September 2002

Post-Sept. 11th International Surveillance Activity - A Failure of Intelligence: The Echelon Interception System & the Fundamental Right to Privacy in Europe

Kevin J. Lawner

Follow this and additional works at: http://digitalcommons.pace.edu/pilr

Recommended Citation
Available at: http://digitalcommons.pace.edu/pilr/vol14/iss2/7

This Article is brought to you for free and open access by the School of Law at DigitalCommons@Pace. It has been accepted for inclusion in Pace International Law Review by an authorized administrator of DigitalCommons@Pace. For more information, please contact cpitton@law.pace.edu.
POST-SEPT. 11TH INTERNATIONAL SURVEILLANCE ACTIVITY — A FAILURE OF INTELLIGENCE: THE ECHELON INTERCEPTION SYSTEM & THE FUNDAMENTAL RIGHT TO PRIVACY IN EUROPE

Kevin J. Lawner*

I. Introduction ....................................... 436
II. Communications Intelligence & the United Kingdom - United States Security Agreement ..... 443
   A. September 11th - A Failure of Intelligence .... 446
   B. The Three Warning Flags ..................... 449
III. The Echelon Interception System .................. 452
   A. The Menwith Hill and Bad Aibling Interception Stations .......................... 452
   B. Echelon: The Abuse of Power .................. 454
IV. Anti-Terror Measures in the Wake of September 11th ............................................... 456
V. Surveillance Activity and the Fundamental Right to Privacy in Europe .............................. 460
   A. The United Nations International Covenant on Civil and Political Rights and the Charter of Fundamental Rights of the European Union... 464
   B. The European Convention for the Protection of Human Rights & Fundamental Freedoms ..... 466
      1. Article 8 of the ECHR ....................... 468
      2. The Case Law: Article 8 of the ECHR ..... 470
      3. The Requirements Imposed by Article 8 of the ECHR ....................................... 474

* J.D. candidate at Pace University School of Law. He holds a B.A. in Philosophy & Religion from Washington College and a M.A. from New York University in Environmental Conservation Education. He extends his sincere thanks to Samantha Riley and Jennifer Hogan for their substantial editorial contributions to this work.
It's going to take all of us to gather the necessary intelligence, the necessary information, to be able to find the location of the terrorists; to work with governments to smoke them out of their safe houses, to get them moving, and then have the courage to bring them to justice.¹

President George W. Bush, September 18, 2001

I. INTRODUCTION

The devastating events of September 11, 2001, have brought home the reality that a shadowy, global network of extremists threatens the peace and security of our nation.² This threat, however, is not new, as U.S. interests have long been the targets of international terrorism.³ The attacks have exposed our vulnerabilities,⁴ and at the same time have generated enormous patriotism, which has immeasurably strengthened our re-

³ In February 1993, a massive bomb destroyed the parking garage at the World Trade Center in New York City. In June 1996, a powerful bomb destroyed Khobar Towers, a U.S. military housing complex in Saudi Arabia. In August 1998 there were simultaneous vehicular bombings of the U.S. embassies in Nairobi, Kenya, and Dar Es Salaam, Tanzania. In October 2000, a boat laden with explosives was detonated alongside the U.S.S. Cole while refueling in the Yemeni port of Aden. See generally KENNETH KATZMAN, CRS REPORT FOR CONGRESS, TERRORISM: NEAR EASTERN GROUPS AND STATE SPONSORS (Sept. 10, 2001).
⁴ See Wilson Statement, supra note 2, at 2-3. See also Converging Dangers in a Post 9/11 World: Hearing Before the Senate Select Comm. on Intelligence, 107th Cong. (2002) (statement of George J. Tenet, Director, Central Intelligence) [hereinafter Tenet Statement]; Mathew Wald, A Nation Challenged: Electric Power System is Called Vulnerable and Vigilance is Sought, N.Y. TIMES, Feb. 28, 2002, at A13 (stating computers and security systems that control electric power around the nation have been probed by terrorists); William Broad, A Nation Challenged: Analyzing Dangers; Scientists Find the New Field of Threat Assessment Full of Uncertainties, N.Y. TIMES, Nov. 29, 2001, at B8 (stating scientists using a new threat assessment technique face uncertainties predicting likelihood of future terrorists attacks).
solve.\textsuperscript{5} While the military strikes of \textit{Operation Enduring Freedom},\textsuperscript{6} and the arrests or detention of terror suspects throughout the world have significantly disrupted Usama bin Laden's Al Qaeda network,\textsuperscript{7} the most recent intelligence reports suggest that bin Laden is still alive,\textsuperscript{8} and hiding in the moun-

\textsuperscript{5} See Wilson Statement, supra note 2, at 3. See also RAPHAEL F. PERL, CRS ISSUE BRIEF FOR CONGRESS, TERRORISM, THE FUTURE, AND U.S. FOREIGN POLICY (Sept. 2001) (hereinafter Perl).


tains somewhere between Afghanistan and Pakistan.\(^9\) Regardless if Usama is killed or survives, the awakening has started,\(^10\) and undoubtedly, his network still remains a threat.\(^11\)

Al Qaeda’s objective is clear, and has been espoused by Usama bin Laden — who has “urged and incited his followers to kill American citizens, in the most unequivocal terms.”\(^12\) As early as 1996, bin Laden declared it “the duty now on every tribe in the Arabian peninsula to . . . cleanse the land from these Crusader occupiers,”\(^13\) and in 1998, he asserted that “the killing of Americans and their civilian and military allies is a religious duty for each and every Muslim to be carried out in whichever country they are . . . .”\(^14\) Later that same year, bin Laden proclaimed it a “religious duty” to acquire weapons of mass destruction to use against the United States.\(^15\) Since that time, ninety-percent-enriched weapons-grade uranium in an amount sufficient to produce an atomic bomb has been reported

\(9\) See supra note 7, and accompanying text.


\(13\) Id. para. 22.

\(14\) Id. (emphasis added).

\(15\) See Tenet Statement, supra note 4.
stolen from an enterprise in the former Soviet Union. After the attacks of September 11, 2001, bin Laden boasted to a Pakistani newspaper that "Al-Qaeda [now] possess[ed] chemical and nuclear weapons," and was prepared to use them if necessary.

Today, "experts agree that the most effective way to fight [international] terrorism is to gather as much intelligence as possible," in order to prevent future attacks before they can be executed. In simple terms, intelligence gathering "gives us an information advantage over our adversaries," and in the wake of September 11, 2001, "[t]he collection and analysis of . . . intelligence and information has become a priority of the highest measure." Since intelligence gathering will be "the front line in the war against [international] terrorism," the new emphasis of the United States Intelligence Community will undoubtedly be on the interception and analysis of foreign communications.

18 See id.
19 Perl, supra note 5, at 4.
20 See id.
21 Mike Hayden, Director of the National Security Agency (N.S.A.), Opening Remarks: Partnerships for Combating Terrorism Forum (Mar. 4, 2002).
24 "The term 'Intelligence Community' refers to the group of fourteen government agencies and organizations that, either in whole or in part, conduct the intelligence of the United States Government: Central Intelligence Agency (CIA); Department of the Treasury; Department of Energy; Department of State; Defense Intelligence Agency (DIA); Federal Bureau of Investigation (F.B.I.); National Imagery and Mapping Agency (NIMA); National Reconnaissance Office (NRO); National Security Agency (N.S.A.); U.S. Air Force Intelligence; U.S. Army Intelligence; U.S. Coast Guard Intelligence; U.S. Navy Intelligence; and U.S. Marine Corps Intelligence." Joint Investigation into September 11th: First Public Hearing Before Joint House/Senate Intelligence, Comm. Hearing, 107th Cong. (2002) (statement by Eleanor Hill, Staff Directory, Joint Inquiry Staff) [hereinafter Hill Statement].
25 See Davis, supra note 23.
Al Qaeda operatives are trained well to protect their sensitive communications,\(^{26}\) and "even against a superior arsenal of technology, there are still plenty of ways for terrorists to avoid detection."\(^{27}\) Intelligence analysts now believe that Usama bin Laden has "morphed his terrorist tactics to keep pace with U.S. intelligence-gathering methods,"\(^{28}\) and that future attacks will likely be planned using both high and low-tech means.\(^{29}\) Still, others believe that in order to elude law enforcement, "bin Laden has ditched his satellite-linked phones, mobile handsets and Internet access in favor of 'Stone Age' messaging techniques . . . ."\(^{30}\) Despite their preferred means of communication, "Al Qaeda cells . . . will continue to pose a threat to U.S. and other western interests."\(^{31}\)

In order to get a first-hand look at how the U.S. Intelligence Community is being primed to prevent future terrorist attacks,\(^{32}\) President George W. Bush recently visited the headquarters of the National Security Agency (N.S.A.).\(^{33}\) Since


\(^{27}\) Susan Stellin, Terror's Confounding Online Trail, N.Y. TIMES, Mar. 28, 2002, at G1.


