberate entry of false information and the acquisition of data under circumstances of duress (e.g., torture), to simple mistake, could corrupt the data, making its use in further analysis somewhat of a moot point. But many of the current systems neither ensure accuracy in third party collection, nor identify the collection point to allow later users of the data to go back to verify the information—much less to ensure the same does not happen as data transfers through the system. Moreover, as noted above, the target rarely knows the data has been gathered, making challenges unlikely. This danger becomes even more pronounced when one considers the possibility that hackers may deliberately penetrate data systems to alter or retrieve information.

In the United States, some question exists as to whether inaccurate data could be used to convict individuals of criminal offences. The Supreme Court has found, for instance, that the exclusionary rule does not apply to errors made by court employees.[716] In his dissent, Justice Stevens admonished that the court's position "overlooks the reality that computer technology has changed the nature of threats to citizens' privacy over the past half century."[717] Justice Ginsburg, also dissenting, referred to the "potential for Orwellian mischief" represented by increasing reliance on technology.[718] We do know that many mistakes are made. Twenty years ago, the FBI conducted a study which revealed that approximately twelve thousand inaccurate reports on suspects wanted for arrest were being transmitted daily. Databanks have since increased in size.[719] The problem of mistake is not limited to American shores: As Part II discussed, the United Kingdom's annual reviews of surveillance powers are replete with observations about basic errors committed by the police and intelligence services.

One final consideration in regard to the substantive data issues centers on a contextual data merger. Here lie concerns about taking information gathered for one specific purpose and applying it to another purpose.

---

[716] Arizona v. Evans, 514 U.S. 1 (1995).

[717] *Id.* at 22 (Stevens, J., dissenting).

[718] *Id.* at 25 (Ginsburg, J., dissenting) (quoting State v. Evans, 866 P.2d 869, 872 (Ariz. 1994), *rev'd*, 514 U.S. 1 (1995)).

[719] STRUM, *supra* note 89, at 133.

Different meanings may emerge in this process, with conclusions that may bear little or no resemblance to reality. Problems arise here particularly when real consequences for individual rights follow.

Not only is there a problem with the transfer of the wrong information, but the shadow of too much information also looms large. As one Privy Counsellor Review committee commented:

> The East German Government may have had files on a quarter of their population, but it failed to predict or prevent its own demise. If there is too much information, it can be difficult to analyse effectively and so can generate more leads than can be followed up or trigger too many false alarms.[720]

These substantive concerns plague the collection of large swathes of information.

2. Political

The political impact of the power to obtain such a broad range of information ought not be underestimated. The concentration of this power in the executive influences the balance in power between the different branches of government.[721] In the past, such accumulations of power have been used for political reasons, ensuring the dominance of the sitting government. From Hoover to Nixon, and beyond, private information became an instrument of control. The veil drawn over access to this information may become an impenetrable wall, with the Judiciary—or the Legislature—loath to second-guess those responsible for ensuring national security. Executive privilege and access to confidential information may prove sufficient to convince the other branches (and, indeed, the public writ large) of the truth of national security claims. Assertions regarding the presence of WMD in Iraq, by both the United States and United Kingdom, provide only the latest example in a long series. In *Korematsu v. United States*, the Judiciary deferred to executive claims regarding privileged information to allow the widespread detention of Americans of Japanese decent during World War II.[722] The secret materials turned out not to exist. In the United Kingdom, the "S" Plan, waved in front of Parliament in 1939, allegedly detailed a communist link with Irish republicanism. This document became the basis on which extreme counterterrorist measures swept through Westminster.

---

[720] Note that KPMG criticized the SAR regime for just this reason: the low signal to noise ratio/over-reporting. PRIVY COUNSELLOR REVIEW COMM., *supra* note 665, at 25-26.

[721] *See also* Roger Clarke, *Information Technology and Dataveillance*, *in* CONTROVERSIES IN COMPUTING 10 (C. Dunlop & R. Kling eds., 1991), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html.

[722] 332 U.S. 213 (1944).

History also demonstrates, particularly in the American context, the widespread use of these powers not just to counter national security threats, but to prevent dissent. In the United States, the witch hunt against Communists resulted in actions being taken against civil rights leaders, the women's movement, and various political parties that disagreed with the *status quo*. Such an atmosphere may discourage citizens from engaging in public discourse, impacting the democratic nature of the state. It may also prevent academics, or those who comment on public policy, from doing so publicly. This means that bad policies may go unexamined, undermining the ability of the state to operate in the most efficient and effective manner possible.

