March 2003

Biography of Timothy H. Edgar

Timothy H. Edgar is a legislative counsel in the Washington Nation Office of the American Civil Liberties Union, responsible for national security, terrorism and immigration.

Mr. Edgar, who hails from Albany, New York, graduated summa cum laude from Dartmouth College in 1994. A magna cum laude graduate of Harvard Law School, class of 1997, Mr. Edgar served as editor of the Harvard Law Review. He was a law clerk to Judge Sandra L. Lynch of the United States Court of Appeals for the First Circuit from 1997 to 1998. Following his clerkship, Mr. Edgar joined the Washington, DC law firm Shea & Gardner, where he worked principally on complex litigation and legislative reform proposals in the area of toxic torts.

Mr. Edgar joined the ACLU in May 2001. Following September 11, 2001, Mr. Edgar's work has focused on the government's response to those attacks and its impact on civil liberties. Mr. Edgar has written extensively on civil liberties issues for Congress and has testified before the United States Commission on Civil Rights. He appears on national and international television and radio to address civil liberties issues, and is often quoted in major newspapers. He is also a regular public speaker both inside and outside the beltway.

Mr. Edgar lives in Maryland with his wife, Dr. Koraly E. Perez-Edgar, a research psychologist at the University of Maryland. They have one son, born September 26, 2001.

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON NATIONAL OFFICE
Laura W. Murphy
Director

1333 H St., NW, 10th Fl., Washington, D.C. 20002

(202) 544-1681 Fax (202) 546-0738

American Civil Liberties Union

Testimony at a Hearing on

"Securing the Freedom of the Nation:
Collecting Intelligence Under the Law"

Before the

House Permanent Select Committee on Intelligence

Submitted by
Timothy Edgar
Legislative Counsel

April 9, 2003

American Civil Liberties Union
Testimony at a Hearing on
"Securing the Freedom of the Nation: Collecting Intelligence Under the Law"
Before the House Permanent Select Committee on Intelligence
Submitted by
Timothy Edgar
Legislative Counsel

April 9, 2003

Chairman Goss, Ranking Member Harman and Members of the Committee:

On behalf of the American Civil Liberties Union and nearly 400,000 members, I welcome this opportunity to present the ACLU's views at this timely hearing on how the intelligence community's efforts to improve the gathering and analysis of information can be undertaken while meeting the demands of the law and fundamental civil liberties.

The challenge to our intelligence community is the same as the challenge for the nation as a whole. Securing the nation's freedom depends not on making a choice between security and liberty, but in designing and implementing policies that allow the American people to be both safe *and* free.

Increased threats of terrorism after September 11, 2001, lightening-fast technological innovation, and the erosion of key privacy protections under the law threaten to alter the American way of life in fundamental ways. Terrorism threatens – and is calculated to threaten – not only our sense of safety, but also our freedom and way of life. Terrorists intend to frighten us into changing our basic laws and values and to take actions that are not in our long-term interests.

The role of this Committee in overseeing these issues is particularly critical because of the fundamental tension between intelligence gathering and civil liberties. Where government is focused on gathering intelligence information not connected to specific criminal activity, there is a substantial risk of chilling lawful dissent. The Federal Bureau of Investigation (FBI) project of conducting "voluntary interviews" with law-abiding Americans has involved questions like how often they worship at a particular mosque or whether they oppose the war in Iraq. Such inquiries plainly have a chilling effect on constitutional rights.[1]

Because the stakes are so high, both for America's safety and its freedom, I would like to begin by articulating what I hope are some basic civil liberties principles on which we can agree. I will then discuss how these principles can be applied to controversial policy changes as they affect the conduct of intelligence activities, data mining, and the sharing of intelligence information among foreign and domestic intelligence and law enforcement

[1] *See* Michael Moss & Jenny Nordberg, *Imams Urged to Be Alert for Suspicious Visitors*, N.Y. Times, April 6, 2003.

organizations. With respect to those that have already been enacted or implemented, I will propose some suggestions for limits and safeguards that should be adopted to protect civil liberties.

Finally, I will discuss the recommendations of the Joint Inquiry of the House and Senate Intelligence Committees into intelligence failures that may have contributed to the September 11, 2001 terrorist attacks. These largely human and organization-centered intelligence problems were identified by the Joint Inquiry on the basis of the intelligence community's real-world experience. Fixing these mostly mundane problems is far more likely improve national security – and will to do so at far less cost to our fundamental freedoms – than changing the laws governing government surveillance or deploying costly, untested "Big Brother" surveillance technologies.