\(^{29}\) See id.

\(^{30}\) Id.


1952,\textsuperscript{34} the N.S.A. has conducted “electronic surveillance to collect foreign intelligence . . .”,\textsuperscript{35} and today, is rumored “to have more computing power than any other institution on earth . . . .”\textsuperscript{36} The “N.S.A.’s mission is to exploit secret foreign communications and produce foreign intelligence information while protecting U.S. communications.”\textsuperscript{37} “The N.S.A. provides valuable intelligence [information] . . . on a wide range of issues of concern to all Americans, such as international terrorism, narcotics trafficking, and [the] proliferation of weapons of mass destruction.”\textsuperscript{38}

From 1996 to 1998, “when bin Laden was beginning his operations out of Afghanistan, [the] N.S.A. knew his phone number and was able to listen in on calls he and his top lieutenants made to Al Qaeda cells around the world.”\textsuperscript{39} Despite U.S. surveillance activity, N.S.A. intercepts could not prevent bin Laden from orchestrating the 1998 bombings of the U.S. embassies in East Africa.\textsuperscript{40} Similarly, the conversations intercepted on the day before September 11, 2001,\textsuperscript{41} could not prevent nineteen Al Qaeda operatives from hijacking four commercial airliners and subsequently crashing the planes into the World Trade Center, the Pentagon, and an empty field in Stony Creek Township, Pennsylvania. As a result, this massive failure of intelligence

\textsuperscript{34} See generally Nat’l Security Council, Intelligence Directive No. 9: Communications Intelligence (Dec. 29, 1952) (stating that the N.S.A. controlled intelligence activities against foreign governments since 1952).


\textsuperscript{38} Hayden Statement, supra note 35.

\textsuperscript{39} 60 Minutes: National Security Meltdown (CBS television broadcast, June 19, 2002) (transcript on file with Pace Int’l L. Rev.).

\textsuperscript{40} See id.

"became the focus of an eight-hour closed door hearing on Capital-Hill."\textsuperscript{42}

The N.S.A.’s vast computing powers and interception capabilities cannot be expected to prevent each and every terrorist attack; however, the use of interception technologies will undoubtedly play a critical role in fighting the war against international terrorism.\textsuperscript{43} Although intelligence gathering services, such as the N.S.A., provide citizens valuable services in "protecting national security and the free order of a democratic state,"\textsuperscript{44} after the devastation of September 11, 2001, Europeans have become increasingly concerned that governments are putting the interests of national security above the respect for individual fundamental rights.\textsuperscript{45} This concern is justified given that national security services often have inadequate control measures, and "there is a high risk of abuse of power and violations of human rights, unless legislative and constitutional safeguards are provided."\textsuperscript{46} Following the attacks, European privacy and civil liberties organizations from Austria, Denmark, Germany, the Netherlands, and the United Kingdom


\textsuperscript{44} \textit{Recommendation 1402; Control of Internal Security Services in Council of Europe}, EUR. PARL. ASS. DEB. 9th Sess. Doc. No. 8301, para. 3 (Apr. 26, 1999) [hereinafter \textit{Recommendation}].


\textsuperscript{46} \textit{Recommendation, supra} note 44, para. 2.
have urged the Council of Europe to defend the fundamental rights and freedoms of Europeans.\textsuperscript{47}

In the wake of September 11, 2001, this note explores the inherent tensions existing between the right of a democratic society to national security and the individual right to privacy in Europe. By focusing on fundamental rights guaranteed to European citizens via international instruments, this note examines how the right to privacy in Europe will be affected by post-September 11th, foreign intelligence gathering activity. Whether under the auspices of the United Kingdom-United States Security Agreement ("UKUSA") Agreement,\textsuperscript{48} advanced international surveillance systems, such as Echelon, can be utilized effectively in a way that is compatible with European law and the fundamental right to privacy.

II. COMMUNICATIONS INTELLIGENCE & THE UNITED KINGDOM-UNITED STATES SECURITY AGREEMENT

Communications intelligence ("COMINT")\textsuperscript{49} is practiced by virtually all developed countries throughout the world in order

\textsuperscript{47} See Evers, supra note 45.

\textsuperscript{48} UKUSA refers to a secret 1948 agreement on Signals Intelligence between the National Security Agency (N.S.A.), the Government Communications Head Quarters (GCHQ) of England, the Communications Security Establishment (CSE) of Canada, the Australian Defense Security Directorate (DSD), and the General Communications Security Bureau (GCSB) of New Zealand. See infra, notes 50-70 and accompanying text for a detailed discussion of UKUSA.

\textsuperscript{49} "Communications Intelligence" is intelligence produced by the study of foreign communications. Intelligence based in whole or in part on Communications Intelligence sources shall be considered Communications Intelligence as pertains to the authority and responsibility of the United States Communications Intelligence Board." Nat'l Security Council, Dep't of State, National Security Council Intelligence Directive No. 9 (Mar. 10, 1950), available at http://www.fas.org/irp/offdocs/nscid09.htm. "Communication intelligence' or 'COMINT' shall be construed to mean all procedures and methods used in the interception of communications other than foreign press and propaganda broadcasts and the obtaining of information from such communications by other than the intended recipients, . . . " Unpublished Memorandum from President Harry S. Truman to the Secretary of State and the Secretary of Defense, Communications Intelligence Activities (Oct. 24, 1952), at http://www.gwu.edu/~nsarchiv/nsa/publications/icoicedoc1.html. "COMINT is technical and intelligence information derived from foreign communications by other than the intended recipients. COMINT is produced by the collection and processing of foreign communications passed by electromagnetic means, . . . and by the processing of foreign encrypted communications, however transmitted." Dep't of Defense, The National Security Agency and The Central Security Service, Department of Defense Directive s-
“to obtain sensitive data concerning individuals, government, trade and international organisations.”

Traditionally associated with the interception of military and diplomatic communications, over the past half-century, COMINT has become “a large-scale industrial activity” providing consumers with intelligence on economic and scientific developments as well.

Following World War II, a secret international agreement known as the United Kingdom–United States Security Agreement (“UKUSA” or the “Agreement”), was made. Formalized in 1948, this clandestine accord effectively fashioned the first cooperative alliance between international intelligence gathering agencies. For more than a half-century, signatories to the UKUSA Agreement have worked together to intercept, analyze, and disseminate COMINT from the world’s communications channels. Since “[t]he UKUSA Agreement is a tiered treaty in which the U.S. is designated as the First Party . . . the United States (and specifically the N.S.A.) is recognized as the dominant party.” While its signatories still refuse to officially acknowledge its existence, the Agreement is explicitly referred to

---


51 See STOA, supra note 50.

52 See id.


54 See STOA, supra note 50.


56 Richelson & Ball, supra note 53, at 7.
in a U.K. Parliamentary monitoring body report\textsuperscript{57} and has been recognized by both the Prime Minister of New Zealand\textsuperscript{58} and the former director of the Australian intelligence service [DSD].\textsuperscript{59}

Prior to 1990, "it is widely accepted that the primary function of the U.S. intelligence system, usually working in close cooperation with western European allies, was to gather intelligence of all types on the former Soviet Union, its allies, and on the Peoples Republic of China."\textsuperscript{60} The fall of communism in the Soviet Union, however, "brought about dramatic changes inside all western intelligence agencies,"\textsuperscript{61} and with its principle target suddenly gone, "intelligence agencies faced a period of downsizing . . . .\textsuperscript{62} Over the next decade, "the N.S.A. lost about 15% of its budget, 20% of its staff, and closed more than 20 overseas field stations."\textsuperscript{63}

After the Cold War, the U.S. Intelligence Community shifted its focus to the collection of economic intelligence, scientific and technological development, narcotics trafficking, money laundering, organized crime, and international terrorism.\textsuperscript{64} It quickly became apparent that international coopera-


\textsuperscript{61} Id. para. 4.

\textsuperscript{62} Id.

\textsuperscript{63} Id.

\textsuperscript{64} See id.
tion among intelligence services was the most effective means of battling these more contemporary global problems. Following September 11, 2001, the sharing of COMINT data between the UKUSA signatories will undoubtedly focus primarily on fighting the war against international terrorism.