One of the technologies developed under TIA was the ability of the state to scan a crowd for deviant behavior—as an early indicator of terrorism. Liberalism, however, is founded on the idea of individual expression, and tolerance for diversity. These undoubtedly would be affected once such a plan is put into place. Added to these considerations is the possibility that information gathered for one purpose will be used for other reasons. In Redwood City, California, for example, in late 1995 the police began installing listening devices to detect gun fire. The police later admitted that these microphones enabled them to listen in to conversations in private dwellings.[723] With surveillance information masked from public scrutiny, it becomes more difficult to uncover the misuse of such capabilities. More specifically, counterterrorist provisions that allow the gathering of such data rarely include strictures on the manner in which it can be used.

3. Legal

The widespread collection of information also impacts the legal system. It shifts the burden in proof. No longer must the state demonstrate individualized suspicion in order to target individuals and invade their privacy; instead, everyone in society becomes suspect, forced to defend themselves when the state reaches its (potentially entirely mistaken) conclusions. The Data Encryption provisions of Britain's RIPA provide a good example: if an individual does not provide the keys upon request, rather than the state having to show that the individual has access to the information sought, the person must prove that his or her memory has failed. And the consequence, up to two years imprisonment, is substantial.

Broader legal issues are felt in both the American and English constitutions. In the United States, these provisions provide a way for the

---

[723] STRUM, *supra* note 89, at 134.

state to dodge the requirements of the Bill of Rights. Instead, the Executive acts under Article II considerations, claiming considerable leeway in implementing its decision. In the United Kingdom, the national security exception, and the blending of crime, terrorism, and national security, alter individual entitlements. While rights related to physical interference with property might continue to be protected in a manner commensurate with the British constitutional tradition, the interception of communications is different in kind. Orders of magnitude *more* information can so be garnered, with significantly greater inroads into privacy, giving the state greater entrée into the psychology of persons in the United Kingdom.

4. Social

Perhaps the greatest impact of the loss of anonymity and movement into psychological surveillance is felt in the social sphere. The widespread collection of information creates an atmosphere of suspicion. This is not a new phenomenon.[724] The problem is that surveillance powers reside in the hands of state officials, are exercised in secret, the extent of their impact is unknown, and no reasonable opportunity to object presents itself. This leaves much to speculation, such as the degree to which private rights are invaded, and whether such powers are necessary. Where information is made public, however, such as in the United Kingdom in 1844, or again in 1957, public concern abates. The significant expansion in technology, and broader state access to private information, again has raised concerns. As the United Kingdom's Interception of Communications Commissioner wrote in 2001, "[m]any members of the public are suspicious about the interception of communications, and some believe that their own conversations are subject to unlawful interception by the security, intelligence or law enforcement agencies."[725] In light of the secrecy that surrounds the collection of such information, the Commissioner's subsequent assurance, "I am as satisfied as I can be that the concerns are, in fact, unfounded," carries little weight.

---

[724] In 1844, a secret Committee of the House of Commons noted "the strong moral feeling which exists against the practice of opening letters, with its accompaniments of mystery and concealment." BIRKETT REPORT, *supra* note 568, ¶ 133. The committee added,

> [t]here is no doubt that the interception of communications . . . is regarded with general disfavour . . . . Whether practised by unauthorized individuals or by officials purporting to act under authority, the feeling still persists that such interceptions offend against the usual and proper standards of behaviour as being an invasion of privacy and an interference with the liberty of the individual in his right to be 'let alone when lawfully engaged upon his own affairs.'

Id.

[725] INTERCEPTION OF COMMUNICATIONS COMMISSIONER, 2001, *supra* note 600, at 2-3.

The United States proves no exception to the rule. The public appears somewhat less than enamored with the sweeping powers contained in the USA PATRIOT Act. Resolutions against this legislation have been passed in 401 cities and counties in forty-three different states, including five state-wide declarations.[726] Cities that have condemned the broader surveillance measures include New York City and Washington, D.C.—the targets of the 9/11 attacks. The federal legislature, picking up on this sentiment, had introduced by the end of 2003 nearly a dozen amendments to mitigate some of the more egregious provisions. From left to right, privacy advocates voiced their concern: in October 2002, House Majority Leader Dick Armey referred to DOJ as "the biggest threat to personal liberty in the country." House Judiciary Committee Chairman, Representative James Sensenbrenner, threatened to subpoena the Attorney General to get answers to questions about DOJ's use of the powers. Conservative commentators, such as William Safire, found themselves in the same camp as liberal icons, such as Senator Edward Kennedy. And strange bedfellows began emerging. Conservative leader Bob Barr, for instance, became a formal advisor to the ACLU—which invited the head of the National Rifle Association to address its annual membership conference.

