Pace International Law Review

Volume 14
Issue 2 *Fall 2002*

Article 7

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

# POST-SEPT. 11TH INTERNATIONAL SURVEILLANCE ACTIVITY — A FAILURE OF INTELLIGENCE: THE *ECHELON* INTERCEPTION SYSTEM & THE FUNDAMENTAL RIGHT TO PRIVACY IN EUROPE

**Kevin J. Lawner***



* 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-

---

[1] President Chirac Pledges Support, Remarks by President Bush and President Chirac of France in Photo Opportunity (Sept. 18, 2001), *at* http://www.whitehouse.gov/news/releases/2001/09/20010918-8.html.

[2] *See Global Threats and Challenges: Hearing Before the Senate Armed Services Comm.*, 107th Cong. 2 (2002) (statement of Vice Admiral Thomas R. Wilson, Director, Defense Intelligence Agency) [hereinafter Wilson Statement].

[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 Yemini 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.[5] While the military strikes of *Operation Enduring Freedom,*[6] and the arrests or detention of terror suspects throughout the world have significantly disrupted Usama bin Laden's Al Qaeda network,[7] the most recent intelligence reports suggest that bin Laden is still alive,[8] and hiding in the moun-

---

[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].

[6] *See generally* THE U.S. ARMY, OPERATION ENDURING FREEDOM, *at* http://www.army.mil/enduringfreedom/default.html (last visited Oct. 16, 2002).

[7] *See generally Somalis Arrest Terror Suspect*, BBC NEWS, Sept. 21, 2001, *at* http://news.bbc.co/uk/hi/world/africa/1723186.stm; *Spain Arrests Six Terror Suspects*, BBC NEWS, Sept. 26, 2002, *at* http://news.bbc.co/uk/hi/world/europe/1564341.stm; *Who is Richard Reid?*, BBC NEWS, Dec. 28, 2001, *at* http://news.bbc.co/uk/1/low/uk/1731568.stm; John Tagliabue, *A Nation Challenged: The Suspects; Arrests in Belgium Highlight Its Role as a Militants' Base,* N.Y. TIMES, Dec. 20, 2001, at B5; *Singapore Arrests Terror Suspects*, BBC NEWS, Jan. 5, 2002, *at* http://news.bbc.co.uk/hi/english/world/asia-pacific/newsid_1743000/1743981.stm; *A Nation Challenged: Suspects; 6 Tied to Terror Are Given to U.S. by Bosnia, Despite Court Ruling*, N.Y. TIMES, Jan. 19, 2002, at A8; Philip Shenon, *A Nation Challenged; U.S. Labels an Arab Captive A Planner of Qaeda Attacks*, N.Y. TIMES, Jan. 23, 2002, at A8; James Risen, *A Nation Challenged: The Threat; Qaeda Still Able To Strike U.S., Head of CIA Says*, N.Y. TIMES, Feb. 7, 2002, at A1; Ian Fisher, *A Nation Challenged: The Balkins: Details of a Terrorist Plot Still Cloaked in Confusion*, N.Y. TIMES, Mar. 7, 2002, at A15; James Risen & Philip Shenon, *U.S. Says It Halted Qaeda Plot to Use Radioactive Bomb*, N.Y. TIMES, June 11, 2002, at A28; Steven Erlanger, *Germans Say Figure Linked to Sept. 11 is in Syria Jail*, N.Y. TIMES, June 19, 2002, at A8; Douglas Frantz, *German Police Quiz Roommate of Top Hijacker*, N.Y. TIMES, July 4, 2002, at A1; *South-East Asia's Terror Clampdown*, BBC NEWS, July 12, 2002, *at* http://news.bbc.co.uk/1/hi/world/americas/2196451.stm; Danny Hakim, *4 Are Charged With Belonging To a Terror Cell*, N.Y. TIMES, Aug. 29, 2002, at A1; Melissa Eddy, *Germans Arrest Pair in Bomb Plot,* THE BOSTON GLOBE, Sept. 7, 2002, at A1; Raymond Bonner, *Plan to Attack Embassies Cited, U.S. Says Qaeda Member Told of Threat to Offices in Asia*, N.Y. TIMES, Sept. 11, 2002, at A1; John F. Burns, *Qaeda Remnants Hunted Along Pakistan Border*, N.Y. TIMES, Sept. 11, 2002, at A23; *Italian Police Arrest Terror Suspects*, BBC NEWS, Sept. 12, 2002, *at* http://news.bbc.co.uk/2/hi/world/europe/2253097.stm; Raymond Bonner, *Singapore Announces Arrests of 21 Men Linked to Planned Attacks on U.S. Targets*, N.Y. TIMES, Sept. 17, 2002, at A17; Philip Shenon, *6 Suspects Charged Under Broadly Worded Act*, N.Y. TIMES, Sept. 17, 2002, at A17; John Kifner & Marc Santora, *U.S. Names 7th Man in Qaeda Cell Near Buffalo and Calls His Role Pivotal*, N.Y. TIMES, Sept. 18, 2002, at A19; John F. Burns, *Afghans Intercept Fuel Truck Aimed at U.S.-Run Air Base*, N.Y. TIMES, Sept. 18, 2002, at A19.

[8] *See* Associated Press, *Senator: Intelligence Indicates bin Laden Still Alive*, USA TODAY, Dec. 31, 2001, *at* http://www.usatoday.com/news/attack/2001/12/31/binladen-alive.htm; *see also Bin Laden 'on TV Soon'*, BBC NEWS, June 23, 2002, *at* http://news.bbc.co.uk/1/hi/world/southg_asia/2060561.stm.

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.

[10] *First War of the Century* (Al-Jazirah television broadcast, Dec. 27, 2001) (statement by Usama bin Laden) (translated by the Foreign Broadcast Information Service) (transcript on file with author).

[11] *See generally America's 'Most Wanted Terrorists'*, BBC NEWS, Oct. 10, 2001, *at* http://news.bbc.co.uk/2/hi/world/americas/1591997.stm; Risen, *supra* note 7; Statement of Defense Official, U.S. Dep't of Defense, Background Briefing on the Al Qaeda Terrorist Network (Feb. 19, 2002), *at* http://www.fas.org/irp/world/para/alqaeda_dod021902.html; James Dao, *Taliban and Al Qaeda Believed Plotting Within Pakistan*, N.Y. TIMES, May 28, 2002, at A1; Howard W. French, *Pakistani Intelligence Officials See Qaeda Peril in Their Cities*, N.Y. TIMES, May 29, 2002, at A8; Eric Schmitt, *Pentagon Official Warns Asians to Guard Against Terror*, N.Y. TIMES, June 1, 2002, at A6; Belinda Rhodes, *Al Qaeda's Continuing Threat*, BBC NEWS, Mar. 11, 2002, *at* http://news.bbc.co.uk/2/hi/world/americas/19999054.stm; *US 'Faces Suicide Bomb Threat'*, BBC NEWS, May 20, 2002, *at* http://news.bbc.co.uk/1/hi/world/americas/1999054.stm; James Risen & Dexter Filkens, *Qaeda Fighters Said to Return to Afghanistan*, N.Y. TIMES, Sept. 10, 2002, at A1; *Al Qaeda Planning Attacks*, BBC NEWS, Sept. 11, 2002, *at* http://news.bbc.co.uk/2/hi/world/americas/2249797; Raymond Bonner, *Plan to Attack Embassies Cited, U.S. Says Qaeda Member Told of Threat to Offices in Asia*, N.Y. TIMES, Sept. 11, 2002, at A1.