Just days before the 2001 attacks on the World Trade Center and the Pentagon, the Senate Select Committee on Intelligence (SSCI) reaffirmed its commitment to revitalizing the N.S.A. by approving the Authorization Bill for Fiscal Year 2002. This allocation of funds represented “the first installment of a multi-year effort to correct serious deficiencies that have developed over the past decade in the Intelligence Community.” Despite its multi-billion dollar-a-year budget, the U.S. Intelligence Community, and the N.S.A. in particular, still “lack the personnel to instantly translate and analyze the high volume of information it collects each day from around the world . . . .” Since the September 11th attacks the U.S. Congress approved the President Bush’s request for $20 billion in additional funds to combat international terrorism, and the “intelligence agencies have experienced a surge in job seekers . . . . Résumés are pouring in . . . at a rate four to six times as high as before the attacks.”

A. September 11th — A Failure of Intelligence

During the months and even years before the attacks of September 11, 2001, the U.S. Intelligence Community and the Bush administration had clear warnings that terrorist organizations, including Al Qaeda were planning to attack targets in

---

65 See id.
67 Id.
69 See US. GENERAL ACCOUNTING OFFICE, COMBATING TERRORISM: SELECTED CHALLENGES AND RELATED RECOMMENDATIONS (Sept. 2001).
the U.S. using aircraft. National Security Advisor, Condoleezza Rice, maintained that the intelligence reports given to the President in the months prior to the attacks suggested only that “traditional hijackings” were being anticipated, and that the impending attacks were thought likely to be directed at targets outside the U.S. “Both in terms of attempts and actual attacks, [however,] there was considerable historical evidence prior to September 11, that international terrorists had planned and were, in fact, capable of conducting major terrorist strikes within the United States.”

The Intelligence Community also possessed ample evidence prior to September 11, 2001, which indicated that terrorists were contemplating the use of airplanes as weapons. Specifically, the Community obtained information in August 1998 “that a group of unidentified Arabs planned to fly an explosive-laden plane from a foreign country into the World Trade Center.” In response to this recent disclosure, “intelligence officials reacted angrily, declaring that the panel had exaggerated some material and taken information out of context so the 1998 threat appeared to mirror the Sept. 11 attacks.”


73 See Gertz, supra note 42.

74 Hill Statement, supra note 24, at 9. “The 1993 attack on the World Trade Center, the subsequent discovery in 1993 of plots to bomb New York City landmarks, and the arrests in 1999 during the Millennium celebrations of an individual with al Qa’ida connections intending to bomb Los Angeles International Airport should have erased any doubts, to the extent they existed, about that point.” Id.


Apparently, it was not until the 1998 embassy bombings in East Africa that the Intelligence Community finally recognized how dangerous a threat Al Qaeda was to U.S. interests.\textsuperscript{78}

In December 1998, the DCI [Director of Central Intelligence] George Tenet provided written guidance to his deputies at the CIA, declaring, in effect, “war” with Bin Laden. DCI Tenet wrote: We must now enter a new phase in our effort against Bin Laden . . . . We are at war . . . . I want no resources or people spared in this effort, either inside [the] CIA or the [Intelligence] Community.\textsuperscript{79}

Despite that declaration of war, however, “there was no massive shift in budget or reassignment of personnel to counterterrorism until after September 11, 2001.”\textsuperscript{80} In fact, the “1998 declaration did not adequately reflect a true ‘war’ effort against bin Laden.”\textsuperscript{81} In 1999, after the so-called “declaration of war,” the DCI’s Counterterrorist Center (“CTC”) only had “three analysts assigned full-time to Bin Laden’s terrorist network worldwide . . . [and] [o]n September 11, 2001, the international analytic unit at F.B.I. headquarters had in place only one analyst to address al Qa’ida.”\textsuperscript{82}

Concerns about Usama bin Laden and the Al Qaeda network grew over the next few years, “and reached peak levels in the spring and summer of 2001, as the Intelligence Community faced increasing numbers of reports of imminent al-Qa’ida attacks against U.S. interests.”\textsuperscript{83} The “chatter” of impending attacks was so great between May and July 2001,\textsuperscript{84} “that the National Security Agency reported at least 33 communications indicating a possible, imminent terrorist attack.”\textsuperscript{85} As a result of these reports, on August 6, 2001, President Bush received a daily briefing entitled “Bin Laden Determined to Strike in the

\textsuperscript{78} See Hill Statement, supra note 24, at 9.
\textsuperscript{79} Id.
\textsuperscript{80} Id. at 10.
\textsuperscript{81} Id. at 18.
\textsuperscript{82} Id.
\textsuperscript{83} Id. at 10.
\textsuperscript{85} Hill Statement, supra note 24, at 20.
U.S.,” which forewarned of an imminent Al Qaeda attack, that planes were likely going to be hijacked, and that buildings in New York City were of particular concern.\textsuperscript{86} Despite these intelligence reports, “authorities did little to ‘harden the homeland’ against an assault.”\textsuperscript{87}

B. The Three Warning Flags

In July and August 2001, just about the time when the rise in intelligence ‘chatter’ began to decrease, “three additional developments occurred in the United States”\textsuperscript{88} that should have raised warning flags: “the Phoenix memo; the detention of Zacarias Moussaoui; and the Intelligence Community’s realization that two individuals with ties to Usama Bin Ladin’s network . . . were possibly in the United States.”\textsuperscript{89} Apparently, however, “[t]he Intelligence Community [. . .] had not connected these individual warning flags to each other, to the ‘drumbeat’ of threat reporting that had just occurred, or to the urgency of the ‘war’ effort . . .”\textsuperscript{90} which had been declared three years earlier.

The first warning flag was raised in July 2001, when the so-called “Phoenix Memo” was sent from the F.B.I.’s field office in Phoenix, Arizona, to a unit within F.B.I. headquarters in Washington, D.C., alerting them “that several Arabs were seeking flight training and other courses involving airport security and airport operations at at least one U.S. flight school.”\textsuperscript{91} The five-page memo written by Agent Kenneth Williams, requested that F.B.I. headquarters “order a check of all flight schools to look for other Arabs who might also be involved,”\textsuperscript{92} and explicitly referred to Usama bin Laden and his Al Qaeda network.\textsuperscript{93} Agent Williams’ recommendation, however, was turned down by F.B.I. headquarters in Washington,\textsuperscript{94} and to compound this failure,

\textsuperscript{86} See Gertz, supra note 42. See also Horrock, supra note 84.
\textsuperscript{88} Hill Statement, supra note 24, at 10.
\textsuperscript{89} Id.
\textsuperscript{90} Id.
\textsuperscript{91} Gertz, supra note 42.
\textsuperscript{92} Id.
\textsuperscript{93} See id. See also Borger, supra note 84.
\textsuperscript{94} See Borger, supra note 84.
they "basically kept this [information] in," and did not share it with the rest of the Community.  

The second warning flag was raised on August 16, 2001, when the F.B.I. arrested Zacarias Moussaoui on immigration charges after flight instructors at the Pan Am International Flying Academy in Eagan, Minnesota, grew suspicious when he "paid $8,000 to learn how to fly a commercial jetliner but had expressed disinterest in learning to take off and land." After his arrest, F.B.I. agents in the Minnesota "field office wanted headquarters to press for a warrant to allow them to search the computer owned by Mr. Moussaoui," but were stifled by F.B.I. headquarters in Washington. When the F.B.I. finally searched Mr. Moussaoui's computer after September 11th, they discovered "cockpit layouts of large commercial aircraft, and phone numbers like one in Germany for the roommate of Mohamed Atta, the ringleader of the plot."  

A "veteran agent and general counsel in the Minneapolis [field] office," Colleen Rowley, later criticized F.B.I. headquarters for blocking "attempts by Minneapolis agents to obtain a warrant to examine Mr. Moussaoui's laptop computer." In response to Ms. Rowley's criticisms, F.B.I. Director Robert S. Mueller III agreed that "the Minneapolis and Phoenix situations should have been handled differently," and that Agent Williams' Phoenix Memo "should have been shared with the CIA." Mr. Mueller also acknowledged that even though the "Moussaoui information and the Phoenix memo went to the same unit at [Washington] headquarters . . . no connection was made

95 See Gertz, supra note 42.
97 Lewis, supra note 96.
99 Id.
100 Lewis, supra note 96.
101 Johnston & Lewis, supra note 98.
102 See generally Oversight Hearings on Counter-Terrorism: Hearing Before the Senate Committee on the Judiciary, 107th Cong. (June 6, 2002) (statement of Colleen M. Rowley, F.B.I. Special Agent and Minneapolis Chief Division Counsel).
103 Lewis, supra note 96.
104 Id.
INTERNATIONAL SURVEILLANCE ACTIVITY

[between the two,]" and he also confessed that "Sept. 11 might have been preventable if officials in his agency had responded differently to all the pieces of information that were available." The third warning flag was raised on August 23, 2001, when the Intelligence Community requested that two Al Qaeda suspects (wanted in connection with the August 2000 attack on the U.S.S. Cole, and later determined to be participants in the September 11th attacks) "be added to the U.S. Department of State’s ‘watch list’ for denying visas" for entry into the United States. While the F.B.I.’s New York field office searched unsuccessfully for the two Al Qaeda suspects, the Los Angeles field office did not even receive the search request until the day of the attacks. Prior to September 11, 2001, however, both suspects were living openly in San Diego, California, and were active members of the San Diego Islamic Center. One of the suspects was actually listed in the public telephone directory, and the other had frequently used his credit card in his own name.

