CHAPTER TWO
PERSONAL PRIVACY

INTRODUCTION

The past two years have seen growing bipartisan concern that Fourth Amendment safeguards against arbitrary governmental intrusion are being eroded in the name of national security. The law regulating the executive branch's authority to pry into Americans' private lives has changed dramatically since September 11. Attorney General John Ashcroft lifted restrictions that had limited FBI monitoring of domestic religious, civic, or political organizations. The PATRIOT Act lowered the standards for clandestine searches, electronic eavesdropping, and secret access to customer records and personal information. The executive has initiated a range of data-mining projects designed to search through vast amounts of personal information, looking for patterns of suspicious behavior. These changes have raised fears that bedrock principles of individualized suspicion and presumptive innocence have been replaced with a new normal of generalized suspicion and surveillance.

In the face of these initiatives, citizens, city councilors, librarians, and legislators from across the political spectrum have begun to challenge the expansion of federal surveillance powers. Bipartisan opposition put an end to the proposed neighbor-to-neighbor spying program Operation TIPS. Three states, as well as 162 towns, counties, and cities have passed resolutions affirming their commitment to civil liberties in the face of encroachments by the PATRIOT Act.[99] Librarians and booksellers have joined a bipartisan group of congressional representatives to press for legislation protecting library and bookstore records from governmental surveillance without judicial supervision. Congress has continued to assert its oversight authority in demanding additional explanation about the scope of the Terrorist (formerly Total) Information Awareness program. The U.S. House of Representatives also voted to roll back authorization for so-called "sneak and peek" warrants that allowed law enforcement to covertly search through private property and then further delay notification of the search.

The recent congressional engagement is encouraging. But more needs to be done to ensure that the tools entrusted to the executive to secure the nation from terrorist attack are consistent with Americans' expectations of privacy. The need for ongoing, stringent oversight of the executive's sweeping new information-gathering powers is starkly highlighted by the General Accounting Office's (GAO) June 2003 conclusion that, even without additional databases for tracking airline passengers and identifying patterns of terrorist activity, "the government cannot adequately assure the public that all legislated individual privacy rights are being protected."[100]

LEGAL BACKGROUND

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*.[101]
>
> **Fourth Amendment**, U.S. Constitution

The Fourth Amendment protects our "persons, houses, papers, and effects" from arbitrary governmental intrusion by requiring authorities to demonstrate that a search is reasonable and based on probable cause to suspect criminal activity. As the U.S. Supreme Court has explained, Fourth Amendment limitations on the executive branch's search and seizure powers are designed to "prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals."[102] It protects what is in essence, our "right to be let alone," a right which U.S. Supreme Court Justice Louis Brandeis termed "the most comprehensive of rights, and the right most valued by civilized men."[103] The right to be let alone also protects the exercise of other fundamental rights, such as the freedom of speech and freedom of religion, which may be chilled by governmental monitoring.

The right to privacy is also protected by international law. Article 17 of the International Covenant on Civil and Political Rights (ICCPR), to which the United States is a party, protects privacy rights in similar terms. Just as the right to free speech is protected by the First Amendment, freedom of expression is protected by Article 19 of the ICCPR. And Article 12 of the Universal Declaration of Human Rights provides that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[104]

THE PATRIOT ACT

In post-PATRIOT America, the FBI no longer needs individualized evidence to suspect that a person is connected to terrorism in order to trawl through a person's reading material, rental car records, school grades, and favorite internet sites, looking for signs of suspicious activity. The PATRIOT Act also allows law enforcement officials to direct the use of highly intrusive surveillance techniques, traditionally available exclusively for foreign intelligence gathering, for investigations that are primarily criminal in nature. This means that federal agents who lack probable cause to get a criminal wiretap may obtain the information they want simply by indicating the case has a purpose connected to foreign intelligence.

Access to Personal Records

> *I think the Patriot Act was not really thought out . . . in our desire for security and our enthusiasm for pursuing supposed[] terrorists, . . we might be on the verge of giving up the freedoms which we're trying to protect . . . I don't think it's anybody's business what I'm reading in the library.*[105]
>
> **Representative Don Young (R-AK)**

Sections 215 and 505 of the PATRIOT Act allow the FBI secretly to access information about U.S. persons (U.S. citizens and legal permanent residents), including library, medical, education, internet, television, and financial records, *without demonstrating any suspicion that the target is involved in espionage or terrorism*.[106] Prior to the PATRIOT Act, the personal records of U.S. persons could only be accessed by the FBI if there were "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[107] The PATRIOT Act dropped this requirement of individualized suspicion.[108]

Moreover, section 215 requests are considered only by the secret Foreign Intelligence Surveillance Court (FISC), which hears the government's requests *ex parte* – in the absence of the target of the search and the target's counsel. Prior to the PATRIOT Act, the FISC could issue orders only for the records held by a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility.[109] Bookstore, library, education, and medical records were not available through secret processes; any request for their production could be challenged in open court. The PATRIOT Act, however, expands the FISC's reach to requests for "any tangible things (including books, records, papers, documents, and other items)," held by any business.[110]