[12] OFFICE OF THE PRIME MINISTER, UK REPORT ON RESPONSIBILITY FOR THE SEPTEMBER 11 TERRORIST ATTACKS, para. 21 (Oct. 4, 2001), http://www.fas.org/irp/news/2001/10/ukreport.html.

[13] *Id.* para. 22.

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

[15] *See* Tenet Statement, *supra* note 4.

stolen from an enterprise in the former Soviet Union.[16] After the attacks of September 11, 2001, bin Laden boasted to a Pakistani newspaper that "Al-Qaeda [now] possess[ed] chemical and nuclear weapons,"[17] and was prepared to use them if necessary.[18]

Today, "experts agree that the most effective way to fight [international] terrorism is to gather as much intelligence as possible,"[19] in order to prevent future attacks before they can be executed.[20] In simple terms, intelligence gathering "gives us an information advantage over our adversaries,"[21] 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."[22] Since intelligence gathering will be "the front line in the war against [international] terrorism,"[23] the new emphasis of the United States Intelligence Community[24] will undoubtedly be on the interception and analysis of foreign communications.[25]

---

[16] *See* NAT'L INTELLIGENCE COUNCIL, ANNUAL REPORT TO CONGRESS ON THE SAFETY AND SECURITY OF RUSSIAN NUCLEAR FACILITIES AND MILITARY FORCES (Feb. 2002), *available at* http://www.fas.org/irp/nic/icarussiansecurity.htm.

[17] *Bin Laden 'Has Nuclear Weapons'*, BBC NEWS, Nov. 10, 2001, *at* http://news.bbc.co.uk/2/hi/world/south_asia/1648572.stm. *See also* Hamid Mir, *Osama Claims He Has Nukes: If US Uses N-Arms It Will Get Same Response*, DAWN THE INTERNET EDITION, Nov. 9, 2001, *at* http://www.dawn.com/2001/11/10/top1.htm.

[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).

[22] OFFICE OF HOMELAND SECURITY, NATIONAL STRATEGY FOR HOMELAND SECURITY 17 (2002).

[23] Shelley Davis, *Piecing It Together*, THE RETIRED OFFICER MAGAZINE, *at* http://www.troa.org/Magazine/June2002/f_piecing.asp (last visited June 12, 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

---

[26] *See* AL QAEDA TRAINING MANUAL, FIFTH LESSON: MEANS OF COMMUNICATION AND TRANSPORTATION, *at* http://www.fas.org.irp/worl/para/manuelpart1.html (last visited June 12, 2002).

[27] Susan Stellin, *Terror's Confounding Online Trail*, N.Y. TIMES, Mar. 28, 2002, at G1.

[28] Daniel Sieberg, *Bin Laden Exploits Technology to Suit his Needs*, CNN.COM, Sept. 21, 2001, *at* http://www.cnn.com/2001/US/09/20/inv.terrorist.search/index.html.

[29] *See id.*

[30] *Id.*

[31] *The Terrorist Threat Confronting the United States: Hearing Before the Senate Select Comm. on Intelligence,* 107th Cong. (2002) (statement by Dale L. Watson, Executive Assistant Director, Counterterrorism and Counterintelligence, Federal Bureau of Investigation), http://www.fas.org/irp/congress/2002_hr/020602watson.html.

[32] *See* Press Release, National Security Agency Central Security Service, President George W. Bush Visits the N.S.A. Commends On 50 Years of Cryptologic Service to the Nation Personally Thanks Work Force For Its Efforts in the War Against Terrorism (June 4, 2002), *at* http://www.nsa.gov/releases/20020604.htm [hereinafter N.S.A. Press Release].

[33] The N.S.A. is a secretive, "separately organized agency within the Department of Defense . . . [that] employs the country's premier codemakers and codebreakers." *Statement for the Record: Hearing on Critical Skills for National Security and the Homeland Security Federal Workforce Act Before the Governmental Affairs Subcommittee on Int'l Security, Proliferation, and Federal Services*, 107th Cong. (Mar. 12, 2002) [hereinafter *Hearing on Critical Skills*]. *See id.*

1952,[34] the N.S.A. has conducted "electronic surveillance to collect foreign intelligence . . . ,"[35] and today, is rumored "to have more computing power than any other institution on earth . . . . ."[36] The "N.S.A.'s mission is to exploit secret foreign communications and produce foreign intelligence information while protecting U.S. communications."[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."[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."[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.[40] Similarly, the conversations intercepted on the day before September 11, 2001,[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

---

[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).

[35] *Statement for the Record: Hearing on the Regulation and Oversight of the National Security Agency's Electronic Surveillance Activities Before the House Permanent Select Committee on Intelligence*, 105th Cong. (Apr. 12, 2002) (statement of N.S.A. Director L.T. Gen. Michael V. Hayden, USAF) [hereinafter Hayden Statement].

[36] James Risen & David Johnston, *Agency Is Under Scrutiny for Overlooked Messages*, N.Y. TIMES, June 20, 2002, at A1.

[37] *Hearing on Critical Skills*, *supra* note 33. *See also* Exec. Order No. 12333, 46 Fed. Reg. 59941 (Dec. 4, 1981).

[38] Hayden Statement, *supra* note 35.

[39] *60 Minutes: National Security Meltdown* (CBS television broadcast, June 19, 2002) (transcript on file with PACE INT'L L. REV.).

[40] *See id.*

[41] On September 10, 2001, N.S.A. intercepts caught Al Qaeda operatives boasting in Arabic that "The match begins tomorrow" and "Tomorrow is Zero Hour." *See* John Diamond & Kathy Kiely, *Heard 9/10: Tomorrow is Zero Hour*, USA TODAY, June 19, 2002, at A1. *See also* John Tagliabue, *Cryptic Tapes From 2000 Hinted at Air Attack in U.S.*, N.Y. TIMES, May 30, 2002, at A1.

"became the focus of an eight-hour closed door hearing on Capital-Hill."[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.[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,"[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.[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."[46] Following the attacks, European privacy and civil liberties organizations from Austria, Denmark, Germany, the Netherlands, and the United Kingdom

---

[42] Bill Gertz, *For Years, Signs Suggested 'That Something Was Up,'* WASH. TIMES, May 17, 2002, at A1. *See also* Kevin Anderson, *US Intelligence Efforts Fractured*, BBC NEWS, May 18, 2002, *at* http://news.bbc.co.uk/2/hi/americas/1994710.stm; Nicholas M. Horrock, *Bush: 9/11 Questions Persist*, WASH. TIMES, May 19, 2002, *at* http://www.washtimes.com/upi-breaking/19052002-051817-3684r.htm; Diamond & Kiely, *supra* note 41; James Risen, *Qaeda Attack Was in Works for 3 Years, Officials Say*, N.Y. TIMES, June 19, 2002, at A18; *Threats and Responses: A Reaction to Sept. 11: 'This is a Massive Failure of Intelligence'*, N.Y. TIMES, Sept. 10, 2002, at A18; James Risen, *White House Drags its Feet on Testifying at 9/11 Panel*, N.Y. TIMES, Sept. 12, 2002, at A12; Hill Statement, *supra* note 24; James Risen, *U.S. Failed to Act on Warnings in '98 of a Plane Attack*, N.Y. TIMES, Sept. 18, 2002, at A6; Part II.A., *infra*.