A major part of the problem, said Mueller, was the fact that the F.B.I.’s computer technology did not permit agents to search existing sources using multiple word phrases, and that "only single word searches like ‘flight’ or ‘school’ could be entered at a time." New York Senator Charles E. Schumer called "the [F.B.I.’s] antiquated system ‘almost laughable,’ and that ‘it [made his] jaw drop to think that on 9/11 or on 9/10 the kind of technology that is available to most school kids, and certainly every small business in this country, wasn’t available to the F.B.I.’" Mr. Mueller admitted that the F.B.I. was "way be-

105 Id.
106 Id.
108 See id.
110 See id.
111 See id.
112 Johnston & Lewis, supra note 98.
113 Id.
hind the curve” and predicted that an upgrade to the system would take at least two to three years to complete.114

The U.S. Intelligence Community spends billions each year “on new collection hardware, [and] spy satellites with real-time imagery of the globe. From space, ground, and sea-based antennae, the [N.S.A.] sucks voice and data streams like a fire hose and pumps them to computer buffers for analysis. Most of the data gathers electronic dust there.”115 In the war against international terrorism, the Achilles’ heel of the N.S.A. is not its lack of technology, but rather its lack of expert linguists capable of translating the sensitive bits of intelligence that are being intercepted around the world.116

III. THE ECHELON INTERCEPTION SYSTEM

A. The Menwith Hill and Bad Aibling Interception Stations

With the support of the UKUSA signatories,117 the N.S.A. implements a globally automated intercept and relay system known as Echelon.118 Tantamount to a global eavesdropping system, Echelon is used by the N.S.A. to intercept ordinary e-mail, fax, telex, and telephone communications from around the world.119 Although the U.S. has gone to great lengths trying to keep Echelon top-secret,120 in July 2001, the European Parliament released an Official Report, confirming its existence as a

---

115 Tyler, supra note 109.
116 See id.
117 In addition to the five original “first parties” to the Agreement (The U.S., U.K., Canada, Australia, and New Zealand), it has been reported that Norway, Denmark, Germany, Italy, Greece, Turkey, Austria, Japan, South Korea, and Thailand have made “third party” agreements with the United States. See Campbell, supra note 55, at 12 (citing Jeffrey Richelson, The U.S. Intelligence Establishment (4th ed. 1999)).
119 See HAGER, supra note 53, at ch. 2.
120 See AMERICAN CIVIL LIBERTIES UNION, ECHELONWATCH: ANSWERS TO FREQUENTLY ASKED QUESTIONS (FAQ) ABOUT ECHELON, at http://www.aclu.org/echelonwatch/faq.html (last visited Oct. 12, 2002).
global system for the interception of private and commercial communications.\textsuperscript{121}

The \textit{Echelon} interception system links supercomputers throughout the world to “automatically search through the millions of intercepted messages for ones containing pre-programmed keywords or fax, telex and e-mail addresses.”\textsuperscript{122} \textit{Echelon} is comprised of approximately twenty interception stations throughout the world,\textsuperscript{123} each “linked directly to the headquarters of the secretive [N.S.A.] headquarters at Fort Mead, Maryland,”\textsuperscript{124} where intercepted data can be analyzed, retained and disseminated. The largest of the N.S.A.’s \textit{Echelon} interception stations is located in Menwith Hill, England,\textsuperscript{125} and in 1992, it is rumored that as many as 1,500 U.S. employees were stationed there.\textsuperscript{126}

At the Menwith Hill interception station, the N.S.A. operates what have been described as “‘giant golf balls,’ called radomes,”\textsuperscript{127} which communicate with satellites in geostationary orbit, to intercept e-mail, fax, and telephone communications from around the world.\textsuperscript{128} British Telecom recently “revealed that at least three major domestic fiber-optic telephone trunk lines — each capable of carrying 100,000 calls simultaneously — were [also] wired through Menwith Hill . . . allow[ing] the N.S.A. to tap into the very heart of the British Telecom network.”\textsuperscript{129} Clearly, “[i]t is a [processing] station which affects people throughout the world.”\textsuperscript{130}

The N.S.A. operates its third largest \textit{Echelon} interception station in Bad Aibling, Germany, on “land that has been declared U.S. territory for the sole purpose of housing a satellite


\textsuperscript{122} HAGER, \textit{supra} note 53, at 29.

\textsuperscript{123} See \textit{US to Close Echelon Spy Station}, at http://news.bbc.co.uk/2/hi/world/europe/1365156.stm (last visited Aug. 9, 2002).

\textsuperscript{124} Asser, \textit{supra} note 118.

\textsuperscript{125} See HAGER, \textit{supra} note 53, at ch. 2.

\textsuperscript{126} See \textit{id}.

\textsuperscript{127} Asser, \textit{supra} note 118.

\textsuperscript{128} See \textit{id}.

\textsuperscript{129} Poole, \textit{supra} note 53, at 8 (“Inside Menwith Hill”) (relying on Duncan Campbell, \textit{BT Condemned for Eliciting Cables to US Sigint Station} (Sept. 4, 1997) at http://duncan.gn.apc.org/menwith.htm (last visited Oct. 12, 2002)).

\textsuperscript{130} HAGER, \textit{supra} note 53, at 40.
As a result of September 11, 2001, the U.S. put off its plans to close the Bad Aibling station because of its importance in fighting the war against international terrorism. The decision to keep the Bad Aibling station open was made by U.S. officials, despite clear warnings that the "tentacles of the Echelon network stretch so far that... involvement could constitute a breach of human rights...".

B. Echelon: The Abuse of Power

Not only do former intelligence service officers attest to the existence of Echelon, but also to the abuse of its power. Evidence received by the Temporary Committee on the Echelon interception system supported the allegation that the N.S.A. had engaged in the unfair use of "its intelligence services to help U.S. firms win contracts." "The first came from a Baltimore Sun report which said the European consortium Airbus lost a $6bn contract with Saudi Arabia after [the] N.S.A. found [that] Airbus officials were offering kickbacks to a Saudi official." Evidence received by the Temporary Committee suggested "intervention by the Advocacy Center to the benefit of U.S. firms," and that Echelon was being used unfairly to engage in industrial espionage by passing sensitive information on to U.S. firms via the CIA.

The testimony of a former N.S.A. employee confirmed that "[a]s early as 1978, Echelon was capable of intercepting telecommunications to and from a particular person via satel-

---

137 Asser, supra note 118.
139 See Asser, supra note 118.
and alleged that conversations of U.S. Senator Strom Thurmond had been intercepted. Another ex-N.S.A. employee testified that industrial espionage had become Echelon's top priority, and that it was routinely being used to benefit U.S. companies. Troubled about the use of Echelon to intercept private civilian communications, this employee contended that it was even being utilized to spy on non-governmental organizations like Amnesty International and Greenpeace.

The testimony of a former Canadian Secret Service ("CSE") employee affirmed that Echelon monitored civilian communications. Alarmingly, he recalled "that the CSE actually had entered the name and telephone number of a woman in a database of possible terrorists because she had used an ambiguous phrase in a harmless telephone conversation with a friend." Another ex-CSE employee, who believed he was expelled from CSE because he criticized their new emphasis on civilian targets, testified to intercepting "information on trade with other countries, including negotiations on NAFTA, Chinese purchases of cereals and French arms sales," and to routinely targeting Greenpeace.

Even the ex-Director of the CIA, James Woolsey, has admitted that the U.S. conducts industrial espionage in Europe. Woolsey, however, maintained that 95% of the 'economic intelligence' collected by the U.S. is obtained by evaluating publicly accessible information, and only 5% comes from stolen secrets. Furthermore, Woolsey insisted that the economic intelligence obtained illegally is not passed on to U.S. companies, and is collected only "in order to combat bribery in connection with the award of [international] contracts."