THE FOREIGN INTELLIGENCE SURVEILLANCE COURT

The FISC was established as part of the 1978 Foreign Intelligence Surveillance Act. The court was originally composed of seven federal judges, but the number was increased to eleven under the PATRIOT Act. The Chief Justice of the U.S. Supreme Court appoints judges to the FISC for staggered terms. Because the judges review the FBI's surveillance applications *ex parte*, only the government can appeal the FISC's decision to modify or deny an application. Appeals are heard by the Foreign Intelligence Court of Review, a secret court composed of three semi-retired federal judges.

Section 505 requests are not subject to any judicial oversight. These "National Security Letters" (NSLs) authorize the FBI to order a telephone company or internet service provider to disclose the target's name, address, length of service, and local and long distance billing records. The FBI may also use NSLs to obtain financial records and information held by consumer credit reporting agencies (data highly prone to error).[111] With no judicial oversight, service providers are compelled to produce these records solely on the basis of a written declaration by the FBI director or his designee that the information is sought for an investigation "to protect against international terrorism or clandestine intelligence activities."[112] Once again, the FBI need no longer demonstrate suspicion that the individual targeted is involved in terrorism. Finally, both section 215 and section 505 orders impose a gag on the provider of the records, making it a crime to reveal that the FBI has seized or searched customer information. Thus, a librarian who speaks out about being forced to reveal a patron's book selections can be subject to prosecution.[113]

Because of the secrecy surrounding these surveillance operations, little is known about how many U.S. persons have been subject to such intrusions. To understand the scope of these new powers, House Judiciary Committee Chairman James Sensenbrenner (R-WI) inquired in July 2002 whether section 215 of the PATRIOT Act had been used to access library, bookstore, or newspaper records and, if so, how many times. The Justice Department refused to answer,

saying that such information is classified.[114] In the meantime, a Freedom of Information Act (FOIA) request by the ACLU on the implementation of the PATRIOT Act garnered 350 pages of heavily redacted material.[115] The FBI had issued enough NSLs to fill six blacked out pages.[116] (Foreign Intelligence Surveillance Act orders by the secret court, discussed below, filled another blacked-out page.[117])

Many have been outspoken about the potential these new surveillance measures have to chill freedom of expression and inquiry. As one librarian put it, section 215 of the PATRIOT Act "conflicts with our code of ethics" because it forces librarians to let the FBI "sweep up vast amounts of information about lots of people – without any indication that they've done anything wrong."[118] In June 2002, a coalition of librarians, booksellers, and others asked Congress to reinstate the pre-PATRIOT system of subpoenas subject to judicial review as the method of obtaining these records.[119] Many of these groups also support a bill sponsored by Representative Bernard Sanders (I-VT) called the Freedom to Read Protection Act (FRPA) (H.R. 1157). The bill aims to raise judicial and congressional oversight of section 215 activity, and it would exempt bookstores and libraries from the new catch-all orders requiring the production of tangible things.[120] Law enforcement officials would still be able to obtain these records, but would have to get a subpoena to do so, subject to normal judicial scrutiny.[121] FRPA now has a bipartisan group of 133 cosponsors in the House.[122]

Electronic Surveillance

The Foreign Intelligence Surveillance Act (FISA)[123] was passed in 1978 in an effort to constrain federal wiretapping authority following revelations of widespread abuse in the 1970s.[124] Rather than allowing the executive unfettered discretion to conduct such searches, FISA authorized counterintelligence agents to wiretap U.S. persons under specific circumstances for the sole purpose of pursuing foreign intelligence information. Subject to fewer restrictions than wiretap searches aimed at criminal targets, FISA orders allowed targets to be: surveilled for 90 days (or up to a year if the target is a "foreign power");[125] kept in the dark about the surveillance unless and until the FBI initiates a prosecution;[126] and deprived of the ability to see or challenge government affidavits against them whenever the attorney general maintained that disclosure would prejudice national security.[127] Most significant, whereas law enforcement officers conducting a criminal investigation had to convince a court that there was probable cause to suspect specific criminal activity to obtain a criminal wiretap warrant,[128] intelligence officials seeking a FISA order only needed to show the FISC that there was probable cause to believe that the target is a foreign power or an agent of a foreign power,[129] and (if a U.S. person) was conducting activities which "involve" or "may involve" a violation of U.S. criminal law.[130] Accordingly, FISA orders were available *only* for "the purpose of" gathering foreign intelligence information.[131]