These developments forced Ashcroft to go on the offensive. He initiated a speaking tour in 2003 to defend the USA PATRIOT Act.[727] The DOJ launched a website called "Preserving life and liberty," which defended the government's use of the legislation.[728] In an irony that appears lost on DOJ, the home page *defending* the expansive surveillance provisions includes a "privacy policy," which reads:

> If you visit our site to read or download information, we collect and store the following information about your visit:
>
> > The name of the Internet domain (for example, 'xcompany.com' if you use a private Internet access account, or 'yourschool.edu' if you are connecting from a university's domain) and the IP address (a number that is automatically assigned to your computer when you are using the Internet) from which you access our site;
> >
> > The type of browser and operating system used to access our site;

---

[726] American Civil Liberties Union, List of Communities That Have Passed Resolutions, http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11294&c=207 (last visited June 9, 2006).

[727] *See, e.g.*, Jeff Johnson, *Congressional Opponents Lash Out at PATRIOT Act, Ashcroft*, CNSNEWS.COM, Sept. 25, 2003, http://www.cnsnews.com/ViewNation.asp?Page=%5CNation%5Carchive%5C200309%5CNAT20030925a.html; *Learning Activity*, CNN STUDENTNEWS, Sept. 8, 2003, http://www.cnn.com/2003/fyi/news/09/07/learning.patriot.act.101/.

[728] U. S. Dep't of Justice, Preserving Life and Liberty, http://www.lifeandliberty.gov/ (last visited June 9, 2006).

> The date and time you access our site;
>
> The Internet address of the Web site from which you linked directly to our site; and
>
> The pages you visit and the information you request.[729]

The web site continues, "In certain circumstances . . . we may take additional steps to identify you based on this information and we may share this information, including your identity, with other government agencies."[730] The government's "privacy policy" appears to be to invade it.

Outside of undermining the population's confidence in the state writ large, the social impact reverberates in the relationship of the population to law enforcement. Creating adversarial relationships may have lasting effects on the state's ability to provide basic services. A startlingly good example here comes from the United States, where the TIPS program sought to train first responders and firefighters to report on "suspicious" behavior. Pressure also mounted on the police to begin collecting and reporting information relating to immigrant communities. These professions have access to private residences and so are in a better position to gather information otherwise masked from state view. The problem, of course, is that if people think that firefighters, or police for that matter, are coming to spy on them and possibly to turn them in to the authorities, people will not call them. It will create an adversarial relationship, making the provision of basic services—which have nothing to do with terrorism and perhaps everything to do, amongst other things, with health, fire, and domestic abuse—that much more difficult.

Another risk centers on the impact of widespread psychological surveillance on social control. In the 20th century, the United States undertook a wide range of programs to try to get inside peoples' heads and to find ways to control them.[731] Despite, or perhaps because of, the outright

---

[729] *Id.*

[730] *Id.*

[731] In Project CHATTER, run from 1947-1953, the Navy administered "truth drugs" (Anabasis aphylla, scopolamine, and mescaline) to people in the United States and overseas. Project BLUEBIRD/ARTICHOKE, run by the CIA from 1950 to 1956, investigated "the possibility of control of an individual by application of special interrogation techniques." Here, hypnosis and sodium pentothal provided the means of choice. MKULTRA, overseen by the CIA from 1950 to the late 1960s, attempted to manipulate human behavior through chemical and biological weapons, as well as "additional avenues to the control of human behavior . . . [such as] radiation electroshock, psychology, psychiatry, sociology, and anthropology, graphology, harassment substances, and paramilitary devices and materials." *Church Committee Vol. 5*, *supra* note 98, at 390. The Army undertook extensive LSD testing towards the same ends. These projects began as efforts to defend the United States, but this purpose soon became subordinate to perfecting techniques, "for the abstraction of

violations of individual rights that occurred, intelligence agencies made deliberate efforts to prevent citizens from even knowing about these programs. The CIA Inspector General wrote in 1957:

> Precautions must be taken not only to protect operations from exposure to enemy forces but also to conceal these activities from the American public in general. The knowledge that the Agency is engaging in unethical and illicit activities would have serious repercussions in political and diplomatic circles and would be detrimental to the accomplishment of its mission.[732]

It would be somewhat naïve to assume that similar efforts to get inside terrorists heads so as to prevent them from acting before they do so (a self-stated aim of TIA, as well as the 2002 National Security Strategy) could avoid similar issues related to social control and secrecy, with significant effects on the social structure of the state.