[43] *See* STAFF OF SENATE COMM. ON COMMERCE, SCIENCE, AND TRANSPORTATION, 107th Cong., 2nd Sess., REPORT ON TECHNOLOGY ASSESSMENT IN THE WAR ON TERRORISM AND HOMELAND SECURITY: THE ROLE OF OTA 107-61 (Comm. Print 2002), *available at* http://fas.org/irp/congress/2002_hr/ota.html. *See also US Losing Hi-Tech Spying Race*, BBC NEWS, Aug. 15, 2001, *at* http://news.bbc.co.uk/2/hi/sci/tech/1491102.stm.

[44] *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 *Recommendation*].

[45] *See* Joris Evers, *Euro Civil Liberty Campaigners Urge Restraint*, CNN.COM, Nov. 4, 2001, *at* http://www.cnn.com/2001/TECH/industry/11/04/civil.liberties.idg/index.html.

[46] *Recommendation*, *supra* note 44, para. 2.

have urged the Council of Europe to defend the fundamental rights and freedoms of Europeans.[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,[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")[49] is practiced by virtually all developed countries throughout the world in order

---

[47] *See* Evers, *supra* note 45.

[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.

[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. "'[C]ommunications 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/ic/icdoc1.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."[50] Traditionally associated with the interception of military and diplomatic communications,[51] over the past half-century, COMINT has become "a large-scale industrial activity" providing consumers with intelligence on economic and scientific developments as well.[52]

Following World War II, a secret international agreement known as the United Kingdom–United States Security Agreement ("UKUSA" or the "Agreement"), was made.[53] Formalized in 1948, this clandestine accord effectively fashioned the first cooperative alliance between international intelligence gathering agencies.[54] 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.[55] Since "[the] 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."[56] While its signatories still refuse to officially acknowledge its existence, the Agreement is explicitly referred to

---

5100.20 (Dec. 23, 1971) (last modified Feb. 8, 1973), *available at* http://www.fas.org/irp/offdocs/nscid09.htm. *See also* NAT'L SECURITY COUNCIL, SIGNALS INTELLIGENCE, NATIONAL SECURITY COUNCIL INTELLIGENCE DIRECTIVE No. 6 (Feb. 17, 1972), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/05-01.htm.

[50] SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT PANEL, EUR. PARL, DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION: PRESENTATION AND ANALYSIS (Dec. 1999) [hereinafter DEVELOPMENT OF SURVEILLANCE TECHNOLOGY]; SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT PANEL, EUR. PARL., DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION (Oct. 1999) [hereinafter STOA], http://www.iptvreports.mcmail.com/ic2kreport.htm.

[51] *See* STOA, *supra* note 50.

[52] *See id.*

[53] *See generally* JAMES BAMFORD, THE PUZZLE PALACE, INSIDE THE NATIONAL SECURITY AGENCY, AMERICA'S MOST SECRET INTELLIGENCE ORGANIZATION (1983); JEFFERY T. RICHELSON & DESMOND BALL, THE TIE THAT BINDS (1985); Nickey Hager, Secret Power (1996); Patrick S. Poole, *Echelon: America's Secret Global Surveillance Network* (1999/2000), *at* http://fly.hiwaay.net/~pspoole/echelon.html.

[54] *See* STOA, *supra* note 50.

[55] *See* Duncan Campbell, *Paper 1: Echelon and its Role in COMINT*, TELEPOLIS, May 27, 2001, para 15-17, *at* http://www.heise.de/tp/deutsch/special/ech/7747/1.html.

[56] RICHELSON & BALL, *supra* note 53, at 7.

in a U.K. Parliamentary monitoring body report[57] and has been recognized by both the Prime Minister of New Zealand[58] and the former director of the Australian intelligence service [DSD].[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."[60] The fall of communism in the Soviet Union, however, "brought about dramatic changes inside all western intelligence agencies,"[61] and with its principle target suddenly gone, "intelligence agencies faced a period of downsizing . . . ."[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."[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.[64] It quickly became apparent that international coopera-

---

[57] *See* INTELLIGENCE AND SECURITY COMMITTEE, ANNUAL REPORT, 1999-2000, Cm. 4897, para. 14 , *available at* http://www.archive.official-documents.co.uk/document/cm48/4897/4897-02.htm#gen76. *See also* Report on the Existence of A Global System For the Interception of Private and Commercial Communications (ECHELON) Interception System, EUR. PARL. DOC. (A5-0264/2001) 59 (2001) [hereinafter Parliament Report on ECHELON].

[58] Noting "[t]he operation of the GCSB is directed solely by the New Zealand Government. It is, however, a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology." DOMESTIC AND EXTERNAL SECURITY SECRETARIAT, DEP'T OF THE PRIME MINISTER AND CABINET OF NEW ZEALAND, SECURING OUR NATION'S SAFETY, HOW NEW ZEALAND MANAGES ITS SECURITY AND INTELLIGENCE AGENCIES 27 (2000), http://www.dpmc.govt.nz/dess/securingoursafety/sons2000.pdf. *See* Parliament Report on ECHELON, *supra* note 57, at 61.

[59] *See* Letter from Martin Brady, Director of DSD, to Ross Coulthart, Reporter, Nine Network Australia (Mar. 16, 1999), *at* http://www.igis.gov.au/annuals/1998_99/annex2.html. *See also* Parliament Report on ECHELON, *supra* note 57, at 62.

[60] Duncan Campbell, *Paper 2: COMINT Impact on International Trade*, TELEPOLIS, May 27, 2001, para. 3, *at* http://www.heise.de/tp/deutsch/special/ech/7752/1.html.

[61] *Id.* para. 4.

[62] *Id.*

[63] *Id.*

[64] *See id.*

tion among intelligence services was the most effective means of battling these more contemporary global problems.[65] 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.[66] 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."[67] 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 . . . ."[68] 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,[69] 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."[70]

### 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.*

[66] *See* Press Release, U.S. Senate Select Committee on Intelligence, Senate Select Committee on Intelligence Authorizes Intelligence Spending for Fiscal Year 2002 (Sept. 6, 2001), *available at* http://www.fas.org/sgp/news/2001/09/ssci_010906.html.

[67] *Id.*

[68] John Diamond & Kathy Kiely, *Heard 9/10: 'Tomorrow is Zero Hour,'* USA TODAY, June 19, 2002, *at* A1.

[69] *See* US. GENERAL ACCOUNTING OFFICE, COMBATING TERRORISM: SELECTED CHALLENGES AND RELATED RECOMMENDATIONS (Sept. 2001).

[70] Eric Schmitt, *A Nation Challenged: The Intelligence Agencies; Job Seekers Flood Spy Agencies*, N.Y. TIMES, Oct. 22, 2001, at B7.

the U.S. using aircraft.[71] 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,[72] and that the impending attacks were thought likely to be directed at targets outside the U.S.[73] "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."[74]

The Intelligence Community also possessed ample evidence prior to September 11, 2001, which indicated that terrorists were contemplating the use of airplanes as weapons.[75] 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."[76] 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."[77]

---

[71] *See* Hill Statement, *supra* note 24, at 26-30. *See also* Gertz, *supra* note 42; David E. Sanger, *Bush Was Warned Bin Laden Wanted To Hijack Planes*, N.Y. TIMES, May 15, 2002, at A1; Philip Shenon, *F.B.I. Knew for Years About Terror Pilot Training, Bureau Failed to Share Its Finding, and to Connect the Dots*, N.Y. TIMES, May 18, 2002, at A1; David Johnston, *Ashcroft Learned of Agent's Alert Just After 9/11*, N.Y. TIMES, May 20, 2002, at A1.