THE ORIGINS OF FISA: THE 1976 CHURCH COMMITTEE REPORT

FISA was one of the reform measures adopted in response to a 1976 report by the U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the Church Committee).[132] The report revealed that on the premise of "national security," U.S. intelligence agencies had been carrying out illegal surveillance of domestic organizations, collecting "vast amounts of information about the intimate details of citizens' lives and about their participation in legal and peaceful political activities."[133] Although the targets of this surveillance were primarily anti-war protesters and civil rights activists (including Dr. Martin Luther King, Jr.), they spanned a broad spectrum of groups, including the Women's Liberation Movement, the John Birch Society, and the American Christian Action Council.[134]

The Church Committee determined that such abuses were an inevitable outgrowth of the executive branch's "excessive" power over intelligence activities, which, until then, had been largely exempted from the normal system of checks and balances.[135] This problem had its roots in the mid-1930s, when President Franklin D. Roosevelt unilaterally authorized the FBI and other intelligence agencies to conduct domestic counterintelligence operations – a practice that grew substantially during the Cold War and during the civil unrest of the 1960s and 1970s. In the latter period, secret surveillance techniques that had been used against suspected Communist agents began to be applied against a wide range of domestic groups advocating for peaceful societal change – groups with no suspected connection to a foreign power.[136] The Church Committee warned that the "system for controlling intelligence must be brought back within the constitutional scheme,"[137] emphasizing that "unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature."[138]

Because FISA made the standards for foreign intelligence wiretaps lower than those constitutionally required for ordinary domestic criminal investigations, courts and the Justice Department erected a filter (often mischaracterized as a "wall") between those conducting domestic law enforcement and foreign intelligence operations.[139] The filter did not prevent intelligence officials from sharing FISA wiretap information about imminent criminal activity. Indeed, prior to the PATRIOT Act, the FBI provided monthly briefings to law enforcement on all counterintelligence investigations in which there were "reasonable indications of significant federal crimes."[140] The filter simply required that raw FISA intercepts be screened so that only the information which might be relevant to criminal activity was passed on to prosecutors.[141] The Criminal Division of the Justice Department was explicitly permitted to "give guidance to the FBI aimed at preserving the option of criminal prosecution,"[142] but the filter ensured that the decision on when to share information obtained with counterintelligence methods resided with intelligence officials. Thus, law enforcement could not use the intelligence division to collect information for a criminal case which it would otherwise be barred from collecting due to insufficient evidence to support a search warrant within the criminal justice system.

Section 218 of the PATRIOT Act altered the 1978 FISA. Whereas the 1978 Act limited FISA surveillance to use in investigations "for *the* purpose of" gathering foreign intelligence,[143] section 218 expanded FISA surveillance to investigations in which the collection of foreign intelligence is merely a "significant purpose" of the surveillance.[144] Thus, as Attorney General

Ashcroft explained in guidelines implementing the new law, FISA can now "be used primarily for a law enforcement purpose, so long as a significant foreign intelligence purpose remains."[145] At the same time, the attorney general replaced existing Justice Department procedures prohibiting "the Criminal Division's directing or controlling the [FISA] investigation toward law enforcement objectives"[146] with new procedures encouraging criminal prosecutors to advise FBI intelligence officials concerning "the initiation, operation, continuation, or expansion of FISA searches and surveillance."[147] The filter no longer operates to prevent law enforcement officials from using FISA orders to avoid Fourth Amendment probable cause requirements.

REQUIREMENTS FOR CRIMINAL AND INTELLIGENCE ELECTRONIC SURVEILLANCE

TITLE III (CRIMINAL LAW)	FISA BEFORE PATRIOT	FISA AFTER PATRIOT
Warrant issued in ordinary federal court	Order issued by secret FISC	Order issued by secret FISC
Probable cause of specified crime	Probable cause that target is a "foreign power" or an "agent" thereof AND if U.S. person, involved in activities which "involve" or "may involve" a crime	Probable cause that target is a "foreign power" or an "agent" thereof AND if U.S. person, involved in activities which "involve" or "may involve" a crime
Available in criminal investigations	Available where collection of foreign intelligence is "the purpose" of the investigation	Available "primarily for a law enforcement purpose, so long as a significant foreign intelligence purpose remains"
Initiated and directed by law enforcement	Initiated and directed by intelligence. Law enforcement prohibited from "directing or controlling the [FISA] investigation toward law enforcement objectives"	Law enforcement may advise intelligence on "the initiation, operation, continuation, or expansion of FISA searches and surveillance"
Authorized for 30 days	Authorized for 1 year against foreign powers, 90 days against their agents	Authorized for 1 year against foreign powers, 90 days against their agents
Notice within 90 days of termination	No notice unless and until prosecution initiated; no right to see application	No notice unless and until prosecution initiated; no right to see application
Targets can pursue civil remedies for illegal wiretaps	Targets have no remedy against illegal wiretaps	Targets have no remedy against illegal wiretaps

Secret Courts Disagree On the Extent of FISA As Amended

> *If direction of counterintelligence cases involving the use of highly intrusive FISA surveillances and searches by criminal prosecutors is necessary to obtain and produce foreign intelligence information, it is yet to be explained to the Court.*[148]
>
> **Foreign Intelligence Surveillance Court (2002)**