The impact that surveillance programs may have on the equality of privacy further compounds the issue. Not *all* citizens will be subject to psychological profiling, but, once certain traits are identified (likely linked to age, religion, country of origin, nationality, or ethnicity), only certain portions of the population will lose degrees of privacy otherwise afforded the majority. Feelings of inequality and claims of injustice may make these groups less prone to participate in civic structures and less able to take advantage of state services when needed.

Still other social concerns present themselves. Perhaps one of the most serious is that past transgressions may become a scarlet letter, emblazoned on citizens' chests, "visible to all and used by the . . . powerful . . . to increase their leverage over average people."[733] This would make the concept of paying one's dues—and then moving forward with a fresh start—somewhat obsolete. Another way to see this is through the lens of self-realization; Westin notes, "[p]art of the value of privacy in the past was that it limited the circulation of recorded judgments about individuals, leaving them free to seek self-realization in an open environment."[734] The relentless collection, storage, and recall of such information may make it difficult for people to overcome the past and to see themselves in a different light.

---

information from individuals whether wiling or not." *Id.* at 393.

[732] *Id.* at 394.

[733] STANLEY & STEINHARDT, *supra* note 503, at 14.

[734] WESTIN, *supra* note 16, at 323.

5. Economic

On the economic front, extensive surveillance may have the effect of discouraging innovation or harming commercial activity.[735] Encryption, for example, is an essential part of commercial security, allowing companies to develop strategies, make bids, and price parts and services, without their competitors' knowledge.[736] The interception of this information, particularly in finance, where money ends up simply a matter of "bits and bytes," may be devastating.[737] It may also raise difficult diplomatic issues: European alarm about Echelon rests in part on concern about economic espionage.[738]

Limits on the development of encryption may hurt domestic security firms' abilities to compete on the international market. In recent congressional hearings, Sam Gejdenson, the ranking member of the House Subcommittee on International Economic Policy and Trade, suggested that the current situation mirrors Dick Cheney's efforts, when Secretary of Defense, to prevent the Secretary of Commerce from lifting controls on 286 computers—at a time when any civilian could buy a 386 at Radio Shack in Beijing.[739] He added, "[t]here is a recent *New York Times* story of a German company basically sending its appreciation to the American Government and the restrictions we placed on encryption because we are about to make them really rich."[740]

Encryption demands may also harm national security interests writ large. As John Gage of Sun Microsystems related to Congress:

> [O]ur concern is that the systems we use for air traffic control, controlling of the power grid, control of the trading floors where $1 trillion a day is traded in New York, in Tokyo, even a momentary disruption there brings chaos to world financial markets.

---

[735] This is not to say that good reasons for a state to want to have access to encrypted data do not exist: Aum Shin ri Kyo, for instance, used encryption to mask computer files that contained plans to carry out a biological attack on the United States. Dorothy E. Denning & William E. Baugh, Jr., *Encryption in Crime and Terrorism*, *in* CYBERWAR 2.0: MYTHS, MYSTERIES AND REALITY 167 (Alan D. Campen & Douglas H. Dearth eds., 1998). Ramzi Yousef, a member of al Qaida partially responsible for the 1993 attack on the World Trade Center, encrypted files that detailed plans to bomb eleven planes over the Pacific Ocean. *Hearings on Encryption Before the H. Comm. on International Relations*, 105th Cong. (1997) (testimony of FBI Director Louis J. Freeh).

[736] DIFFIE & LANDAU, *supra* note 215, at 42.

[737] *Id.*

[738] *See supra* notes 406-409.

[739] *Encryption: Individual Right to Privacy vs. National Security: Hearing before the Subcommittee on International Economic Policy and Trade of the Committee on International Relations*, 105th Cong. (1997) [hereinafter *Encryption Hearing*].

[740] *Id.* at 3.