[72] *See* Gertz, *supra* note 42. *See also* David Corn, *The bin Laden Warnings: Why Did Bush Keep It a Secret?* THE NATION, May 16, 2002, *at* http://www.thenation.com/capitalgames/index.mhtml?bid=3#pid=60.

[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.*

[75] *See id.* at 26-30. *See also* James Risen, *U.S. Failed to Act on Warnings in '98 of a Plane Attack*, N.Y. TIMES, Sept. 18, 2002, at A6.

[76] Hill Statement, *supra* note 24, at 27. *See also 9/11 Inquiry Reveals WTC Threat in 1998*, N.Y. TIMES, Sept. 18, 2002, *at* http://www.nytimes.com/reuters/news/nows-attack-intelligence.html; *Report Cites Warnings Before 9/11*, CNN.COM, Sept. 18, 2002, *at* http://cnn.com/2002/ALLPOLITICS/09/18/intelligence.hearings/index.html.

[77] James Risen, *Intelligence Officials Discount '98 Report From Caribbean of Plot to Hit Trade Center*, N.Y. TIMES, Sept. 20, 2002, at A14.

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.[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.[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."[80] In fact, the "1998 declaration did not adequately reflect a true 'war' effort against bin Laden."[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."[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."[83] The "chatter" of impending attacks was so great between May and July 2001,[84] "that the National Security Agency reported at least 33 communications indicating a possible, imminent terrorist attack."[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

---

[78] *See* Hill Statement, *supra* note 24, at 9.

[79] *Id.*

[80] *Id.* at 10.

[81] *Id.* at 18.

[82] *Id.*

[83] *Id.* at 10.

[84] *See* Nicholas M. Horrock, *Bush: 9/11 Questions Persist*, WASH. TIMES, May 19, 2002, *at* http://www.washtimes.com/upi-breaking/19052002-051817-3684r.htm. *See also* Julian Borger, *U.S. Asks: Just What Did Bush Know?*, GUARDIAN UNLIMITED, May 17, 2002, *at* http://guardian.co.uk/september11/story/0,11209,717179,00.html.

[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.[86] Despite these intelligence reports, "authorities did little to 'harden the homeland' against an assault."[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"[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."[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 . . . "[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."[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,"[92] and explicitly referred to Usama bin Laden and his Al Qaeda network.[93] Agent Williams' recommendation, however, was turned down by F.B.I. headquarters in Washington,[94] and to compound this failure,

---

[86] *See* Gertz, *supra* note 42. *See also* Horrock, *supra* note 84.

[87] *Congress Opens Investigation of Sept. 11 Attacks to Public*, N.Y. TIMES, Sept. 18, 2002, *at* http://www.nytimes.com/aponline/national/AP-Attacks-Intelligence.html.

[88] Hill Statement, *supra* note 24, at 10.

[89] *Id.*

[90] *Id.*

[91] Gertz, *supra* note 42.

[92] *Id.*

[93] *See id. See also* Borger, *supra* note 84.

[94] *See* Borger, *supra* note 84.

they "basically kept this [information] in," and did not share it with the rest of the Community.[95]

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."[96] 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,"[97] but were stifled by F.B.I. headquarters in Washington.[98] 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."[99]

A "veteran agent and general counsel in the Minneapolis [field] office,"[100] 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."[101] In response to Ms. Rowley's criticisms,[102] F.B.I. Director Robert S. Mueller III agreed that "the Minneapolis and Phoenix situations should have been handled differently,"[103] and that Agent Williams' Phoenix Memo "should have been shared with the CIA."[104] Mr. Mueller also acknowledged that even though the "Moussaui information and the Phoenix memo went to the same unit at [Washington] headquarters . . . no connection was made

---

95 *See* Gertz, *supra* note 42.

96 *Id. See also* Neil A. Lewis, *F.B.I. Chief Admits 9/11 Might Have Been Detectable*, N.Y. TIMES, May 30, 2002, at A1.

97 Lewis, *supra* note 96.

98 *See* David Johnston & Neil A. Lewis, *Whistle-Blower Recounts Faults Inside the F.B.I.*, N.Y. TIMES, June 6, 2002, *at* http://www.nytimes.com/2002/06/07/politics/07INQU.html.

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.*

[between the two,]"[105] 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."[106]

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.[107] 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.[108] 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.[109] One of the suspects was actually listed in the public telephone directory,[110] and the other had frequently used his credit card in his own name.[111]

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."[112] 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."[113] Mr. Mueller admitted that the F.B.I. was "way be-

---

105 *Id.*

106 *Id.*

107 *See* Hill Statement, *supra* note 24, at 21.

108 *See id.*

109 *See* Patrick E. Tyler, *Feeling Secure, U.S. Failed to Grasp bin Laden Threat*, N.Y. TIMES, Sept. 7, 2002, *at* http://www.nytimes.com/2002/09/08/international/asia/08ATTA.html?tntemail0 (last visited Sept. 8, 2002).

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

---

[114] *See id. See also* James Risen & David Johnston, *F.B.I. Was Warned It Could Not Meet Terrorism Threat*, N.Y. TIMES, May 31, 2002, at A1.

[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).

[118] *See* HAGER, *supra* note 53. *See also* Duncan Campbell, *Inside ECHELON. The History, Structure and Function of the Global Surveillance System Known as ECHELON*, TELEPOLIS, July 25, 2000, *at* http://www.heise.de/tp/english/inhalt/te/6929/1.html; Parliament Report on ECHELON *supra* note 57; Martin Asser, *Echelon: Big Brother Without a Cause?, at* http://news.bbc.co.uk/2/hi/world/europe/820758.stm (last visited Aug. 9, 2002).

[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.[121]

The *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."[122] *Echelon* is comprised of approximately twenty interception stations throughout the world,[123] each "linked directly to the headquarters of the secretive [N.S.A.] headquarters at Fort Mead, Maryland,"[124] where intercepted data can be analyzed, retained and disseminated. The largest of the N.S.A.'s *Echelon* interception stations is located in Menwith Hill, England,[125] and in 1992, it is rumored that as many as 1,500 U.S. employees were stationed there.[126]

At the Menwith Hill interception station, the N.S.A. operates what have been described as "'giant golf balls,' called radomes,"[127] which communicate with satellites in geostationary orbit, to intercept e-mail, fax, and telephone communications from around the world.[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 Telecomm network."[129] Clearly, "[i]t is a [processing] station which affects people throughout the world."[130]

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

---

121 *See* Paul Meller, *European Parliament Adopts 'Echelon' Report*, *at* http://www.cnn.com/2001/tech/internet/09/07/echelon.report.idg/index.html (last visited Feb. 9, 2002). *See also* Parliament Report on ECHELON, *supra* note 57.

122 HAGER, *supra* note 53, at 29.

123 *See US to Close Echelon Spy Station*, *at* http://news.bbc.co.uk/2/hi/word/europe/1365156.stm (last visited Aug. 9, 2002).

124 Asser, *supra* note 118.

125 *See* HAGER, *supra* note 53, at ch. 2.

126 *See id.*

127 Asser, *supra* note 118.

128 *See id.*

129 Poole, *supra* note 53, at 8 ("Inside Menwith Hill") (*relying on* Duncan Campbell, *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)).