In March 2002, the new procedures authorizing prosecutors to direct FISA investigations came before the FISC. Although in its 25-year history the FISC has reportedly approved without modification all but five government applications,[149] the court roundly rejected the attorney general's new interpretation of the amended FISA and took the unprecedented step of publishing its decision. The FISC determined that allowing criminal prosecutors to direct the use of FISA surveillances is "designed to… enhance criminal investigation and prosecution… instead of being consistent with the need… to obtain, produce, and disseminate foreign intelligence information."[150]

The executive appealed the decision to the Foreign Intelligence Surveillance Court of Review (Court of Review). Meeting for the first time in its 25-year history, the three-judge Court of Review overruled the FISC, holding that criminal prosecutors may direct FISA investigations. The only restriction on FISA powers imposed by the Court of Review is that the FISA process may not be used with the "sole objective of criminal prosecution."[151] This standard is satisfied "[s]o long as the government entertains a realistic option of dealing with the [suspected foreign agent] other than through criminal prosecution."[152]

Again, the secrecy surrounding FISA surveillance makes oversight difficult. Since the unprecedented release of the FISC and Court of Review opinions, the FISC rulings have remained secret, as before. And people monitored under FISA do not find out that the court has approved the investigations unless and until they are prosecuted. Nonetheless, there are some preliminary indications of the extent to which FISA has been used. The FISC itself has complained that executive branch agents, including the FBI Director, have repeatedly misled the court in order to circumvent the filter between criminal and intelligence operations.[153] The FISC recalled a litany of "misstatements and omissions of material facts" "in some 75 FISA applications related to major terrorist attacks directed against the United States."[154] Furthermore, government statistics show that between 2001 and 2002 the number of FISA orders increased by 31 percent while the number of ordinary criminal surveillance warrants dipped by 9 percent.[155] The number of FISA orders issued in 2002 is 21 percent greater than the largest number in the previous decade, and FISA orders now account for just over half of all federal wiretapping conducted.[156] The Justice Department has admitted that other provisions of the PATRIOT Act have been applied beyond the intended counterterrorism scope of the Act. For example, Sections 216, 220 and 319 have been exploited to track not only terrorist conspirators, but also "at least one major drug distributor… thieves who obtained victims' bank account information and stole the money… a fugitive who fled on the eve of trial… a hacker who stole a company's trade secrets… [and] a lawyer [who] had defrauded his clients."[157]

In addition, the number of "emergency" FISA orders issued has exploded in the past year. Under current law, so-called "emergency" surveillance may be conducted on the authorization of the attorney general for 72 hours before it must be reviewed and approved by the FISC.[158] This emergency procedure does not require the executive to establish probable cause or seek any prior judicial approval.[159] According to FBI Director Robert Mueller, the FBI has "made full and very productive use of the emergency FISA process," "including 170 emergency FISAs" which is more than triple the total number employed in the prior 23-year history of the FISA statute. [160]

Proposals for Further Expanding FISA

In February 2003, the non-partisan government watchdog, the Center for Public Integrity, leaked a copy of proposed legislation drafted in secret by the Justice Department. The secret proposals were entitled the Domestic Security Enhancement Act of 2003, dubbed PATRIOT II after the leak.[161] The draft act aimed to abolish three key protections from surveillance for U.S. persons by: (1) allowing foreign intelligence surveillance of individuals with no known links to any foreign government or to any group engaged in international terrorism, but suspected of plotting international terrorism individually;[162] (2) dropping the requirement that surveillance of a U.S. person may only be conducted if the individual is engaging in activities that "involve" or "may involve" some violation of law;[163] and (3) allowing the attorney general to authorize the imposition of wiretaps for up to 15 days without judicial review in the event of a congressional authorization of military force or an attack on the United States "creating a national emergency" (under current law, the attorney general has this 15-day power only after a congressional declaration of war).[164]

The public outcry following the leak of PATRIOT II appears to have dampened White House support for the bill as a comprehensive package of proposals.[165] The Justice Department, however, has not stopped pushing for more powers. A new vehicle for this expansion has been circulating among members of the Senate Judiciary Committee and is expected to be introduced in the fall of 2003.[166] The draft bill, the Vital Interdiction of Criminal Terrorist Organizations (VICTORY) Act,[167] contains provisions similar to PATRIOT II, allowing the attorney general to issue administrative subpoenas (which do not require judicial approval) in the course of domestic as well as international terrorism investigations.[168] These administrative subpoenas are issued at the discretion of the attorney general and require the production of "any records or other things relevant to the investigation," including those held by providers of electronic communication services.[169] Such subpoenas are subject to fewer restrictions and less oversight than even NSLs, discussed above. NSLs may not be issued solely on the basis of First Amendment activities.[170] The FBI may disseminate information gained from an NSL only where it is clearly relevant to the statutory authority of the receiving agency.[171] And all NSL requests must be reported on a semi-annual basis to various Senate and House committees.[172] None of these restrictions applies to administrative subpoenas.[173] As discussed in Chapter 1, President Bush publicly requested that the Justice Department be given this new subpoena power in a speech at the FBI Academy on September 10, 2003. In addition, the VICTORY Act proposes to further insulate law enforcement from accountability for abuse of electronic surveillance, by prohibiting courts from suppressing evidence derived from a wiretap absent proof that law enforcement acted in "bad faith."[174]