If the current allegations are true, [however,] all abiding European citizens...
and companies are at risk of being monitored every day without any legal basis.\footnote{Yaman Akdeniz, Statement for the European Parliament, Temporary Committee on the Echelon Interception System, CYBER RIGHTS & CIVIL LIBERTIES, Mar. 22, 2001, at http://www.cyber-rights.org/reports/echelon_ya.pdf.}

IV. ANTI-TERROR MEASURES IN THE WAKE OF SEPTEMBER 11TH

tion-sharing. Unquestionably, the new investigative tools made available to intelligence gathering agencies throughout the world will play an integral role in fighting the war against international terrorism.

In the wake of September 11, 2001, the European Union ("EU") has also approved tough new measures to prevent future terrorist attacks. Just nine days after the attacks, "EU justice and home affairs ministers approved a total of thirty-seven proposals intended to stop terrorist groups from operating in the EU and to strengthen police and justice cooperation with the U.S." The newest EU anti-terror measures include a European search and arrest warrant, an agreement to strengthen information sharing among EU law enforcement authorities, and the establishment of an anti-terror unit within Europol.

Since September 11, 2001, at least forty countries have adopted a declaration expressing their "wholehearted support" for sharing intelligence on terrorist activity, and today, EU leaders continue to meet with U.S. officials regarding their supporting role in the war against terrorism. The Director of Europol, however, has recently warned that not all Member States


154 See Bush Remarks, supra note 151.


are prepared to exchange intelligence data with other countries and that the central problem involved balancing fundamental civil rights and freedoms with the increased need for international security measures.

Prime Minister Blair declared that the U.K. stood "side by side with . . . [the U.S.] now, without hesitation," and vowed to take action at every single level to eradicate the threat posed by international terrorism. Subsequently, the U.K. requested that communications service providers retain all logs of e-mails sent and received, all logs showing internet usage, and all logs of sources, destinations and times of all calls made on telephone networks. Not surprisingly, there has been wide criticism of the U.K. plan that would give law enforcement officials sweeping access to personal data. Even the U.K. Information Commissioner wrote: "The scope of the powers proposed to be given to the secretary of state is immensely broad. The lack of any overt safeguards against abuse indicates a lack of proportionality such as to render the prospective legislation incompatible with European [C]onvention rights."

Federal Chancellor Gerhard Schroeder also made assurances that Germany was prepared to "give its unreserved support to the United States of America" in the war against international terrorism. Toward that end, a number of "changes to German law [have been] rushed through both chambers of

159 See id.
160 See id.
161 Prime Minister of the United Kingdom Tony Blair, Remarks by the President and Prime Minister of the United Kingdom Tony Blair (Sept. 20, 2001), http://www.whitehouse.gov/news/releases/2001/09/20010920-7.html.
162 See id.
164 See Patrick Wintour, Lords 'Sabotage' Forces Concessions on Terror Bill, Guardian Unlimited, Dec. 8, 2001, at http://politics.guardian.co.uk/attacks/story/0,1320,615398,00.html.
165 Id.
the German parliament . . . " despite warnings about the "dangers for personal privacy . . . arising from new supervisory powers and the virtually unlimited access . . . by the intelligence services and national law enforcement agencies to [personal] data." 168 In particular, experts in Germany "criticized the extension of powers made to the intelligence services, as well as the inter-linking of data between various secret services." 169 "U.S. Attorney General John Ashcroft, [however,] praised Germany's newly enacted law . . . [as] a necessary measure in the war against terrorism." 170

On October 26, 2001, President George W. Bush signed the USA Patriot Act into law. 171 The USAPA not only grants U.S. authorities wide-ranging surveillance powers, 172 but removes several of the checks and balances that were in place prior to September 11, 2001, that prevented U.S. authorities from improperly conducting surveillance activities. 173 For computer users especially, the USAPA opens the door for widespread surveillance activity of the internet and e-mail systems. 174 Furthermore, "the protections against the misuse of these authorities — by the foreign intelligence agencies to spy on U.S. citizens and by law enforcement to use foreign intelligence authority to exceed their domestic surveillance authority — have

---


168 See Second Anti-terrorism Package, DIE BUNDESREGIERUNG, supra note 167.

169 Id.


171 See USAPA, supra note 151.

172 See Bush Signs Antiterrorism Bill into Law, supra note 151.


174 See id.
been greatly reduced." President Bush, however, maintains that the USAPA "protects, rather than erodes, civil liberties by increasing federal authorities' ability to prevent, rather than just respond to terrorist attacks." Since September 11, 2001, the N.S.A. has undoubtedly stepped up its use of the Echelon interception system "to monitor domestic and international e-mail traffic." In response, civil libertarians have expressed concern that the increased surveillance power provided by the USAPA will have an adverse impact on personal privacy because "in the government's fast-moving and expansive search for terrorists," an enormous amount of personal data will be intercepted, analyzed, and archived. If the proper safeguards are not put into place, the fundamental right to privacy in Europe may become the next casualty in the U.S. led war against international terrorism.

V. SURVEILLANCE ACTIVITY AND THE FUNDAMENTAL RIGHT TO PRIVACY IN EUROPE

Any activity "involving the interception of communications and even the recording of data by intelligence services ... represents a serious violation of an individual's privacy." The unrestricted interception of private communications by government authorities is only permitted in a 'police state.' In contrast, in the EU Member States, which are mature democracies," the necessity for government intelligence services to respect an individual's privacy is "unchallenged and is generally enshrined in national constitutions." "Privacy thus enjoys special protection: potential violations are authorized only following analysis of the legal considerations and in accordance with the principle of proportionality."

175 Id.
176 Bush Signs Antiterrorism Bill into Law, supra note 151.
177 Thorsberg, supra note 153.
178 Id.
179 See id.
181 See id.
182 Id.
183 Id.
184 Id.
The European Union has always affirmed its commitment to the protection of human rights and fundamental freedoms.185 The Treaty on European Union ("TEU") (as amended by the Amsterdam Treaty)186 ensures citizens of EU Member States the protection of those fundamental rights and freedoms guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR").187 These rights and freedoms are not only binding on Member States, but the "Union is also required to comply . . . in its legislation and administration."188 "This includes respect for privacy of communications and personal data."189

"In principle, activities and measures undertaken for the purposes of state security or law enforcement do not fall within the scope of the EC Treaty [Establishing the European Community ("EC Treaty")]. . . ."190 As a result, when a Member State utilizes the Echelon interception system for national security purposes, e.g., combating international terrorism, the State interference is entirely beyond the scope of the EC Treaty.191 Since Article X of the EC Treaty commits Member States to act

187 See The Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocol No. 11, Nov. 4, 1950, Europ. T.S. No. 5, 213 U.N.T.S. 221 [hereinafter ECHR]. See also TEU arts. 6, 7. Article 6 of the Treaty states:

(1) The Union is founded on the principles of liberty, democracy, respect for human rights, and fundamental freedoms, and the rule of law, principles which are common to the Member States.

(2) The Union shall respect all fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1959 and as they result from the constitutional traditions common to the Member States, as general principles of Community law.

in good faith, the use of Echelon to intercept private communications for industrial espionage purposes would be “fundamentally at odds with the concept of common-market underpinning the EC Treaty, as it would amount to a distortion of competition.” When a Member State utilizes the Echelon interception system to gain intelligence for industrial espionage purposes, either by “allowing its own intelligence service to operate such a system, or by giving foreign intelligence services access to its territory for this purpose, it would undoubtedly constitute a breach of EC law.”

When a EU Member State utilizes the Echelon interception system for national security purposes, e.g., combating international terrorism, they “cannot therefore be in breach of the EC’s data protection directives” because Directives 95/46/EC and 97/66/EC do not apply “to the processing of data

---

192 See EC Treaty art. 10. “Member States shall take appropriate measures, whether general or particular, to ensure fulfillment of the obligations arising out of this Treaty or resulting from action taken by the institutions of the Community. They shall facilitate the achievement of the Community's tasks. They shall abstain from any measures which could jeopardize the attainment of the objectives of this Treaty.” Id.


194 Id.

195 Id. at 80-81.

196 Id. at 81.

197 See id. at 80. Article 1 of the Directive states: “In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 1, 1995 O.J. (L281)1 [hereinafter Data Directive]. Article 3(2) of the Directive states: “This Directive shall not apply to the processing of personal data: in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the European Union, and in any case to processing operations concerning public security, defense, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.” Id. art. 3(2), 1995, O.J. (L281) 2.