> . . . [I]t is real world stuff. And what do we have today? We have insecure operating systems, insecure networks, and a wonderful 1976 invention.[741]

Tom Parenty, the Director of Security at Sybase Corporation, added, "[t]he broad use of cryptography in U.S. software products is indispensable in protecting all of the infrastructures upon which all of our lives depend."[742] It does seem that the claims of law enforcement and the intelligence community have been a bit overstated. In the United States, federal and state officials are required to report when electronic surveillance encounters encryption.[743] In 2000, twenty-two state cases and zero federal cases encountered masked material. In no case was an investigation inhibited.[744] Overseas, the reason Part III of RIPA is not yet in effect is precisely because it has not become an issue.

B. OPTIONS

A common charge levied against articles that discuss surveillance centers on the "perilous times" argument: "[W]hat would you have us do when faced by a significant threat—particularly from terrorism?" While it is not the intention of this article to provide an exhaustive analysis of the policy options available, this section briefly sketches six alternatives that merit further discussion: (1) the creation of a property right in personal information; (2) the regulation of access, transfer, use, and retention of data with remedies for violations; (3) the scaling back of existing powers; (4) delimiting what constitutes "national security"; (5) providing safeguards and oversight functions; and, (6) eliminating sunset provisions. The combination of these would minimize intrusiveness, maximize fairness, and still allow the state to respond in an effective manner to terrorist challenge.

Perhaps the most intriguing option centers on the creation of a property right in personal information. An idea put forward in the mid-20th century by Alan Westin, this would amount to the "right of decision over one's private personality."[745] The handling of that information by another would create certain duties and liabilities: "With personal information so defined,

---

[741] *Id.* at 48. Gage went on to surf the Internet in front of the committee, showing them strong encryption programs available from Finland, Croatia, Sweden. *Id.*; *see also* OFFICE OF TECH. ASSESSMENT, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE OTA-BP-ITC-149, GP STOCK #052-003-01418-1, at 25-26 (1995), *available at* http://www.askcalea.com/docs/digitalage.pdf; DIFFIE & LAUDAU, *supra* note 215, at 23;

[742] *Encryption Hearing*, *supra* note 739, at 33.

[743] 18 U.S.C. § 2519(2)(b) (2000).

[744] STATISTICS DIV., ADMIN. OFFICE OF THE U.S. COURTS, 2000 WIRETAP REPORT 11 (2001), *available at* http://www.epic.org/privacy/wiretap/stats/2000_report/2000wttxt.pdf.

[745] WESTIN, *supra* note 16, at 324.

a citizen would be entitled to have due process of law before his property could be taken and misused by government or by agencies exercising such enormous public power that they would be held to the same rules as government."[746] Thus, whenever certain systems obtain data, the individual would have an opportunity to examine it, to challenge its accuracy (possibly in an administrative proceeding, with judicial oversight), and to answer such allegations as might be made. Upon administrative and judicial direction, the answer may either be appended to the information or, if found convincing, prevent the original data from being retained.

At a minimum, it would seem an opportune moment to reconsider the state of privacy law writ large, particularly in the United States. Regulating the collection, transfer, and retention of data, while providing a remedy for violations of existing law, would go some way towards addressing many of the concerns this article raises raise. Different interested parties advocate a number of guidelines to this effect. Without going through each, I present those that I find most compelling.

First, no personal information should be collected in the first place without the explicit permission of the individual involved, or without the entity seeking the information clearly identifying its purpose in doing so. Only those authorized to enter data into the system may do so, with their traceable identity linked to the data throughout its life. This will allow for later challenge should the data be used in a manner detrimental to the rights of the subject. Second, unless the target so consents, no personal information can be shared with other institutions or organizations (either public or private) for reasons other than that for which the data was collected. In these circumstances, both parties would provide notice that the sharing had occurred. Third, where the state seeks access, it would have to demonstrate a compelling need for the data. Here, consideration might be given to the role of the judiciary or an executive arbitration body in determining access. Fourth, those entities handling personal information would be required to enact security measures to prevent unauthorized access. Fifth, and finally, adequate enforcement mechanisms would have to be created to ensure the above. This would mean both oversight functions and a remedy for violations of the regulations. As in the United Kingdom, the oversight functions would include four types: independent annual reviews, individual audits, and complaints tribunals, as well as legislative oversight. Remedies may range from criminal penalties and damages to injunctions—including the sanction of losing access to the system. These

---

[746] *Id.* at 325.

mechanisms would enshrine the twin principles of transparency and accountability.