REQUIREMENTS FOR ACCESSING PERSONAL RECORDS

PATRIOT § 215	**PATRIOT § 505 (NSLS)**	**DRAFT VICTORY ACT § 503 (Administrative Subpoenas)**
Issued by FISC after *ex parte* hearing	No judicial oversight; written declaration of FBI director or designee	No judicial oversight; written declaration of attorney general
Apply to "any tangible things" held by any business	Apply to telephone, internet, financial institution and credit reporting records	Apply to "any records or other things relevant to the investigation"
May not issue solely on the basis of First Amendment activities	May not issue solely on the basis of First Amendment activities	No protection for First Amendment activities
No restrictions on dissemination to other governmental agencies	Information gathered may be disseminated only where it is clearly relevant to the statutory authority of the receiving agency	No restrictions on dissemination to other governmental agencies
Semi-annual report on requests to House and Senate committees on the judiciary	Semi-annual report on requests to various House and Senate committees	No reporting requirement

KEEPING TABS ON DOMESTIC ACTIVITIES

> *I get very, very queasy when federal law enforcement is effectively . . . going back to the bad old days when the FBI was spying on people like Martin Luther King.*[175]
>
> **Representative F. James Sensenbrenner, Jr. (R-WI)**

In May 2002, Attorney General Ashcroft unilaterally overturned regulations preventing FBI agents from monitoring domestic religious, political, and civic organizations without some suspicion of wrong-doing.[176] These protections had been adopted in 1976, in the wake of the Senate Church Committee's findings on the abuses of the FBI and other intelligence agencies engaged in domestic spying. Under the attorney general's new guidelines, FBI agents may attend public events such as political rallies and religious services, surf the internet, and mine commercial databases as part of a broad mission to prevent or detect terrorism. The Justice Department Inspector General has announced that he will be reviewing the implementation of the new guidelines,[177] but no information is available yet. In the meantime, domestic intelligence operations continue with little guidance as to how FBI agents decide when they are appropriate, and no mechanism for accountability or redress.

Airline Watchlists

The Transportation Security Administration (TSA) was created by the Aviation and Transportation Security Act of 2001,[178] and charged with overseeing the security of all modes of transportation. The TSA's current system for preventing terrorist access to airplanes relies on airline watchlists compiled from a variety of government sources. At least two types of watchlist are maintained: a "no-fly" list of terrorist suspects, and a "selectee" list targeting people who must be subjected to rigorous screening before they are allowed to fly.[179] The TSA has refused to supply details of who is on the lists and why. However, according to TSA documents obtained through a FOIA suit filed by the ACLU, the list of targeted people has been growing daily in response to requests from the intelligence community, DHS, and other agencies.[180]

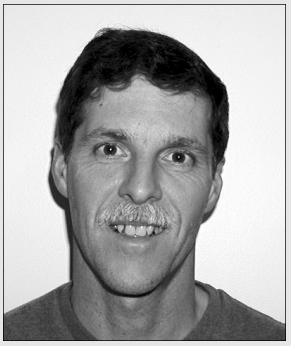
To comply with the Aviation and Transportation Security Act,[181] TSA also continues to develop a new passenger screening system called the Computer Assisted Passenger Pre-Screening System II (CAPPS II).[182] CAPPS II will eventually replace the current program (CAPPS I), while retaining the same primary mission of "ensur[ing] passenger and aviation security." TSA initially indicated that CAPPS II would be used only to identify individuals (including U.S. citizens) with potential ties to international terrorist organizations. In an Interim Privacy Notice issued on July 22, 2003, however, TSA made clear that CAPPS II's reach would be expanded to identify: (1) individuals with possible ties to domestic terrorism; (2) individuals with outstanding federal or state arrest warrants for violent crimes; and potentially (3) visa and immigration law violators.[183]

THE STORY OF SISTER VIRGINE LAWINGER

"On April 19, 2002, I was supposed to fly from Milwaukee to D.C. for a weekend of peace-activism opposing military aid to Columbia and the infamous School of the Americas, a U.S. training camp for foreign militias in Ft. Benning, Georgia. Twenty of my group of 37 were refused boarding passes, questioned, and delayed for so long that we missed the plane. We were finally allowed to fly the next day, but we missed an entire day of our activities. Many of the group were high school and college students getting their first experience of participation in the democratic process. Instead they learned how easily the civil rights they take for granted can be usurped. I wanted to know why 20 peace activists including nuns and high-school students would be flagged as potential threats to airline security, so I started what turned out to be a really long process of getting information from the government via the Freedom of Information Act (FOIA). After months of dialogue with many different agencies, the TSA acknowledged that a file existed, but refused to release it on the grounds that it had been exempted from FOIA. The ACLU appealed this decision and finally got hold of the document – with all the pertinent information blacked out. After all this time and effort, I still can't find out why I was flagged or whether and how I ended up on a terrorist watch-list."