198 See Parliament Report on ECHELON, supra note 57, at 80. Article 1 of the Directive states: “This directive provides for the harmonization of the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the telecommunications sector and to ensure the free movement of such data and of telecommunications equipment and services in the Community.” Council Directive 97/66 of 15 December 1977 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, art. 1, 1998 O.J. (L024) 1. Article 3 of the Directive states: “This
concerning public security, defense, [and] State security.

Similarly, the use of *Echelon* to process data intercepted from private communications cannot be in breach of Article 286 of the EC Treaty or Regulation 45/2001 because neither is applicable to the processing of data concerning State security, defense, or public security. The use of *Echelon* by a Member State to intercept competitive intelligence for industrial espionage purposes, however, would "be an infringement of the data protection directives for the telecommunications sphere," as the interception is "not being carried out for the purposes of security or law enforcement . . . and would consequently fall fully within the scope of the directive."

European law enforcement agencies have recommended "the adoption of 'data retention' requirements" that would require communications service providers to "archive information detailing the telephone calls, e-mail messages and other communications of their users." In the aftermath of September 11, 2001, Member States were finally able to reach political agreement on a Directive to update the existing Directive 97/66/EC.

---


200 See EC TREATY art. 286. Article 286 (1) of the Treaty states: "Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty." Article 286 (2) of the Treaty states: "The Council shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions appropriate."

201 See Parliament Report on ECHELON, supra note 57, at 81. See also Council Regulation 45/2001 of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on Free Movement of Such Data, art. 20(1)(d), 2001 O.J. (L008) 1.


203 Id. at 82.

204 Id.


206 Id.
EC.207 In July 2002, the European Parliament formally
adopted Directive 2002/58/EC,208 which permits Member States
to implement national measures that authorize the retention of
personal data.209 While Member States have until October 31,
2003 to implement the Directive, some States (e.g., Belgium,
France, Great Britain, and Spain) have already provided na-
tional regulations for the retention of electronic data.210 In the
interim, however, Directive 2002/58/EC neither "alters the ex-
isting balance between the individual's right to privacy and the
possibility for Member States to take measures . . . necessary
for the protection of public security, defense, [and] State secu-

A. The United Nations International Covenant on Civil and
Political Rights and The Charter of Fundamental
Rights of the European Union

"Privacy and freedom of expression are fundamental
human rights recognised in all major international and regional
agreements and treaties."216 At the United Nations level, Arti-
cle 17 of the U.N. International Covenant on Civil and Political Rights of December 16, 1966 (ratified by EU Member States), guarantees the fundamental right to privacy. The Covenant's Optional Protocol authorizes a "[Human Rights] Committee to receive and examine communications from individuals who claim to have been the victim of a breach of one of the rights established by the ICCPR." Since the Covenant's Optional Protocol has not been signed by the U.S., "individuals cannot appeal to the Human Rights Committee in the event of the violation of the Covenant by the U.S.A."

At the European level, the Charter of Fundamental Rights of the European Union was drafted with the objective of instituting measures in Europe for the protection of fundamental rights. In particular, Article 7 of the Charter expressly states that individuals have a fundamental right to respect for his or her private communications, and Article 8 affirms that individuals have a fundamental right to the protection of their personal data. Since the Charter has not yet been incorpo-


218 See ICCPR, supra note 217, art. 17. Article 17(1) of the Covenant states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." Id. Article 17(2) of the Covenant states: "Everyone has the right to the protection of the law against such interference or attacks." Id.

219 Conventions of the United Nations and of the Council of Europe on Human Rights, Status of Ratification of the Main International Texts on the Protection of Human Rights Adopted Under the Auspices of the United Nations, EUROPEAN PARLIAMENT, at http://www.europarl.eu.int/comparl/libe/elsj/charter/un_legislation_en.htm; Article 41(1) of the Covenant reads: "A State Party to the present Covenant may at any time declare under this article that it recognizes the competence of the Committee to receive and consider communications to the effect that a State Party claims that another State Party is not fulfilling its obligations under the present Covenant." Id.


222 See id. at pmbl.

223 See id. art. 7. "Respect for private and family life: Everyone has the right to respect for his or her private and family life, home, and communications." Id.

224 See id. art. 8. Article 8 of the Charter states:

(1) Everyone has the right to the protection of personal data concerning him or her.
rated into the EU Treaty, it is only binding “on the three institutions which pledged to comply with it in the Formal Declaration adopted during the Nice European Council: the Council, the Commission, and the European Parliament.”

Even when the Charter acquires full legal force through its incorporation into the Treaty, due account will have to be taken of its limited scope. Pursuant to Article 51, the Charter applies to “the institutions and bodies of the Union . . . only when they are implementing Union law.”

B. The European Convention for the Protection of Human Rights & Fundamental Freedoms

The European Convention for the Protection of Human Rights and Fundamental Freedoms (“ECHR” or the “Convention”) of November 4, 1950 (ratified by all Member States), is one of the greatest achievements of modern Europe. Governed by the rules of international law, the ECHR creates a uniform level of protection for the fundamental rights and freedoms guaranteed to all EU citizens. The ECHR not only guarantees respect for private and family life, home and correspondence “but also establishes the right to receive and impart information and ideas without interference by public authority . . . .” Today, the ECHR is the only effective European instrument that comprehensively protects individual privacy rights, and it now provides more than 450 million citizens of EU Member States the right to bring allegations claiming a vio-

(2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

(3) Compliance with these rules shall be subject to control by an independent authority. Id.

226 Id.
227 See generally ECHR, supra note 187.
229 See id.
231 Id.
lation of their rights under the Convention before the European Court of Human Rights ("the Court").

Section II of the Convention establishes the Court, a legal forum for "applications from any person, non-governmental organization or group of individuals claiming to be the victim of a violation . . . of the rights set forth in the Convention . . . ." The Court's jurisdiction extends "to all matters concerning the interpretation and application of the Convention," and parties contract "under international law to guarantee the rights enshrined in the ECHR and . . . [declare] that they will comply with the judgments of the European Court . . . ." Upon receiving an application alleging a breach of a protected right, the Court reviews the relevant national legal provisions and hands down judgment that "shall, if necessary, afford just satisfaction to the injured party."

The fundamental rights enshrined in the ECHR are not linked to nationality, but represent generally accepted rights guaranteed to all persons within the jurisdiction of the contracting parties. "The rights guaranteed by the ECHR vis-à-vis a contracting state are thus also enjoyed by persons outside the territory of that state if those persons suffer interference in the exercise of their right to privacy." This is particularly important here, since a specific characteristic of the issue of fundamental rights in the area of telecommunications surveillance is the fact that there may be a substantial geographical distance between the state responsible for the surveillance, the person under surveillance, and the location where the interception is actually carried out.

---

233 See Beddard, supra note 228, at 1.
234 ECHR, supra note 187, § 2, art. 34.
235 Id. § 2, art. 32.
236 Parliament Report on ECHELON, supra note 57, at 84.
237 ECHR, supra note 187, art. 41.
239 See id.
1. **Article 8 of the ECHR**

Article 8 of the ECHR guarantees everyone "the respect for his private and family life, his home and his correspondence."\(^2\)\(^4\)\(^2\) Although the plain language of the Convention contains no explicit reference to the protection of private telecommunications,\(^2\)\(^4\)\(^3\) the Court makes clear that the covert interception of private telecommunications falls within the scope of Article 8.\(^2\)\(^4\)\(^4\) Article 8 provides Europeans such broad protection against government interference with private telecommunications, that it "covers not only the substance of the communications, but also the act of recording external data."\(^2\)\(^4\)\(^5\) "In other words, even if an intelligence service merely records data such as the time and duration of calls and the numbers dialed, this represents a violation of privacy."\(^2\)\(^4\)\(^6\)

The essential object of Article 8 is to protect against arbitrary State interference with private communications.\(^2\)\(^4\)\(^7\) In order for State interference not to infringe on Article 8 of the Convention, "it must, according to paragraph 2, first of all have been *in accordance with the law*."\(^2\)\(^4\)\(^8\)

---

\(^2\)\(^4\)\(^2\) ECHR, *supra* note 187, art. 8. Article 8 of the Convention states:

1. Everyone has the right to respect for his private life and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the existence of this right except such as in accord 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. *Id.*

\(^2\)\(^4\)\(^3\) See *id.*


\(^2\)\(^4\)\(^8\) The Court has held that, [the expression *'in accordance with the law' in paragraph 2 of Article 8 requires that interference must have some basis in domestic law. Compliance with domestic law, however, does not suffice: the law in question must be accessible to the individual concerned and its consequences for
[I]n the context of covert surveillance by public authorities domestic law must provide protection against arbitrary interference with an individual's right under Article 8; [and] the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions under which authorities are entitled to resort to such covert measures.249