Intelligence Gathering and Civil Liberties Principles

First, no liberty interest should be sacrificed to implement "feel-good" anti-terrorism policies that have not be shown to actually improve national security.

Too often, changes to surveillance laws and deployment of the latest technological security solutions have been undertaken without considering the empirical evidence of whether such policy changes will actually improve security.

For example, even after enactment of broad new intelligence-gathering powers in the USA PATRIOT Act of 2001,[2] the Department of Justice began almost immediately to press for new authority to obtain surveillance orders of lone individuals under the Foreign Intelligence Surveillance Act (FISA). When responding to questions by Senate Judiciary Committee members concerning why additional authorities were needed, the Administration had no answer based on real-world experience. As explained by Senators Leahy, Grassley and Specter in their interim report issued February 2003:

> "[W]hen asked to 'provide this Committee with information about specific cases that support your claim to need such broad new powers,' DOJ was silent in its response and named no specific cases showing such a need, nor did it say that it could provide such specificity even in a classified setting. In short, DOJ sought more power but was either unwilling or unable to provide an example as to why."[3]

As I will discuss further below, this emphasis on changing the legal standards that govern intelligence surveillance distracts attention from the real intelligence problems, which were identified in this report of Senate Judiciary Committee members, in the Joint Inquiry of this Committee and its Senate counterpart, and elsewhere. These problems are largely a result of bureaucratic breakdowns and failure to deploy existing authorities as a result of longstanding structural problems and a lack of human resources.

---

[2] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[3] FISA Oversight in the 107th Congress: FISA Implementation Failures, Interim Report by Senators Leahy, Grassley and Specter (February 2003), at p. 7.

Similarly, cities and towns across the United States have accelerated their deployment of video surveillance systems, red-light cameras, and facial recognition technology often without examining the decidedly mixed record of such costly systems. In many cases, the empirical evidence does not back up proponent's extravagant security claims, suggesting the money would be better spent on proven law enforcement techniques. For example, according to one study, after security cameras were installed in downtown Glasgow, Scotland "reductions were noted in certain categories but there was no evidence to suggest that the cameras had reduced crime overall in the city centre."[4] Similarly, police on the beat in Tampa, Florida suspended facial recognition technology because it simply does not work.[5]

There is a danger that unrestricted data surveillance, like video surveillance, will be embraced by political leaders eager to tout the latest security technology. The Markle Foundation Task Force, headed by Zoë Baird and James Barksdale, warns against heeding what it calls "[e]xtravagant claims . . . about the potential uses of data mining, matched by similarly extravagant notions of the vast private or public databases that should be opened to such journeys of exploration."[6] As I discuss below, the intelligence community, including the Federal Bureau of Investigation, has much more mundane needs. Dollars spent chasing experimental and unproven technologies can be spent more wisely on addressing the known weaknesses in government agencies.

One reason why data mining could ultimately prove to be a false security solution is the unreliability of much information in the computer data to be "mined." As the technologists say, "garbage in, garbage out." For example, the Consumer Federation of America and the National Credit Reporting Association found in a new study that 10 percent of credit reports contain errors in names or other identifying information, yet these faulty reports will be a source of data to be mined by the Transportation Security Administration in its "enhanced" Computer Assisted Passenger Profiling System (CAPPS II).[7]

Where a change to basic surveillance laws, or deployment of a privacy-invasive technology cannot be shown to improve security, there simply is no reason to institute the change. Where there is no proven security benefit, there is no reason to balance such a benefit against the known loss of privacy or other civil liberties that would result from deploying the technology.

---

[4] Jason Ditton, "The Effect of Closed Circuit Television Cameras on Recorded Crime Rates and Public Concern About Crime in Glasgow," The Scottish Office Central Research Unit Main Findings, No. 30 (1999), available at http://www.scotcrim.u-net.com/researchc2.htm

[5] Jay Stanley & Barry Steinhardt, "Drawing a Black: The Failure of Facial Recognition Technology in Tampa, Florida," An ACLU Special Report, Jan. 3, 2002, at http://archive.aclu.org/issues/privacy/drawing_blank.pdf

[6] Protecting America's Freedom in the Information Age: A Report of the Markle Foundation Task Force (October 2002), at 27.

[7] *See* Dana Hawkins, *Digging Through Data for Omens*, U.S. News & World Report, April 7, 2003, available at http://www.usnews.com/usnews/issue/030407/tech/7data.htm

Second, fundamental liberties must not be sacrificed to advancing technologies that make current legal protections obsolete; the Constitution protects "people, not places."