Sister Virgine Lawinger, Dominican nun (as told to the Lawyers Committee)

THE STORY OF RETIRED COAST GUARD OFFICER LARRY MUSARRA



"On July 31, 2002 my wife and I were taking our son by plane to attend a special needs school. Unfortunately, we weren't able to check in on the Instant Ticket Machine and when the supervisor couldn't fix the problem, they told us 'I'm sorry Mr. Musarra but you are on an FBI watch list.' I reminded them that I was a retired Coast Guard Officer, who had flown in and out of the Juneau Airport for seven years. We were finally allowed on the flight after extensive screening but no-one could explain why I would be on an FBI Watch List.

In the next year we made 10 round trip flights to visit our son and we endured the same problems every time: web check-in denied; e-ticket check-in denied; hour-long waits for boarding passes; special screening. The entire Juneau High School wrestling team was held up by extra screening on each of the seven occasions that they traveled with my middle son during that period. My eldest son nearly missed flights home from college on two occasions. It was very inconvenient to fly, our trips took longer to check in, and we lost the bonus miles Alaska Airlines was offering for web check-in.

When reporters started investigating my story the TSA blamed the airline, Alaska Airlines blamed TSA, and the FBI implied that maybe I was a terrorist. The TSA even told one reporter that her article was helping the other side! After rampant finger-pointing, a reporter from the *Wall Street Journal* finally got to the bottom of the story. Alaska Airlines was using an outdated name matching system that was developed decades ago for totally different purposes. I even received all my web check-in miles after another article that was printed in our local paper. The irony of the situation is that during this period, the TSA, which already employs a few of my fellow retired "Coasties," offered me a job!"

Larry Musarra (as told to the Lawyers Committee)

As envisaged, CAPPS II would assign a security risk rating to every air traveler based on information from commercial data providers (such as the "credit header" information – name, address, telephone – held by companies affiliated to credit agencies), as well as from government intelligence. CAPPS II is intended "to avoid the kind of miscommunication and improper identification that has, on occasion, occurred under the systems currently in use."[184] However, the new system will not only rely on the same intelligence information making up the watchlists, but will also be vulnerable to error introduced by reliance on commercial databases.[185]

The first public information on the proposed new system generated enormous public concern.[186] TSA subsequently reached out to privacy organizations, industry groups and others to discuss the system, and DHS Secretary Tom Ridge suspended development of CAPPS II pending assessment of its privacy implications by the newly appointed DHS Chief Privacy Officer, Nuala O'Connor Kelly.[187] Based in part on these recommendations, a revised public notice was published on August 1, 2003 (the Interim Notice).[188] As set forth therein, CAPPS II will first seek to verify identity by checking name, address, telephone number, and date of birth against the "credit header" information – name, address, telephone – held by companies affiliated with

credit agencies. Passenger details will be transmitted to the commercial entity, which will return an authentication score reflecting the accuracy of the match between the data it holds and the data sent by TSA. CAPPS II will then generate a "numerical risk score," setting the level of screening to which a passenger must be subjected. The score is calculated by checking the commercial identity information against "records obtained from other government agencies, including intelligence information, watch lists, and other data."

The Interim Notice states that "DHS is currently developing a robust review and appeals process, to include the DHS privacy office." Despite such promises, many remain concerned both about the high likelihood of error, and the inadequate mechanisms for challenging the system. For example, the algorithms used by credit reporting agencies to generate "credit header" information ignore minor differences that occur in identifiers, such as incorrect digits in a social security number, leading to the erroneous combination of information from different individuals into one file.[189] Further errors may be introduced by credit bureau reliance on information from public records that often lack unique identifiable information.[190] As the Electronic Privacy Information Center observed in Senate testimony, "[v]ictims of mixed files find it extremely difficult to correct this problem."[191]

The broad category of "domestic terrorist organizations" also raises fears that those involved in peaceful protest or other groups will continue to be identified as potential security risks.[192] And while the Interim Notice provides that "passengers can request a copy of most information contained about them in the system from the CAPPS II passenger advocate," it also states that passengers may access and contest only the data that *they provided* to the system. CAPPS II would remain exempt from existing legislation that requires agencies to provide individuals with access to government records and the opportunity to correct them.[193] Compared to the access mechanism that would otherwise be provided for by statute, the CAPPS II proposal offers no opportunity for judicial review of any TSA decision to deny access to particular records.[194] Furthermore, TSA has proposed that CAPPS II be exempted from a standard Privacy Act requirement that an agency maintain only such information about a person as is necessary to accomplish an authorized agency purpose.[195]