Consistent with the thrust of my argument throughout this piece, that the United States and United Kingdom have gone too far in their surveillance powers, a third option centers on scaling back existing authorities. For the United States, this would mean limiting the expansion of Article II claims to cases involving suspected terrorists. It would mean taking a hard look at the growing role of the Department of Defense in domestic information-gathering and analysis. It would also mean *not* creating a third category somewhere between criminal law and national security to deal with the terrorist challenge. This proposal reflects an approach taken by the Bush Administration in the Draft Enhancing Domestic Security Act of 2003. The Judiciary, however, reluctant to intrude in the Article II powers, may find it equally difficult to assert its authority over some sort of hybrid category. The United States also could move to a system that requires individualized suspicion for the collection of information—instead of drawing on broad data mining powers to place the entire population under surveillance. In the United Kingdom, scaling back the powers would include preventing the introduction of Part III of the ATCSA—a section already deemed unnecessary in the current technological environment. Efforts could be made to return the burden of proof to the state and to require individualized suspicion for the use of surveillance powers.

Another option that could be considered is an effort by the Legislature to delimit what falls within the remit of national security. During the Second Reading of the 1989 Security Service Act, which, it will be recalled, placed MI5 on a statutory footing, the Home Secretary said, "[b]y its very nature, the phrase [national security] refers and can only refer to matters relating to the survival or well being of the nation as a whole, and not to party political or sectional interests."[747] What falls within the gamut of matters related to the well-being of a state, however, can be rather broad. The House of Lords, for instance, does not consider it to be limited to direct threats to national security.[748] Lord Slynn warned against introducing a statutory definition, saying, "[t]he question of whether something is 'in the interests' of national security is not a question of law. It is a matter of judgement and policy." Indeed, the European Commission noted in 1993

---

[747] 143 PARL. DEB., H.C. (6th Ser.) (1988) 1105 (U.K.) (statement of Douglas Hurd).

[748] Sec'y of State for the Home Dep't v. Rehman [2001] UKHL 11 (H.L.) (appeal taken from Eng.) (U.K.).

that no precise definition of what is in the interests of "national security" exists.[749]

What makes the breadth of this conception of import is the repeated expansion of state powers where "national security" is at stake. David Feldman, writing about the incorporation of the European Convention of Human Rights into British law, argued that the courts should adopt a proportionality test.[750] Some rights, regardless of the national interests claimed, remain exempt from incursion. For others, a careful balance between the interference with rights and the threat posed by not engaging in the activity matters. Feldman concedes that while courts may be comfortable adjudicating in some areas, in others the Judiciary will be less inclined to intervene; nevertheless, they ought to still be able to examine the issue through the lens of proportionality.

Another approach that may yield more satisfactory results would be to limit the ends for which information is sought by including certain crimes in the definition of "national security." Again, this article is not the correct venue to pursue this idea in depth, but it offers one way to prevent the misuse of executive power.

What is interesting in the United Kingdom is that the structure adopted to authorize the use of extraordinary powers in some sense gets at the undefined nature of national security: MI5 and GCHQ, for instance, are more likely to be seeking what most would consider national security ends than, say, the public health authorities. Here, the secretive nature of these organizations is of the utmost importance.

As Baroness Hilton, speaking in the House of Lords, noted,

> MI5 does not have a system of clear accountability . . . it is a secret organization; its budget is secret; its members and resources are secret. It is accorded special privileges by the courts: for example its internal paperwork is protected from disclosure; and its members can be given anonymity as witnesses. So its proceedings are not open. It has no public complaints system . . . .[751]

To counter this secrecy and to ensure that surveillance powers are being properly directed, Parliament created four Commissioners and a complaints tribunal. The effectiveness of these mechanisms, however, remains less than clear. The Investigatory Powers Commissioner for Northern Ireland, for instance, does not make *any* public reports. Those issued by the Interception Commissioner (who does not address the

---

[749] COUSENS, *supra* note 565, at 86 (citing Esbester v. United Kingdom, 18 EUR. H. R. REP. 72 (1993) (Court decision)).

[750] *See id.* at 87 (citing DAVID FELDMAN, PROPORTIONALITY AND THE HUMAN RIGHTS ACT (1998, 1999)).