When the Bill of Rights was written, protecting personal privacy was largely an issue of protecting the integrity of physical property – and so the Fourth Amendment speaks of the people's right to security in their "persons, houses, papers, and effects . . . ." Today, our most intimate conversations, correspondence and records are apt to be recorded digitally, rather than contained in paper records secured in private homes and offices. Likewise, the most routine details of daily life – credit card purchases at a drug store or bookstore, passage through a toll booth or subway station, the television shows recorded by a digital video recorder – now leave electronic footprints scattered across a myriad of computer databases.

Traditionally, both the courts and Congress have been slow to react to the both the opportunities and challenges of new technology. For four decades, the Supreme Court failed to give legal protection to the content of telephone conversations against government wiretapping, engaging in legal hairsplitting about whether particular eavesdropping devices physically penetrated a "constitutionally protected area." It was not until the late 1960s that the Supreme Court finally entered the telephone age, ruling that a wiretap, just like a physical search, required a warrant procedure based on a court's prior finding of probable cause. As the Supreme Court explained, "the Fourth Amendment protects people, not places." *Katz* v. *United States*, 389 U.S. 347 (1967).

Today, the transformation of our society from one dependent on the primarily on the privacy of "persons, houses, papers, and effects" in the physical world is accelerating exponentially. As the result of this transformation, a host of previously anonymous behavior and private information can now be captured and linked to a specific person without any trespass into the person's home or office.

Our laws are struggling to catch up. So far, the courts have left largely immune from Fourth Amendment scrutiny a range of highly personal information – including financial records, medical records, and library and book records – on a theory that there is no reasonable expectation of privacy in information in the hands of third parties. *See, e.g., United States* v. *Miller*, 425 U.S. 435 (1976).

Congress has responded by enacting a patchwork of privacy laws that offer some protection to certain kinds of information, usually in response to controversy about government snooping in particularly sensitive records. For example, in response to an inquiry into Supreme Court nominee Robert Bork's videotape rental records, Congress enacted the Video Privacy Protection Act of 1988. One reason why so many Americans fear widespread data surveillance is the simple fact that "[i]n the United States there is no omnibus statute or constitutional provision that provides comprehensive legal protection for the privacy of personal information."[8]

[8] Gina Marie Stevens, Congressional Research Service Report for Congress, "Privacy: Total Information Awareness Programs and Related Information Access, Collection, and Protection Laws," at 4 (updated Feb. 6, 2003).

Today, we live a world in which a personal calendar or journal – once stored in paper form in a home, office, or briefcase – is now as likely to be stored on a personal digital assistant connected to a server owned by a third party. In such a world, the courts should reconsider the idea that information held by third parties lacks constitutional protection.

Third, there is no "national security" or "intelligence gathering" exception to the Constitution's fundamental guarantees of individual liberty; as with all governmental powers, these powers are properly subject to checks and balances.

While the government has both the power and the obligation under the Constitution to defend the nation and its security, these powers cannot be exercised in a manner that contravenes individual constitutional liberties. Among others, these include the First Amendment's guarantee of freedom of speech, religion, and association, and the Fourth Amendment's protection against unreasonable searches and seizures. In addition, as with all government powers, national security and intelligence gathering powers should be subject to checks and balances, including meaningful judicial review and probing oversight by the Congress.

In *United States* v. *United States District Court* (*"Keith"*), 407 U.S. 297 (1972), the Supreme Court decided that wiretapping was subject to the Fourth Amendment even if it was conducted for national security purposes. That case involved a domestic terrorist conspiracy to bomb the office of the Central Intelligence Agency in Ann Arbor, Michigan. Still, without dismissing the real national security threat posed by such illegal activity, the Supreme Court rejected Attorney General John Mitchell's claim of a clandestine domestic intelligence gathering power that would allow the Executive Branch to wiretap without court review or Congressional authorization.

Such an unchecked power, the Supreme Court observed, would inevitably pose dangers to lawful dissent:

> "Though the investigative duty of the executive may be stronger in such [national security] cases, so also is there greater jeopardy to constitutionally protected speech. . . . History abundantly documents the tendency of Government – however benevolent and benign its motives – to view with suspicion those who most fervently dispute its policies. . . . The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power." *Keith*, 407 U.S. at 313-314.

The Supreme Court's warnings were certainly prescient, as later revelations of John Mitchell's role in the unlawful monitoring of President Nixon's political opponents made clear. Congress responded to these and other similar abuses by passing the Foreign Intelligence Surveillance Act of 1978, setting forth a comprehensive framework for national security wiretapping that brought such surveillance under the rule of law.