Terrorism Information Awareness

> *The most pressing threat to liberty is a compulsory database encompassing everyone... like the TIA that would permit real-time monitoring of our whereabouts, movements and transactions. This is a Big Brother scenario, one of constant surveillance or harassment of citizens unrelated to addressing terrorist threats. You can't opt out.*[196]
>
> **Clyde Wayne Crews,** Jr., Director of Technology Studies, Cato Institute

In 2002, the Defense Department announced the development of the Total Information Awareness project (TIA). As envisaged by the Defense Advanced Research Projects Agency (DARPA), TIA would deploy government software to search a broad range of domestic and foreign, public and private commercial databases, "searching for patterns that are related to predicted terrorist activities."[197] TIA was intended to enable the government to search personal data, including: religious and political contributions; driving records; high school transcripts;

book purchases; medical records; passport applications; car rentals; phone, e-mail, and internet search logs. These searches would not be confined to information regarding individuals with links to terrorist organizations, would not require prior judicial approval, and would not be subject to legal challenge by those whose data are searched.

The development of TIA began without public notice, a single congressional hearing, or a plan for oversight and accountability mechanisms. As the controversy surrounding TIA grew, information about the program started to disappear from the official TIA website.[198] Biographical information about the TIA development team appeared and then was removed from DARPA's Information Awareness Office website in November 2002; the TIA logo, a globe topped by an all-seeing eye on a pyramid with the slogan, "Knowledge is Power," was removed from the site; diagrams describing how TIA was to operate have been replaced by less detailed versions. In April 2003, DARPA renamed the project *Terrorism* Information Awareness, and in August the program's controversial director Admiral John Poindexter resigned from his position, after his promotion of a project for predicting terrorist attacks with an online futures market.[199] Although DARPA's original information to contractors stated that "the amounts of data that will need to be stored and accessed will be unprecedented, measured in petabytes,"[200] DARPA later told Congress that "the TIA program is not attempting to create or access a centralized database that will store information gathered from various publicly or privately held databases… TIA would leave the underlying data where it is."[201]

Members of Congress and non-governmental organizations from across the political spectrum expressed grave concerns about the privacy implications of the program,[202] and also its efficacy and cost. DARPA itself acknowledged that "TIA may raise significant and novel privacy and civil liberties policy issues."[203] The Association for Computing Machinery's U.S. Public Policy Committee (USACM), representing 70,000 information technology professionals, expressed "significant doubts" that TIA could achieve its stated goal of prevention. Instead, according to USACM, TIA "would provide new targets for exploitation and attack by malicious computer users, criminals, and terrorists," "increase the risk of identity theft," and provide new opportunities for "harassment or blackmail by individuals who have inappropriately obtained access to an individual's information."[204] DARPA's promise to "develop algorithms that prevent unauthorized access… and provide an immutable audit capability so investigators and analysts cannot misuse private data without being identified as the culprits,"[205] is unlikely to allay expert fears, since both prevention of unauthorized access and creation of audit trails are challenging research problems in themselves. Indeed, "it is unlikely that sufficiently robust databases of the required size and complexity, whether centralized or distributed, can be constructed, financed, and effectively employed in a secure environment, *even with significant research advances*."[206]

Intelligence officials have also expressed doubts about TIA's effectiveness. Maureen Baginski, FBI executive assistant director for intelligence, and Alan Wade, CIA chief information officer, described the project as "unbounded" and said that "[t]he scope may be too big."[207] USACM has said that even an optimistic estimate of likely "false positives… incorrectly

labeling someone as a potential terrorist" could result in "as many as 3 million citizens being wrongly identified each year."[208] The experience with errors in airline watchlists, detailed above, lends weight to USACM's fears. Nonetheless, DARPA has disclaimed responsibility for inaccuracies in the commercial databases on which TIA would rely. It said that "TIA… [is] simply a tool for more efficiently inquiring about data in the hands of others…. [C]oncerns… about the quality and accuracy of databases that are in private hands… would exist regardless of the method chosen to query these databases and, thus, do not present a concern specific to TIA."[209]

To its credit, Congress has taken public concern, expert warnings, and the deficiencies of DARPA's report seriously, and has begun to move to rein in TIA. On July 14, 2003, the Senate adopted a provision eliminating funding for TIA research and development, and requiring specific congressional authorization for the deployment, implementation, or interdepartmental transfer of any component of the TIA program.[210] The House also adopted a provision requiring congressional authorization for TIA activities affecting U.S. citizens, but it did not cut off funding.[211] The White House has announced its disapproval of these moves, "urg[ing] the Senate to remove the provision."[212] Despite the assertion of congressional oversight, TIA is still very much part of the executive's efforts.