130 HAGER, *supra* note 53, at 40.

receiving facility."[131] 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.[132] 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 . . . ."[133]

### B. Echelon: *The Abuse of Power*

Not only do former intelligence service officers attest to the existence of *Echelon*,[134] but also to the abuse of its power.[135] 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."[136] "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."[137] Evidence received by the Temporary Committee suggested "intervention by the Advocacy Center to the benefit of U.S. firms,"[138] and that *Echelon* was being used unfairly to engage in industrial espionage by passing sensitive information on to U.S. firms via the CIA.[139]

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-

---

131 Parliament Report on ECHELON, *supra* note 57.

132 *See Bad Aibling Station to Close*, U.S. ARMY INTELLIGENCE AND SECURITY COMMAND, May 31, 3001, *available at* http://www.inscom.army.mil/bas_to_close.asp. *See also US to Defer Spy Station Closure,* WASH. POST, Oct. 25, 2001, *at* http://www.washingtonpost.com/wp-srv/aponline/20011025/aponline131445_000.htm; Tony Czuczka, *US to Shut Spy Base in Germany,* June 5, 2001, *at* http://www.cndyorks.gn.apc.org/yspace/articles/badaiblingtoclose2.htm.

133 *E-mail Users Warned Over Spy Network*, BBC NEWS, May 29, 2001, *at* http://news.bbc.co.uk/1/hi/world/europe/1357264.stm.

134 *See* Parliament Report on ECHELON, *supra* note 57, at 67.

135 *See* Thomas Catan, *Secrets and Spies*, FIN. TIMES (London), May 31, 2000, *at* http://www.fas.org/sgp/news/2000/05/ft053100.html.

136 Parliament Report on ECHELON, *supra* note 57, at 68.

137 Asser, *supra* note 118.

138 Parliament Report on ECHELON, *supra* note 57, at 68.

139 *See* Asser, *supra* note 118.

lite,"[140] and alleged that conversations of U.S. Senator Strom Thurmond had been intercepted.[141] 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.[142] 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.[143]

The testimony of a former Canadian Secret Service ("CSE") employee affirmed that *Echelon* monitored civilian communications.[144] 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."[145] 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,"[146] 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.[147] 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.[148] 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."[149] "If the current allegations are true, [however,] all abiding European citizens

---

140 Parliament Report on ECHELON, *supra* note 57, at 71.

141 *See id.*

142 *See id.*

143 *See id.*

144 *See* Parliament Report on ECHELON, *supra* note 57, at 72.

145 *Id.* at 71.

146 *Id.* at 72.

147 *See* James Woolsey, former CIA Director, Briefing at the Foreign Press Center (Mar. 7, 2000), *available at* http://cryptome.org/echelon-cia.htm. (last visited Oct. 12, 2002).

148 *See* Parliament Report on ECHELON, *supra* note 57, at 72.

149 *Id.*

and companies are at risk of being monitored every day without any legal basis."[150]

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

In the year following September 11, 2001, nations throughout the world have adopted comprehensive measures designed to prevent future terrorist attacks.[151] One such national measure, the USA Patriot Act ("USAPA"),[152] now provides the United States with the additional tools required for enhanced surveillance operations, government coordination, and informa-

---

[150] 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.

[151] *See generally* Press Release SC/7518, United Nations Security Council, Security Council Unanimously Adopts Wide-Ranging Anti-Terrorism Resolution; Calls For Suppressing Financing, Improving International Cooperation; Resolution 1373 also Creates Committee to Monitor Implementation (Sept. 28, 2001), http://www.un.org/News/Press/docs/2001/sc7158.doc.htm; Press Release Press 327 Nr: 12019/01, Brussels, Extraordinary Council Meeting - Justice, Home Affairs and Civil Protection (Sept. 20, 2001), http://ue.eu.int/Newsroom/LoadDoc.asp?MAX=1&BID=86&DID=68116&LANG=1; *EU Unites Region Against Terror,* CNN.COM, Oct. 21, 2001, *at* http://www.cnn.com/2001/WORLD/europe/10/20/gen.summit.eu/index.html; *UK Passes Anti-terror Law,* CNN.COM, Dec. 14, 2001, *at* http://www.cnn.com/2001/WORLD/europe/12/14/gen.britain.law/index.html; *UK MP's Vote For Anti-Terror Bill,* CNN.COM, Nov. 20, 2001, *at* http://www.cnn.com/2001/WORLD/europe/11/20/gen.britain.bill/index.html; The Regulation of Investigatory Powers (Interception of Communications: Code of Practice) (2002) SI 2002/1693 [hereinafter SI 2002/1693]; The Regulation of Investigatory Powers (Covert Surveillance: Code of Practice) (2002) SI 2002/1933 [hereinafter SI 2002/1933]; The Regulation of Investigatory Powers (Maintenance of Interception Capability: Code of Practice) (2002) SI 2002/1931 [hereinafter SI 2002/1931]; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USAPA]. *See also Bush Signs Antiterrorism Bill Into Law,* CNN.COM, Oct. 26, 2001, *at http://www.cnn.com/2001/US/10/26/rec.bush.antiterror.bill/index.html; President Bush, Remarks by the President at the Signing of the Patriot Act,* ONLINE NEWS HOUR, Oct. 26, 2001, http://www.pbs.org/newshour/bb/terrorism/bush_terrorismbill.html [hereinafter *Bush Remarks*]; *France Toughens Antiterror Laws,* CNN.COM, Nov. 1, 2001, *at* http://www.cnn.com/2001/WORLD/europe/11/01/inv.france.measures/index.html; Anthony DePalma, *A Nation Challenged: Security Concerns, Canada Altering Its System of Vigilance Against Terror,* N.Y. TIMES, Dec. 3, 2001, at B4; *Passwords Access for Police,* THE NEW ZEALAND HERALD, Mar. 19, 2002, http://www.nzherald.co.nz/storydisplay.cfm?storyID=1240906; *Colombia Authorizes Warrantless Arrests, Citing Terror Fight,* N.Y. TIMES, Sept. 12, 2002, at A7.

[152] *See* USAPA, *supra* note 151.

tion-sharing.[153] 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.[154]

In the wake of September 11, 2001, the European Union ("EU") has also approved tough new measures to prevent future terrorist attacks.[155] 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."[156] 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.[157]

Since September 11, 2001, at least forty countries have adopted a declaration expressing their "wholehearted support" for sharing intelligence on terrorist activity,[158] 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

---

153 *See* OFFICE OF HOMELAND SECURITY, *supra* note 22, at 47; Frank Thorsberg, *PC World Poll Highlights Privacy Concerns*, CNN.COM, Oct. 8, 2001, *at* http://www.cnn.com/2001/TECH/industry/10/08/privacy.poll.idg/index.html; *Bush Signs Antiterrorism Bill into Law*, *supra* note 151; *Bush Remarks*, *supra* note 151.

154 *See Bush Remarks*, *supra* note 151.

155 *See* Commission Proposal for a Council Framework Decision on Combating Terrorism, 2001 O.J. (C 364); *Europe Agrees Anti-Terror Laws*, CNN.COM, Sept. 20, 2001, *at* http://www.cnn.com/2001/WORLD/europe/09/20/gen.eu.ministers/index.html.

156 *Europe Agrees Anti-Terror Laws*, *supra* note 155. *See also EU Governments Want the Retention of All Telecommunications Data for General Use by Law Enforcement Agencies Under Terrorism Plan*, STATEWATCH NEWS ONLINE, Sept. 2001, *at* http://www.statewatch.org/news/2001/sep/20authoritarian.htm; *Interception of Telecommunications in the EU*, STATEWATCH NEWS ONLINE, Nov. 2001, *at* http://www.statewatch.org/news/2001/oct/15intercept.htm.