Safeguards also must exist to protect First Amendment freedoms of speech, worship and association. When conducting counter-terrorism and counter-intelligence investigations, the Department of Justice operates under guidelines approved by the Attorney General. The purpose of investigative guidelines is to ensure that intrusive investigative techniques are used to monitor terrorists, spies, and foreign agents, not political or religious organizations engaged in lawful dissent. These guidelines recognize that such techniques, which are left largely unregulated by the Fourth Amendment, pose a risk to First Amendment freedom of association.

Unfortunately, these guidelines have recently been weakened with respect to domestic terrorism investigations, permitting greater surveillance of lawful groups rather than terrorism organizations. Major parts of guidelines for foreign intelligence and terrorism investigations remain classified, so it is impossible to judge whether they achieve their stated purposes.

The Supreme Court has recognized a "vital relationship between freedom to associate and privacy in one's associations." *NAACP* v. *State of Alabama*, 357 U.S. 449, 462 (1958). Where individuals participate in unpopular political or religious organizations, members of those organizations fear – often with good reason – "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility." *Id.* Routine, intrusive government investigations of lawful, but unpopular, political organizations would clearly pose a serious risk to the First Amendment because their members would fear that such information, if leaked, could be used against them.

It is no answer to these legitimate concerns that police officers who monitor political or religious meetings, compile dossiers on political activists, or infiltrate lawful protest organizations are complying with the Fourth Amendment and are doing no more than any member of the public could do on his or her own. When government acts, it has a special obligation to respect constitutional rights – which include the First as well as the Fourth Amendment – an obligation not imposed on private citizens.

Fourth, Congress should make the decision whether to implement changes that tread on civil liberties and, if so, what safeguards and limits to impose.

In a democratic society, accountable and representative institutions, not bureaucrats, should make the fundamental choices about what trade-offs are acceptable to improve national security. Unfortunately, on too many occasions, large-scale policy intelligence initiatives have been implemented without adequate national debate and without an opportunity for the people's representatives to decide whether such initiatives should go forward.

It should be the government's burden to establish, to the satisfaction of Congress, that intelligence gathering initiatives do not pose a threat to fundamental American values. In some cases, as with the Administration's "Operation TIPS" proposal to enlist millions of Americans, including workers with access to private homes, as amateur terrorism investigators, Congress will decide simply to forbid the policy from going forward at all

because it cannot be implemented consistently with fundamental American civil liberites.[9] In other cases, where Congress may determine that such policy changes can be instituted consistent with American notions of freedom and autonomy, protection of fundamental civil liberties must be considered as part of the design of the policy itself, not appended as an afterthought.

At the federal level, the best way to ensure that such consideration is given is to require prior Congressional authorization for new intelligence gathering activities and technologies that raise serious civil liberty concerns. The Pentagon's controversial "Total Information Awareness" program is a paradigm example. The Wyden Amendment, adopted as part of the 2003 Omnibus Appropriations Resolution, forbids the domestic deployment of the program without prior Congressional authorization. Such a requirement of prior authorization does not mean that all research or consideration of a policy will come to a halt. Rather, it simply means that there will be a public debate before such mass data surveillance is permitted inside the United States.

Applying Civil Liberties Principles to Selected Intelligence Policy Proposals

With these principles in mind, I turn now to explain the ACLU's concerns around specific policies concerning the conduct of intelligence and law enforcement activities under the USA PATRIOT Act, data mining and surveillance, and sharing of intelligence information among foreign and domestic intelligence and law enforcement organizations.

Intelligence and law enforcement activities under the USA PATRIOT Act.

The USA PATRIOT Act substantially altered a number of key legal authorities governing intelligence gathering within the United States, primarily by weakening judicial review and other checks and balances on government intelligence and law enforcement powers. Some of the more significant changes include provisions that allow:

(1) Secret access to sensitive personal records that previously were protected from disclosure in the absence of a grand jury subpoena (section 215);

(2) Use of intelligence surveillance powers, instead of criminal surveillance powers, even where the "primary purpose" of the surveillance is criminal prosecution rather than the gathering of intelligence (section 218);

(3) Use of "pen register" and "trap and trace" devices that capture detailed e-mail header and Internet URL information without an electronic surveillance order based on probable cause of criminal activity (sections 214, 216);

(4) Secret searches that allow the government to delay, potentially indefinitely, notice of the execution of a search warrant in any criminal case (section 213);

[9] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002), at § 880 (prohibiting "Operation TIPS").