[751] 572 PARL. DEB., H.L. (5th Ser.) (1996) 401 (U.K.) (statement of Baroness Hilton).

operation of surveillance authorities in Northern Ireland) lack important details. They have yet to report on external warrants, and they consciously do not discuss warrants issued by the Foreign Office. The Commissioners themselves do not look at the number or extent of warrantless interceptions; nor do they consider each warrant. Instead, the practice of successive Commissioners has been to select and inspect warrants randomly (with the exception of counter-subversion activities, in which case the Commissioner inspects each one.) Only a fraction of the complaints submitted to the seven-member Investigatory Powers Tribunal are investigated (3 out of 22 in 2000, 71 of 102 in 2001, and 67 out of 130 in 2002.) Their policy is to neither confirm nor deny whether surveillance had actually taken place. Without notice, however, how are individuals going to be able to take the security services to task? When British subjects do suspect that they are under surveillance, the provision of evidence to the Tribunal is voluntary, and hearsay can be accepted. Following on the tradition of the Interception of Communications Tribunal (established in 1986 and superseded by the Investigatory Powers Tribunal), the Tribunal has yet to uphold a single complaint.[752] Legislation, moreover, specifically exempts Commissioners and the Tribunal from judicial oversight.[753]

During the Parliamentary debates on the 1997 Police Bill, Lord Browne-Wilkinson expressed his alarm at the use of executive warrants:

> We have no written Constitution. We do not enjoy specific constitutional rights against the state. Our freedom depends . . . only, on the fact that no Minister, no administrator and no member of the police has any greater power or any greater right than any other citizen to enter our property or to seize our person. In particular, the state and its officers have no power to enter our houses or workplaces or to seize our property.[754]

The use of prior authorization and independent Commissioners served as a sort of compromise; but these bodies still report within the executive branch, exempt from judicial scrutiny and oversight. The standard used, moreover, is weak: reasonable suspicion, not probable cause.

As was previously noted, British law as currently written does not allow intercepted communications to be used in judicial proceedings. Where the other policy recommendations look at ways to minimize

---

[752] The Intelligence Services Commissioner looks at activities of the Intelligence Services, officials of the Ministry of Defence and HM Forces outside of Northern Ireland. COUSENS, *supra* note 565, at 198-99.

[753] *See, e.g.*, Interception of Communications Act 1985, § 7(8), Schedule ¶ 3(2) (Scot.); Police Act 1997, ch. 50, § 91(10) (U.K.), *available at* http://www.opsi.gov.uk/acts/acts1997/97050—j.htm#91.

[754] 575 PARL. DEB. H.L. (5th Ser.) (1996) 810 (U.K.).

surveillance, greater use of intercepts in the judicial system may result in stronger procedural controls being introduced to ensure a minimum amount of intrusion into the sphere of privacy. Review committees have consistently called for legalization of intercepted communications to make it possible to prosecute more terrorist crimes.[755]

What minimal forays have been made in the United States in this direction leave something to be desired: The President's Board on Safeguarding Americans' Civil Liberties provides a good example of what *not* to do. The Deputy Attorney General chairs the organization and sets the agenda. All twenty members come from the same agencies using the surveillance powers. Almost all are either presidential appointees or senior staff members who serve appointees. The board can only advise. They act under no obligation to provide either information or findings to the public. The body, moreover, does not act in an ombudsperson role.[756] In the renewal of the USA PATRIOT Act, Congress introduced some mechanisms to provide enhanced oversight of the surveillance authorities. But the reporting requirements are limited, and only address some of the powers granted to the Executive since 9/11. Here, only depending on the hearings being called is insufficient: such inquiries offer snapshots, not ongoing regulation of the use of such powers. They also leave gaps in the scrutiny afforded. While the House and Senate both held hearings on the NSA surveillance program, for instance, neither has inquired systematically into either NSLs or the DOD's changing domestic role. Control of the executive and legislative branches by the same political party, moreover, may make it difficult for such hearings to even be called. Furthermore, relying on the suspension of funds does not appear to have the intended effect; the amount of discretionary funding available means that programs can continue. TIA and TIPS provide two ready examples. Actions such as creating independent review bodies, introducing an audit process, establishing an effective ombudsperson, and providing for regular congressional review, deserve further discussion.

The final option to highlight is the possibility of eliminating sunset provisions altogether. The argument here is that temporary powers rarely turn out to be so; instead, they simply become a baseline, on which further powers are built. Part of the difficulty is that as soon as the provisions become law, the rationale shifts: those wanting to repeal the measures must demonstrate that in withdrawing them more violence will not occur—or that some level of violence is acceptable. The former is impossible to

---

[755] PRIVY COUNSELLOR REVIEW COMMITTEE, *supra* note 637, at 8-9.