157 *See Interception of Telecommunications in the EU*, *supra* note 156; Press Release: 175 Nr: 9620/02, Luxembourg, 2436th Council Meeting Justice, Internal Affairs, and Civil Protection (June 13, 2002), http://ue.eu.int/Newsroom/makeFrame.asp?MAX=1&BID=86&DID=71236&LANG=1&File=/pressData/en/jha/71236.pdf&Picture=0 [hereinafter Press Release: 175 Nr: 9620/02]. Established in 1992 and beginning operations in 1994, Europol is the European Union law enforcement organization that handles criminal intelligence between Member States. *See* The European Police Office - Fact Sheet, *at* http://www.europol.eu.int/content.htm?facts/en.htm.

158 *See* Press Release: 175 Nr: 9620/02, *supra* note 157.

are prepared to exchange intelligence data with other countries[159] and that the central problem involved balancing fundamental civil rights and freedoms with the increased need for international security measures.[160]

Prime Minster Blair declared that the U.K. stood "side by side with . . . [the U.S.] now, without hesitation,"[161] and vowed to take action at every single level to eradicate the threat posed by international terrorism.[162] 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.[163] Not surprisingly, there has been wide criticism of the U.K. plan that would give law enforcement officials sweeping access to personal data.[164] 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."[165]

Federal Chancellor Gerhard Schroeder also made assurances that Germany was prepared to "give its unreserved support to the United States of America"[166] 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.*

163 *See Data Surveillance Introduced in UK and USA*, STATEWATCH NEWS ONLINE, Sept. 2001, *at* http://www.statewatch.org/news/2001/sep/11retorder.htm; *UK Plans for the Retention of Data for 12 Months,* STATEWATCH NEWS ONLINE, Nov. 2001, *at* http://www.statewatch.org/news/2001/nov/17ukdata.htm; SI 2002/1693, *supra* note 151; SI 2002/1933 *supra* note 151; SI 2002/1931, *supra* note 151.

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.*

166 Federal Chancellor Gerhard Schroeder of Germany, Policy Statement Made to the German Bundestag (Sept. 19, 2001), http://eng.bundesregierung.de/dokumente/Rede/ix_56718.htm.

the German parliament . . . "[167] 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

---

[167] Elisabeth Zimmerman, *Second Package of Anti-terror Laws Rushed Through German Parliament*, WORLD SOCIALIST WEB SITE, Jan. 15, 2002, *at* http://www.wsws.org/articles/2002/jan2002/anti-j15.shtml. *See Cabinet Approves Draft Legislation Against Terrorism*, DIE BUNDESREGIERUNG, http://eng.bundesregierung.de/top/dokumente/Rede/ix_56718.htm?template=single&id=56718&script=1&ixepf=_56718 (last updated Aug. 11, 2001); *Second Anti-Terrorism Package Approved,* DIE BUNDESREGIERUNG, http://eng.bundesregierung.de/top/dokumente/Rede/ix_56718.htm?template=single&id=56718&script=1&ixepf=_56718 (last updated July 1, 2002).

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

[169] *Id.*

[170] Associated Press, *Ashcroft Praises German Anti-Terror Law*, CBSNEWS.COM, Dec. 14, 2001, *at* http://www.cbsnews.com/stories/2001/12/14/attack/main321361.shtml.

[171] *See* USAPA, *supra* note 151.

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

[173] *See EEF Analysis of the Provisions of the USA Patriot Act that Relate to Online Activities*, ELECTRIC FRONTIER FOUNDATION, Oct. 31, 2001, *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

[174] *See id.*

been greatly reduced."[175] 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."[176]

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."[177] 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,"[178] an enormous amount of personal data will be intercepted, analyzed, and archived.[179] 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."[180] The unrestricted interception of private communications by government authorities is only permitted in a 'police state.'[181] "In contrast, in the EU Member States, which are mature democracies,"[182] the necessity for government intelligence services to respect an individual's privacy is "unchallenged and is generally enshrined in national constitutions."[183] "Privacy thus enjoys special protection: potential violations are authorized only following analysis of the legal considerations and in accordance with the principle of proportionality."[184]

---

175 *Id.*

176 *Bush Signs Antiterrorism Bill into Law, supra* note 151.

177 Thorsberg, *supra* note 153.

178 *Id.*

179 *See id.*

180 Parliament Report on ECHELON, *supra* note 57, at 83.

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

---

185 *Citizens' Rights, Fundamental Rights,* EUROPA, *at* http://www.europa.eu.int/abc/cit1_en.htm (last visited Nov. 19, 2002).

186 *See* TREATY ON EUROPEAN UNION, Feb. 10, 1997, O.J. C 340/145 [hereinafter TEU].

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.

188 Parliament Report on ECHELON, *supra* note 57, at 81.

189 Akdeniz, *supra* note 150. *See* Parliament Report on ECHELON, *supra* note 57, at 81.

190 Parliament Report on ECHELON, *supra* note 57, at 80. *See* TREATY ESTABLISHING THE EUROPEAN COMMUNITY, O.J. C 340/173 [hereinafter EC TREATY], *incorporating changes made by* Treaty on European Union, Feb. 7, 1992, O.J. C 224/1.

191 *See* Parliament Report on ECHELON, *supra* note 57, at 80-81.

in good faith,[192] 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."[193] 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."[194]

When a EU Member State utilizes the *Echelon* interception system for national security purposes,[195] e.g., combating international terrorism, they "cannot therefore be in breach of the EC's data protection directives"[196] because Directives 95/46/EC[197] and 97/66/EC[198] 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.*

[193] Parliament Report on ECHELON, *supra* note 57, at 82.

[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 . . . ."[199] Similarly, the use of *Echelon* to process data intercepted from private communications cannot be in breach of Article 286 of the EC Treaty[200] or Regulation 45/2001[201] because neither is applicable to the processing of data concerning State security, defense, or public security.[202] 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,"[203] 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."[204]

European law enforcement agencies have recommended "the adoption of 'data retention' requirements"[205] that would require communications service providers to "archive information detailing the telephone calls, e-mail messages and other communications of their users."[206] 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/

---

Directive shall not apply to the activities which fall outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union, and in any access to activities 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. 1, 1998 O.J. (L024) 3.

[199] Parliament Report on ECHELON, supra note 57, at 80-81.

[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) *Id.*

[202] *See* Parliament Report on ECHELON, *supra* note 57, at 81.

[203] *Id.* at 82.

[204] *Id.*

[205] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), DATA RETENTION (Aug. 2002), *at* http://www.epic.org/privacy/intl/data_retention.html [hereinafter EPIC].

[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 national regulations for the retention of electronic data.[210] In the interim, however, Directive 2002/58/EC neither "alters the existing 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 security,"[211] nor precludes States from carrying out "the lawful interception of electronic communications."[212]

As a general proposition, the *Echelon* interception system "is not in breach of Union law because it does not concern the aspects of Union law that would be required for there to be incompatibility."[213] This applies, however, only where *Echelon* is utilized exclusively for national security purposes.[214] If, on the other hand, *Echelon* is utilized to collect competitive intelligence for "industrial espionage directed against foreign firms, this would constitute an infringement of EC law."[215]

### 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-

---

[207] *See* Council Directive 2002/58 of 31 July 2002 The Directive on Privacy and Electronic Communications 2002 O.J. (L 201) 4 [hereinafter Council Directive 2002/58/EC], *available at* http://www.dti.gov.uk/cii/regulatory/telecomms/telecommsregulations/comms_dpd.shtml#ov.