Terrorist Threat Integration Center (TTIC)

Although Congress has taken steps to prevent deployment of TIA without congressional authorization, a new initiative with a much lower profile, the Terrorist Threat Integration Center (TTIC), has the potential to achieve the same invasions of privacy without transgressing those new legislative restrictions. The TTIC initiative was announced by the White House on January 28, 2003, and has been described as "a multi-agency joint venture that integrates and analyzes terrorist-threat related information, collected domestically or abroad, and disseminates information and analysis to appropriate recipients."[213] TTIC's mission is to "serve as the central hub to provide and receive [counterterrorism] information."[214] In order to achieve this goal, TTIC has the extraordinary power to task elements of all the federal intelligence and security agencies (including DHS, FBI, CIA, and the Defense Department) with the collection of information for analysis by TTIC.[215] As TTIC's director has stated:

> [A]nalysts assigned from the other TTIC partner organizations [Justice Department, FBI, DHS, Defense Department, State Department, and CIA] have exceptionally broad access to intelligence. Within TTIC, there is desktop access to all partner agency networks… result[ing] in unprecedented sharing of information… critical to… federal, state, local, and law enforcement entities.[216]

Thus far, the executive has provided few details about the type of information that TTIC will task, receive, and analyze. This worries privacy advocates such as Lee Tien of the Electronic Frontier Foundation, who fears that TTIC may be an attempt to "duck all those [TIA-related] questions and go ahead with programs that don't have any connection to Poindexter and get away from the swamp that TIA is in."[217] Indeed, TTIC Director John Brennan has expressed enthusiasm for the TIA program and confidence in its privacy protections.[218] According to Mr. Brennan, discussions are already underway between TTIC and DARPA about making parts of

the TIA program work for TTIC.[219] Tien's concerns are shared by David Sobel, general counsel of the Electronic Privacy Information Center, who observed that TTIC is "potentially a huge repository of information concerning American citizens…. There's nothing in what has been made publicly available that would contain a limitation on such collection."[220] TTIC will "[h]ave unfettered access to all intelligence information – from raw reports to finished analytic assessments – available to the U.S. government,"[221] and will "be able to reach back to its participating parent agencies' base resources as necessary to meet its extraordinary requirements."[222] This means that TTIC will "integrate information from the federal, state and local level as well as the private sector."[223]

TTIC raises further privacy concerns because it has been placed under the control of the Director of Central Intelligence (DCI).[224] The DCI serves as the head of CIA and of the aggregate U.S. intelligence services. Although TTIC is not part of CIA,[225] placing TTIC, and its ability to command collection of information by other agencies, under the control of the DCI may make available to CIA the "police, subpoena, or law enforcement powers or internal security functions" that are statutorily forbidden to it under the National Security Act.[226] Further, while TTIC is under the control of the DCI rather than DHS, its authority will not be subject to the crucial oversight provisions of the Homeland Security Act of 2002. The Homeland Security Act assigned the task of coordinating and analyzing terrorism-threat information to DHS,[227] which is subject to numerous statutory oversight procedures not applicable to TTIC. If TTIC were housed within DHS, TTIC's authority would be limited by DHS' statutory charter, and TTIC's power would be constrained by congressional budgetary control, as well as by DHS' civil rights and privacy officers.[228] As structured, TTIC is subject to no such restraints. TTIC, in short, seems to assume duties that Congress explicitly allotted to DHS, without adopting the oversight controls that Congress provided for DHS.

RECOMMENDATIONS

1. Congress should repeal section 215 of the PATRIOT Act to restore safeguards against abuse of the seizure of business records, including records from libraries, bookstores, and educational institutions, where the danger of chilling free expression is greatest. Congress should also amend section 505 of the PATRIOT Act to require the FBI to obtain judicial authorization before it may obtain information from telephone companies, internet service providers, or credit reporting agencies.

2. Congress should review changes to FBI guidelines that relax restrictions on surveillance of domestic religious and political organizations to ensure that there are adequate checks on executive authority in the domestic surveillance arena. The guidelines should be specifically amended to better protect against the use of counterterrorism surveillance tools for purely criminal investigations.

3. Congress should delay implementation of the Computer-Assisted Passenger Pre-Screening System II pending an independent expert assessment of the system's feasibility, potential impact on personal privacy, and mechanisms for error correction. Separately, Congress should immediately eliminate all funding for "Total [or Terrorism] Information Awareness" research and development.

4. The Terrorist Threat Integration Center should be housed within DHS where it may be subject to oversight by departmental and congressional officials – who can investigate possible abuses of civil rights and civil liberties.

5. Congress should establish a senior position responsible for civil rights and civil liberties matters within the DHS Office of the Inspector General. This position would report directly to the Inspector General, and be charged with coordinating and investigating civil rights and civil liberties matters in DHS.