Article 8(2) of the Convention provides the legal basis for State interference with private communications.250 Contracting Parties, however, are not completely unrestricted in their authority to interfere with an individual's private life, and may only do so "for purposes listed in the second paragraph of Article 8, and in particular, in the interest of national security . . . ."251 Since the scope of Article 8(2) "only covers forms of interference 'necessary in a democratic society,'"252 Contracting
Parties are not justified in utilizing the Echelon interception system for the gathering of competitive intelligence for industrial espionage purposes.\(^{253}\)

While national security, e.g., combating international terrorism, can clearly be invoked by a Contracting State to justify the interception of private communications,\(^{254}\) the principle of proportionality still applies.\(^{255}\) The Court has held that a "State may not, in the name of the struggle against . . . terrorism, adopt whatever measures they deem appropriate."\(^{256}\)

In that connection, the European Court of Human Rights has clearly stated that the interest of the State in protecting its national security must be weighed against the seriousness of the invasion of an individual's privacy.\(^{257}\)

As a result, the "mere usefulness or desirability [of intelligence] is not sufficient justification"\(^{258}\) for the interference with private communications. The belief, therefore, "that the interception of all private telecommunications, even if permissible under national law, represents the best form of protection [against international terrorism], would amount to a breach of Article 8."\(^{259}\)

2. The Case Law: Article 8 of the ECHR

Given the covert nature of national intelligence services, the interception of private communications demands a careful

\(^{253}\) See Parliament Report on ECHELON, supra note 57, at 86.

\(^{254}\) See id. at 86.

\(^{255}\) See id.


\(^{259}\) Parliament Report on ECHELON, supra note 57, at 86-87 (emphasis added).
weighing of competing interests\textsuperscript{260} and requires that adequate provisions be made for the stringent monitoring of covert surveillance activities.\textsuperscript{261}

The European Court of Human Rights has explicitly drawn attention to the fact that a secret surveillance system operated for the purpose of protecting national security carries with it the risk that, under the pretext of defending democracy, it may undermine or even destroy the democratic system, so that more effective guarantees are needed to prevent such misuse of powers.\textsuperscript{262}

The use of \textit{Echelon} for the interception of private "communications can constitute an interference with the right to respect for private life and correspondence in breach of Art. 8(2), unless it is carried out in accordance with a legal provision capable of protecting against arbitrary interference by the State with the rights guaranteed."\textsuperscript{263} Moreover, the Court has held that since Article 8(2) "provides for an exception to a right guaranteed by the Convention, [it] is to be narrowly interpreted,"\textsuperscript{264} and in any given case, the need for the interference with private communications must be convincingly established.\textsuperscript{265}

Furthermore, the relevant provisions of domestic law must be both accessible and their consequences foreseeable, in that the conditions and circumstances in which the state is empowered to take secret measures such as telephone monitoring should be clearly indicated . . . .\textsuperscript{266}

In a case raising the applicability of a Swedish law with Article 8 of the Convention,\textsuperscript{267} the Court held that the law, which provided a system for maintaining a secret register of pri-

\begin{footnotesize}
\textsuperscript{260} See \textit{id. See also} Leander, 9 Eur. H.R. Rep. at 452.


\textsuperscript{264} Klass, 2 Eur. H.R. Rep. at 230.

\textsuperscript{265} \textit{See} Akdeniz, \textit{supra} note 150.


\textsuperscript{267} \textit{See} Leander, 9 Eur. H.R. Rep. 433.
\end{footnotesize}
vate information, was sufficiently clear that the interference with private life was "in accordance with the law."268 Noting that in special cases of national security, "the arrangements governing the foreseeability requirement must differ from those in other areas,"269 the Court concluded that the national law incorporated sufficient precautionary measures to meet the requirements of Article 8 of the Convention, and that the interference with privacy was lawful.270

In a case raising the applicability of a German law with Article 8 of the Convention,271 complainants argued that their fundamental right to privacy had been violated because the law did not require authorities to notify the individuals subject to surveillance after the surveillance had taken place.272 After holding that telephone conversations are "within ambit of 'private life' and the concept of 'correspondence,'"273 the Court agreed that the applicants may have been victims of a violation of Article 8 of the Convention.274 In order to determine whether the interference was 'necessary in a democratic society,'275 the Court developed a test that turned on the existence of adequate safeguards against possible abuse. Simply, "[t]he Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse."276

The Court initially expressed concern about the supervisory controls over the surveillance,277 but then held that the German law authorized the surveillance to an "official qualified for judicial office and by the Parliamentary Board and the

---

268 Id. (emphasis added).
269 Parliament Report on ECHELON, supra note 57, at 86.
272 See JACOBS & WHITE supra note 270, at 207.
273 Id.
274 See id.
275 See id. The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued. Parliament Report on Fundamental Rights, supra note 217, at 47. See also Foxley v. the United Kingdom, App. No. 33274/96, para. 43 (June 20, 2000).
277 See JACOBS & WHITE, supra note 270, at 207.
Commission." Taking judicial notice of technological improvements in the means of communications surveillance, and an increase in terrorist activity in Europe, the Court concluded that the German legislative scheme for regulating surveillance activities satisfied the requirements of Article 8 of the Convention, and that the Applicant's fundamental right had not been violated.

In a subsequent English case, law enforcement authorities were engaged in surveillance activity that involved the covert interception of telecommunications. The deficiency of an appropriate statutory framework governing the U.K.'s surveillance activity, however, proved fatal to the government's case. The Court stated:

[The law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities. To that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking.]

The Court concluded that the governmental interference with the Applicant's private telecommunications was not "in accordance with the law," and therefore a violation of Article 8 of the Convention.

Two subsequent French cases revealed the Court had found some middle ground. French courts have repeatedly interpreted their legislative framework as permitting the interception of private communications by senior law enforcement officials with the proper judicially issued warrants. To be 'in accordance with the law,' however, "the quality of the law must be such as to provide safeguards against what is a serious interference with private life." Since the French statutory frame-

---

279 See JACOBS & WHITE, supra note 270, at 207-08.
281 See JACOBS & WHITE supra note 270, at 208.
283 See JACOBS & WHITE supra note 270, at 208.
285 See JACOBS & WHITE supra note 270, at 208-09.
286 Id.
work was seriously lacking in measures to prevent abuse, the Court found violations of Article 8. The interception of private communications by the intelligence services of Contracting Parties, therefore, can only be consistent with the fundamental right to privacy guaranteed by the Convention if they are accompanied by an adequate system of checks and other measures to protect against the misuse of power.

3. *The Requirements Imposed by Article 8 of the ECHR*

The activities of an ECHR Contracting Party's intelligence service must be compatible with the requirements of law, and services must not move to circumvent Article 8 of the Convention. In particular, a Contracting Party must not be allowed to evade the requirements of law "by employing assistance from other intelligence services . . ." whose "activities are subject to less stringent rules." "Otherwise, the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance." One implication of this is that data exchanges "between intelligence services are permissible only on a restricted basis." Intelligence services "may seek from one of its counterparts only data obtained in a manner consistent with the conditions laid down in its own national law." Moreover, "[t]he geographical scope for action laid down by [national] law . . . may not be extended by means of agreements with other [intelligence] services," and a service "may carry out operations on behalf of another country's intelligence service . . . only if it is satisfied

287 See Jacobs & White, supra note 270, at 209. "The French system was very short on processes to prevent abuse, with key aspects of the process not adequately defined, such as the categories of person liable to have their telephone tapped or the nature of the offenses which warranted such measures." Id.

288 See id.

289 See Parliament Report on Fundamental Rights, supra note 222, at 47. See also Parliament Report on ECHELON, supra note 57, at 87.


291 See id.

292 Id.

293 Id.

294 Id.

295 Id. at 88.


297 Id.
that the operations are consistent with the national law of its
own country." Even though intercepted data may be "in-
tended for another country, this in no way alters the fact that
an invasion of privacy which could not be foreseen by the legal
subject concerned constitutes a violation of fundamental
rights." Another implication is that Contracting Parties
"may not allow other countries' intelligence services to carry out
operations on their territory if they have reason to believe that
those operations are not consistent with the conditions laid
down by the ECHR." 

"By ratifying the ECHR, the Contracting Parties undertook
to subject the exercise of their sovereignty to a review of its con-
sistency with fundamental rights." The Contracting Parties
"cannot seek to circumvent this requirement by foregoing the
exercise of that sovereignty," and they remain responsible for
surveillance operations taking place within their own territory,
even "if the sovereignty is usurped by the intelligence activities
of another State." Thus, when a Contracting Party allows a
non-Contracting Party to operate intelligence services from
within its territory, "the protection requirement is much
greater, because another authority is exercising its sover-
eignty. The only logical conclusion is that States must carry out
checks to ensure that the activities of intelligence services on
their territory do not represent a violation of human rights." 