[208] *See id.*

[209] *See id.*

[210] *See* EPIC, *supra* note 205.

[211] Council Directive 2002/58, *supra* note 207, para. 11.

[212] *Id.*

[213] Parliament Report on ECHELON, *supra* note 57, at 82.

[214] *See id.*

[215] *Id.*

[216] Akdeniz, *supra* note 150. *See also* Parliament Report on ECHELON, *supra* note 57, at 83.

cle 17 of the U.N. International Covenant on Civil and Political Rights of December 16, 1966 (ratified by EU Member States),[217] guarantees the fundamental right to privacy.[218] 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."[219] 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."[220]

At the European level, the Charter of Fundamental Rights of the European Union[221] was drafted with the objective of instituting measures in Europe for the protection of fundamental rights.[222] In particular, Article 7 of the Charter expressly states that individuals have a fundamental right to respect for his or her private communications,[223] and Article 8 affirms that individuals have a fundamental right to the protection of their personal data.[224] Since the Charter has not yet been incorpo-

---

[217] *See* Committee Report on the Situation as Regards Fundamental Rights in the European Union, EUR. PARL. DOC. (A5-0223/2001) 45 (2001) [hereinafter Parliament Report on Fundamental Rights]. *See also* International Covenant on Civil and Political Rights Dec. 19, 1966, S. Exec. Doc. E, 95-2 (1978), 999 U.N.T.S. 171 [hereinafter ICCPR].

[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.*

[220] Parliament Report on ECHELON, *supra* note 57, at 84.

[221] *See* Charter of Fundamental Rights of the European Union, Dec. 7, 2000, O.J. C 364/1 (2000).

[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."[225]

> 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.'[226]

### 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),[227] is one of the greatest achievements of modern Europe.[228] Governed by the rules of international law,[229] the ECHR creates a uniform level of protection for the fundamental rights and freedoms guaranteed to all EU citizens.[230] 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 . . . ."[231] Today, the ECHR is the only effective European instrument that comprehensively protects individual privacy rights,[232] 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.*

225 Parliament Report on ECHELON, *supra* note 57, at 84.

226 *Id.*

227 *See generally* ECHR, *supra* note 187.

228 *See* R. BEDDARD, HUMAN RIGHTS AND EUROPE 1 (1993).

229 *See id.*

230 *See* Parliament Report on ECHELON, *supra* note 57, at 84.

231 Parliament Report on Fundamental Rights, *supra* note 217, at 45.

232 *See* Parliament Report on ECHELON, *supra* note 57, at 84.

lation of their rights under the Convention before the European Court of Human Rights ("the Court").[233]

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 . . . ."[234] The Court's jurisdiction extends "to all matters concerning the interpretation and application of the Convention,"[235] 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 . . . ."[236] 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."[237]

The fundamental rights enshrined in the ECHR are not linked to nationality,[238] but represent generally accepted rights guaranteed to all persons within the jurisdiction of the contracting parties.[239] "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."[240] 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.[241]

---

[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.

[238] *See* Parliament Report on ECHELON, *supra* note 57, at 85.

[239] *See id.*

[240] *Id.* (*citing* Loiziduo v. Turkey, App. No. 15318/89, 40 Eur. Ct. H.R. 435, 514 (1993)).

[241] Parliament Report on ECHELON, *supra* note 57, at 85.

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."[242] Although the plain language of the Convention contains no explicit reference to the protection of private telecommunications,[243] the Court makes clear that the covert interception of private telecommunications falls within the scope of Article 8.[244] 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."[245] "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."[246]

The essential object of Article 8 is to protect against arbitrary State interference with private communications.[247] 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.*'"[248]

---

[242] 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.*

[243] *See id.*

[244] *See* Parliament Report on ECHELON, *supra* note 57, at 85-86. *See also* Klass v. Federal Republic of Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214 (1978) (Court); Khan v. The United Kingdom, App. No. 35394/97, 31 Eur. H.R. Rep. 45 (2000).

[245] Parliament Report on ECHELON, *supra* note 57, at 85.

[246] *Id. See* Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 (1984).

[247] *See* Parliament Report on Fundamental Rights, *supra* note 217, at 47. *See also* Camp and Bourimi v. The Netherlands, App. No. 28369/95 (Oct. 2000), http://hudoc.echr.coe.int/hudoc/ViewRoot.asp?Item=0&Action=Html&X=1205020948&Notice=0&Noticemode=&RelatedMode=0.

[248] The Court has held that,

> [t]he 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

---

> him must also be foreseeable. However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields.

Leander v. Sweden, App. No. 9248/81, 9 Eur. H.R. Rep. 433, 450 (1987). The phrase *'in accordance with law'* also implies

> that there must be a measure of legal protection in domestic law against arbitrary interference by public authorities with the rights safeguarded in paragraph 1. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Undoubtedly . . . the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same as in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to put restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret and potentially dangerous interference with the right to respect for private life and correspondence.

Malone, 7 Eur. H.R. Rep at 40. *See* Klass, 2 Eur. H.R. at 232.

249 Parliament Report on Fundamental Rights, *supra* note 217, at 47.

250 *See* ECHR, *supra* note 187, art. 8(2).

251 Parliament Report on ECHELON, *supra* note 57, at 86.

252 *Id.* (emphasis added). In determining whether interference with private life is 'necessary in a democratic society,' the Court has summarized certain principles:

> (a) the adjective 'necessary' is not synonymous with 'indispensable,' neither has it the flexibility of such expressions as 'admissible,' 'ordinary,' 'useful,' 'reasonable' or 'desirable'; (b) the Contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposi-

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

---

> tion of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention; (c) the phrase 'necessary in a democratic society' means that, to be compatible with the Convention, the interference must, *inter alia,* correspond to a 'pressing social need' and be 'proportionate to the legitimate aim pursued'; (d) those paragraphs of Article of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted.

Silver v. United Kingdom, App. No. 38394/97, 5 Eur. H.R. Rep. 347, 376 (1983). *See also* Khan, 31 Eur. H.R. Rep. para. 26.

253 *See* Parliament Report on ECHELON, *supra* note 57, at 86.

254 *See id.* at 86.

255 *See id.*

256 Klass, 2 Eur. H.R. Rep. at 232.

257 Parliament Report on ECHELON, *supra* note 57, at 86. *See* Leander, 9 Eur. H.R. Rep. at 452.

258 Parliament Report on ECHELON, *supra* note 57, at 86. *See* Silver, 5 Eur. H.R. Rep. at 376.

259 Parliament Report on ECHELON, *supra* note 57, at 86-87 (emphasis added).

weighing of competing interests[260] and requires that adequate provisions be made for the stringent monitoring of covert surveillance activities.[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.[262]

The use of *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."[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,"[264] and in any given case, the need for the interference with private communications must be convincingly established.[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 . . . .[266]

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

---

[260] *See id. See also* Leander, 9 Eur. H.R. Rep. at 452.

[261] *See* Parliament Report on ECHELON, *supra* note 57, at 87. *See also* Klass, 2 Eur. H.R. Rep. at 232.

[262] Parliament Report on ECHELON, *supra* note 57, at 87. *See* Leander, 9 Eur. H.R. Rep. at 453.