[756] *See* Exec. Order No. 13,353, 69 Fed. Reg. 53,585 (Sept. 1, 2004), *available at* http://www.whitehouse.gov/news/releases/2004/08/20040827-3.html.

show, and the second is politically unpalatable. And so temporary measures quickly become a permanent part of the state response, with more measures introduced following the next attack. They thus function simply to make inroads into individual rights somehow more palatable. But this fiction does long-term damage to the state. Eliminating sunset provisions may force legislatures to consider the long-term impact of broader surveillance powers beyond the immediate threat posed by terrorism.

CONCLUDING REMARKS

In 1948, George Orwell's novel *1984* captured the corrosive impact of broad state surveillance. The main character, Winston Smith, a citizen of a state called Oceania (coincidentally, a fictional representation of the United States and United Kingdom), lived under the all-seeing eye of Big Brother. Nearly two decades later, Vance Packard echoed his concerns in *The Naked Society*. Alan Westin's *Privacy and Freedom* subsequently generated increased attention to the issue. In 1984, Congress, finally alarmed by the growth of technology, held hearings on the subject. Glenn English opened the proceedings:

> I don't think that anyone . . . can seriously argue that in 1984 we've realized George Orwell's vision of a totalitarian world of constant fear, repression, and surveillance. What is important is that the technology that would enable Mr. Orwell's vision to become a reality already exists. The issue that we must face is how to control the technology before it controls us.[757]

At that time, only forty-five percent of the public knew how to use computers, but sixty-nine percent expressed concern that an Orwellian society was at hand.[758] This paper has essentially argued that, sped by claims of national security and the need to fight terrorism, *1984* approaches.

In the United States, where no general right to privacy exists, two sets of authorities have emerged. The first, largely the realm of criminal law, evolved from trespass doctrine and the exclusionary rule to a reasonable expectation of privacy; where such exists, outside of a handful of exceptions, law enforcement must obtain prior judicial authorization for physical searches to meet the requirements of the Fourth Amendment. Title III sets an even higher standard for wiretapping and electronic bugs.

The second set of authorities, the same ones claimed by the current administration to defend the NSA's domestic surveillance program, centered on national security, not criminal law. Here, largely unfettered by judicial requirements, the Executive claims Article II authority. The 20th

---

[757] *Privacy and 1984*, *supra* note 213, at 2.

[758] *Id.* at 4, 7.

century witnessed the state's first use—and misuse—of these powers in peace time. FISA scaled back the Executive, while still granting it domain over national security concerns. The Executive, however, almost immediately began chipping away at the restrictions. CALEA, the USA PATRIOT Act, the weakening of the attorney general guidelines, and post-9/11 surveillance operations represent the latest—and most radical—expansion of this realm. The growth of military involvement here is of note, as are the many data mining operations underway. TIA, ADVISE, MATRIX, and other efforts represent a fundamental shift in the type of surveillance in which the state can engage.

Like the United States, the United Kingdom does not recognize a general right to privacy. Instead, the state historically addressed conditions that implicated particular privacy interests. In 1998, the Human Rights Act introduced a broader right to privacy. This legislation, however, only required that other statutes be read as far as possible in a manner consistent with the ECHR. The Convention, moreover, includes a specific exception for matters related to national security. This does not mean that the Convention had no affect on British law relating to counterterrorism and surveillance. On the contrary, the European Court repeatedly found the lack of legislation authorizing specific surveillance mechanisms, and the absence of effective oversight, to be a breach of the ECHR. Each time the United Kingdom acted to address these concerns, however, the government seems to have expanded the underlying state. The system for warrants remains entirely within the executive domain; and the standard employed—reasonable suspicion—relatively weak.

Outside of counterterrorism, the development of technology has propelled the amount of data that can be obtained, analyzed, and shared forward at a dizzying rate. The information revolution, the growth of digital record-keeping, and the development of public identification, search, and tracking systems have played a central role. In both societies, anonymity is being lost, and what started as physical or data surveillance has moved into the realm of psychological surveillance. Perhaps nowhere is this clearer than in data mining operations such as TIA and MATRIX. Substantive risks attend, as do political, legal, social, and economic fabric concerns.

While it is not the intention of this article to provide a complete analysis of the policy options available, six possibilities deserve greater attention: creating a property right in personal information, regulating the access, transfer and retention of data while providing remedies for violations, scaling back the existing powers, more narrowly defining "national security," creating effective safeguards, and eliminating clauses

that allow for such powers to be "temporary." Whichever of these, or other policy options, are adopted by the states, the time is ripe to consider the effect of counterterrorism and advances in technology on surveillance in the United States and United Kingdom. Both countries now face something different in kind—not degree—than what has come before.