If, for example, the U.S. were utilizing their Echelon satel-
ite receiving stations at Menwith Hill, U.K., and Bad Aibling,
Germany "to engage in the interception of non-military commu-
nications ... [by] private individuals or firms from an ECHR
Contracting Party, supervisory requirements would come
into play under the ECHR. In practical terms, ECHR Contracting Parties, Germany and the United Kingdom, are
required to establish that the activities of the American intelli-
gence services do not represent a violation of fundamental

298 Id.
299 Id.
300 Id. (citing Dimitri Yernault, ECHELON and Europe, The Protection of Pri-
vacy Against Communications Espionage, J. of the CTS., EUR. L., at 187 (2000)).
302 Id.
303 Id.
304 Id.
This is even more crucial now, in the wake of September 11, 2001, in light of the concern in Europe over the N.S.A.'s covert intelligence activities, and considering the enhanced U.S. surveillance powers, and strengthened cooperation and information sharing in the war against international terrorism.

When surveillance activities involve cooperation between two Contracting Parties, "both can assume, up to a certain point, that the other is complying" with the Convention. This assumption usually "applies until evidence emerges that an ECHR Contracting Party is violating the Convention on a systematic, long-term basis." Since the U.S. is not "an ECHR Party and it has not made its intelligence operations subject to a similar supervisory system," no such assumption applies.

Europeans have good reason to be concerned about U.S. surveillance activities in Europe, particularly in light of the fact that many of the relevant rules that "apply to the activities of the N.S.A. abroad . . . are classified" and not made available to the public. Disquietingly, the U.S. House of Representatives and Senate committees, which subject the N.S.A. to oversight, "show little interest in the activities of N.S.A. abroad," and even the N.S.A. recently backed out of meetings with a committee sent to Washington to learn more about the Echelon interception system.

There would seem to be good reason, therefore, to call on Germany and the United Kingdom to take their obligation under

---

305 Id. at 88-89.
306 Id. at 89.
308 Id.
309 See id.
310 See id.
311 See id.
312 See id.
ECHR seriously and to make authorization of further intelligence activities by N.S.A. on their territory contingent on compliance with ECHR.\footnote{Parliament Report on ECHELON, supra note 57, at 89.}

4. U.S. Intelligence Gathering Activity: Conformity with the ECHR

The covert interception of private communications in Europe by U.S. intelligence services can only be in conformity with the ECHR if the following three requirements are met. First, U.S. interference with private communications in Europe “may only be carried out on the basis of legal rules which are generally accessible and whose implications for individuals are foreseeable.”\footnote{Id.} This requirement, however, “can be met only if the U.S. discloses to the public in Europe how and under what circumstances intelligence-gathering is carried out.”\footnote{Id.} In addition, when U.S. regulations governing the interference with private communications in Europe are incompatible with the terms of the Convention, they “must be brought into line with the level of protection provided in Europe.”\footnote{Id.}

Second, U.S. interference “must be proportional, and . . . the least invasive methods must be chosen.”\footnote{Id.} Since only interference carried out by a European intelligence service can be reviewed in the national courts, “operations constituting interference must be carried out, as far as possible, by the German or U.K. authorities,”\footnote{Id. at 90.} especially when surveillance activity is being carried out for law enforcement purposes.\footnote{See Parliament Report on ECHELON, supra note 57, at 90.} Although the U.S. has “repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes,”\footnote{Id. (citing James Woolsey, Why We Spy on Our Allies, WALL ST. J., Mar. 17, 2000, at A14).} unless there is evidence of criminal activity

the USA must leave the task of law enforcement to the host countries. If there is no such evidence, [the] surveillance must be re-
garded as unproportional, a violation of human rights and thus inadmissible. In other words, compliance with the ECHR can be guaranteed only if the USA restricts itself to surveillance measures conducted for the purpose of safeguarding its national security, but not for law enforcement purposes.\textsuperscript{322}

Lastly, "[ECHR] has stipulated that compliance with fundamental rights is contingent on the existence of adequate monitoring systems and guarantees against abuse."\textsuperscript{323} The N.S.A.'s utilization of the \textit{Echelon} interception system from satellite receiving stations in EU Member States, therefore, can only be consistent with the fundamental right to privacy in Europe "if the USA introduces appropriate, checks on such operations carried out for the purposes of safeguarding its national security or if the N.S.A. makes its operations on European territory subject to the authority of the control bodies set up by the host state, i.e., Germany or the United Kingdom."\textsuperscript{324}

\section*{VI. Analysis}

In the aftermath of September 11, 2001, the European Parliament has swept aside concerns about the \textit{Echelon} interception system, as well as the N.S.A.'s covert surveillance activities in Europe.\textsuperscript{325} After a cursory debate, a British Labor Party member justified the move, stating that there "is not enough information on \textit{Echelon}, beyond its existence, to debate the matter [more] fully."\textsuperscript{326} A Green Party member, however, "suggested that the Parliament is reluctant to probe the matter [more] fully for fear of jeopardizing relations between the EU and the United States,"\textsuperscript{327} and that "they [simply] didn't want to rock the boat."\textsuperscript{328} Nonetheless, civil rights groups view the recent \textit{Echelon} debate in the European Parliament as a major victory that "fire[d] a warning shot across the bows of the N.S.A."\textsuperscript{329}

\textsuperscript{322} \textit{Id.}
\textsuperscript{323} \textit{Id.}
\textsuperscript{324} \textit{Id.}
\textsuperscript{326} \textit{Id.}
\textsuperscript{327} \textit{Id.}
\textsuperscript{328} \textit{Id.}
\textsuperscript{329} \textit{Id.}
Presently, Echelon's satellite receiving stations collect the remnant wavelengths of global communications throughout the world, and dictionary supercomputers instantly search the intercepts for keywords that might provide the U.S. Intelligence Community valuable COMINT. Echelon's interception capabilities go far beyond traditional wiretapping techniques, however, as the surveillance system allows the N.S.A. to intercept an enormous number of private communications simultaneously. Although Echelon's vast interception capabilities make it an effective tool in fighting the war against international terrorism, its broad surveillance powers clearly infringe upon the fundamental right to privacy in Europe.

The U.S. Intelligence Community spends billions of dollars for state-of-the-art communications technologies, but has never confirmed the existence of Echelon. The European Parliament, however, recently confirmed Echelon's existence as a global system for the interception of private and commercial communications. Notwithstanding its interception capabilities, international terrorist organizations can easily deceive Echelon's supercomputers by crafting cryptic communications that do not use traditional words of terror like 'bomb' and 'embassy' when planning an attack. As a result, Echelon is not so much a concern for international terrorists, but rather for the millions of people throughout the world whose private communications are routinely intercepted from the airwaves without warning.

Having already invested billions on Echelon, the N.S.A. will undoubtedly continue to utilize its interception capabilities to fight the war against international terrorism. Even after their widely publicized failure to translate cryptic messages intercepted on September 10, 2001, until the day after the attacks, the N.S.A. remains hopeful that Echelon's interception capabilities will help to prevent future terrorist attacks. Since the N.S.A. cannot process, analyze, and disseminate sensitive COMINT in real time, advanced international interception systems, such as Echelon, will continue to be unsuccessful in preventing major terrorist attacks against our homeland.

VII. Conclusion

As a result of the tragic events which shook our nation on September 11, 2001, the primary focus of the U.S. Intelligence
Community will be on the collection, analysis, and dissemination of data concerning international terrorist organizations. Toward that end, the USAPA now provides U.S. intelligence services the wide-ranging surveillance powers required to effectively fight the war against international terrorism. Since the need for international cooperation among intelligence services will be essential to winning the war against terrorism, the U.S. will continue to work closely with its UKUSA partners around the world.

The N.S.A. will continue to play a lead role in the global hunt for international terrorists and will undoubtedly continue to utilize Echelon to eavesdrop on global communications. Wielding the new surveillance tools provided by the USAPA, the N.S.A. will now bring its broad powers to bear on European citizens from its interception stations throughout the world. Even in the context of fighting the war against international terrorism, the N.S.A.'s surveillance activities in Europe must be subject to rigorous oversight, and guarantees must be provided to safeguard against abuse. If the N.S.A.'s surveillance activities abroad continue to remain classified, and the circumstances under which the U.S. can exercise surveillance on European citizens are not made available to the public, then advanced international interception systems, such as Echelon, will continue to infringe upon the fundamental right to privacy in Europe.