[263] Akdeniz, *supra* note 150, at 3. *See* Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep. 14 (1985). *See also* Valenzuela Contreras v. Spain, App. No. 27671/95, 28 Eur. H.R. Rep 483 (1999).

[264] Klass, 2 Eur. H.R. Rep. at 230.

[265] *See* Akdeniz, *supra* note 150.

[266] *Id. See* Kruslin v. France, App. No. 11801/85, 12 Eur. H.R. Rep. 547 (1990). *See also* Huvig v. France, App. No. 11105/84, 12 Eur. H.R. Rep. 528 (1999); Halford v. United Kingdom, App. No. 20605/92, 24 Eur. H.R. Rep. 523 (1997); Valenzuela Contreras, 28 Eur. H.R. Rep. 483.

[267] *See* Leander, 9 Eur. H.R. Rep. 433.

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 Parlimentary Board and the G10

---

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

[269] Parliament Report on ECHELON, *supra* note 57, at 86.

[270] *See* FRANCIS G. JACOBS & ROBIN WHITE, THE EUROPEAN CONVENTION ON HUMAN RIGHTS 209 (1996).

[271] *See* Klass, 2 Eur. H.R. Rep. 214.

[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).

[276] *Id.* (*quoting* Klass, 2 Eur. H.R. Rep. at 232). *See* JACOBS & WHITE, *supra* note 270, at 207

[277] *See* JACOBS & WHITE, *supra* note 270, at 207.

Commission."[278] 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.[279]

In a subsequent English case,[280] law enforcement authorities were engaged in surveillance activity that involved the covert interception of telecommunications.[281] 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:

> [T]he 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.[282]

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.[283]

Two subsequent French cases revealed the Court had found some middle ground.[284] 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.[285] 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."[286] Since the French statutory frame-

---

[278] *Id.* (*quoting* Klass, 2 Eur. H.R. Rep. at 255).

[279] *See* JACOBS & WHITE, *supra* note 270, at 207-08.

[280] *See* Malone, 7 Eur. H.R. Rep. 14 (1984).

[281] *See* JACOBS & WHITE *supra* note 270, at 208.

[282] *Id.* (*quoting* Malone, 7 Eur. H.R. Rep. at 45).

[283] *See* JACOBS & WHITE *supra* note 270, at 208.

[284] *See id. See also* Hurig v. France, 4 Eur. Ct. H.R. 164, 220 (1990); Kruslin v. France, 7 Eur. Ct. H.R. 167, 223 (1990).

[285] *See* JACOBS & WHITE, *supra* note 270, at 208-09.

[286] *Id.*

work was seriously lacking in measures to prevent abuse,[287] the Court found violations of Article 8.[288] 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.[289]

### 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,[290] and services must not move to circumvent Article 8 of the Convention.[291] In particular, a Contracting Party must not be allowed to evade the requirements of law "by employing assistance from other intelligence services . . ."[292] whose "activities are subject to less stringent rules."[293] "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."[294]

One implication of this is that data exchanges "between intelligence services are permissible only on a restricted basis."[295] 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."[296] Moreover, "[t]he geographical scope for action laid down by [national] law . . . may not be extended by means of agreements with other [intelligence] services,"[297] 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.

[290] *See* Parliament Report on ECHELON, *supra* note 57, at 87.

[291] *See id.*

[292] *Id.*

[293] *Id.*

[294] *Id.*

[295] *Id.* at 88.

[296] Parliament Report on ECHELON, *supra* note 57, at 88.

[297] *Id.*

that the operations are consistent with the national law of its own country."[298] Even though intercepted data may be "intended 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."[299] 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."[300]

"By ratifying the ECHR, the Contracting Parties undertook to subject the exercise of their sovereignty to a review of its consistency with fundamental rights."[301] The Contracting Parties "cannot seek to circumvent this requirement by foregoing the exercise of that sovereignty,"[302] 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."[303] 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 sovereignty. 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."[304]

If, for example, the U.S. were utilizing their *Echelon* satellite receiving stations at Menwith Hill, U.K., and Bad Aibling, Germany "to engage in the interception of non-military communications . . . [by] private individuals or firms from an ECHR [C]ontracting [P]arty, supervisory requirements would come into play under the ECHR. In practical terms, ECHR [C]ontracting [P]arties, Germany and the United Kingdom, are required to establish that the activities of the American intelligence services do not represent a violation of fundamental

---

298 *Id.*

299 *Id.*

300 *Id.* (*citing* Dimitri Yernault, *ECHELON and Europe, The Protection of Privacy Against Communications Espionage*, J. OF THE CTS., EUR. L., at 187 (2000)).

301 Parliament Report on ECHELON, *supra* note 57, at 88.

302 *Id.*

303 *Id.*

304 *Id.*

rights."[305] 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"[306] with the Convention. This assumption usually "applies until evidence emerges that an ECHR [C]ontracting [P]arty is violating the Convention on a systematic, long-term basis."[307] Since the U.S. is not "an ECHR [C]ontracting [P]arty and it has not made its intelligence operations subject to a similar supervisory system,"[308] no such assumption applies.[309]

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"[310] and not made available to the public.[311] 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,"[312] 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.[313]

> 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.

307 Parliament Report on ECHELON, *supra* note 57, at 89.

308 *Id.*

309 *See id.*

310 *Id.*

311 *See id.*

312 *Id.*

313 *See* Steve Kettmann, *U.S. Echelon Snub Angers Europe*, WIRED NEWS, May 18 2001, *at* http://www.wired.com/news/privacy/0,1848,43921,00.html. For more information regarding the European Echelon probe, see generally Declan McCullah, *Euros Continue Echelon Probe,* WIRED NEWS, Apr. 24, 2001, *at* http://www.wired.com/news/privacy/0,1848,43270,00.html; Press Statement, Carlos Coelho, Chairman of the European Parliament Temporary Committee on the Echelon Interception System (May 10, 2001), *at* http://www.eurunion.org/news/press/2001/echelonstatement.htm.

> ECHR seriously and to make authorization of further intelligence activities by N.S.A. on their territory contingent on compliance with ECHR.[314]

### 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."[315] 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."[316] 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."[317]

Second, U.S. interference "must be proportional, and . . . the least invasive methods must be chosen."[318] 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,"[319] especially when surveillance activity is being carried out for law enforcement purposes.[320] Although the U.S. has "repeatedly tried to justify the interception of telecommunications by accusing the European authorities of corruption and taking bribes,"[321] 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-

---

314 Parliament Report on ECHELON, *supra* note 57, at 89.

315 *Id.*

316 *Id.*

317 *Id.*

318 *Id.*

319 *Id.* at 90.

320 *See* Parliament Report on ECHELON, *supra* note 57, at 90.

321 *Id.* (*citing* James Woolsey, *Why We Spy on Our Allies,* WALL ST. J., Mar. 17, 2000, at A14).

> 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.[322]

Lastly, "[ECHR] has stipulated that compliance with fundamental rights is contingent on the existence of adequate monitoring systems and guarantees against abuse."[323] The N.S.A.'s utilization of the *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."[324]

## VI. ANALYSIS

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

---

322 *Id.*
323 *Id.*
324 *Id.*
325 *See* Niall McKay, *Did EU Scuttle Echelon Debate?*, WIRED NEWS, July 19, 2002, *at* http://wired.com.news/politics/0,1283,15429,00.html.
326 *Id.*
327 *Id.*
328 *Id.*
329 *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.