(5) Domestic intelligence wiretaps and other intelligence gathering at the direction of the Director of Central Intelligence, in spite of the statutory prohibition that bars the Central Intelligence Agency from exercising "internal security functions"[10] (section 901); and

(6) Sharing of sensitive law enforcement information, such as grand jury information, with the intelligence community without the approval of a United States district judge (section 203).

These authorities were enacted without adequate Congressional consideration of their effectiveness or their impact on civil liberties. They did not respond to specific gaps in legal authority that had been identified by any independent inquiry as contributing to the September 11, 2001 attacks. Rather, they were approved by Congress in unusual haste in the highly charged weeks just after the attacks under pressure from the Administration. The law was passed without a single public hearing at which members could hear the pros and cons of making these changes. In the House, basic Committee prerogatives were ignored by the Congressional leadership; in the Senate, the bill went straight to the floor without Committee consideration. The truncated process alone should cast doubt on whether such changes comply with the basic civil liberties principles I outlined above.

Some of these new authorities (but not all) must be reauthorized by Congress or they will expire after December 31, 2005. Whether or not a given power is subject to the USA PATRIOT Act's sunset provision (section 224), Congress should take the opportunity to reconsider the Act as a whole, and, where appropriate, enact limits and safeguards to protect civil liberties.

To determine whether to reauthorize the authorities provided in the USA PATRIOT Act, Congress should apply the civil liberties principles outlined above. Congress should determine whether these authorities have contributed substantially to improving national security in specific cases, whether their use has infringed on fundamental civil liberties or otherwise been the subject of abuse, and whether additional safeguards, including meaningful judicial oversight or other limits can be incorporated to protect fundamental constitutional rights.

In order to aid its decision, Congress must undertake comprehensive oversight of the USA PATRIOT Act and other anti-terrorism powers in order to determine whether the specific powers the government has been granted have been effectively used to thwart terrorism. In addition, such oversight could allay fears that these powers have been abused or point to particular limitations that would allow the government to continue its legitimate anti-terrorism efforts while protecting the constitutional rights of the American people.

One area that certainly requires searching oversight by this Committee is a startling increase in "emergency wiretaps" under FISA. In testimony before the Senate Judiciary Committee, Attorney General Ashcroft said that the Department of Justice had obtained

[10] 50 U.S.C. § 403-3(d)(1).

170 such orders since the September 11, 2001 attacks – more than triple the number of such emergency orders that had been authorized in the prior two decades.[11] These orders were not the subject of any prior judicial process. Congress should review these orders to determine who was subject to such surveillance and ensure there was good cause for bypassing the FISA court.

While such oversight is ongoing, Congress should consider, even before the sunset expires, drafting some modest corrections to the USA PATRIOT Act that would, without repealing the Act as a whole, allay public fears of unchecked surveillance powers. These could include:

(1) **Meaningful judicial oversight for inquiries into sensitive, First Amendment-protected records.** Library users are concerned that broad inquiries into the reading habits of their patrons could chill legitimate inquiry and research into controversial subjects. Congress should enact legislation to prohibit the government from accessing such records without a specific law enforcement or intelligence target in mind.

(2) **Reasonable limits on secret searches.** The USA PATRIOT Act provision authorizes notice of the execution of a warrant to be delayed, potentially indefinitely. This power should be limited to terrorism cases, and notice should be given within some fixed period of time.

(3) **Criminal discovery rights for FISA wiretaps in criminal cases.** While intelligence wiretaps could be used in criminal cases before passage of the USA PATRIOT Act, such use is likely to become more common because of the USA PATRIOT Act changes. In cases involving ordinary criminal wiretaps, the accused gets access to the wiretap application and much of the surveillance information. In cases involving intelligence wiretaps, however, this information is often classified, which puts the accused at an unfair disadvantage. Congress should enact procedures for handling intelligence wiretap information in criminal cases modeled on the Classified Information Procedures Act,[12] which provides the defense with an unclassified summary of classified information.

None of these sensible corrections to the USA PATRIOT Act's powers would impede information sharing or prevent the intelligence and law enforcement communities from taking full advantage of their considerable surveillance and intelligence gathering powers in order to protect America from terrorism.

Finally, whatever one's views on the wisdom or necessity of the powers granted to the government in the USA PATRIOT Act or changes in regulations or other longstanding policies, such a fundamental shift in surveillance and law enforcement powers plainly requires vigorous oversight on both effectiveness and civil liberties grounds. Congress

[11] Richard B. Schmitt, *U.S. Expands Clandestine Surveillance Operations*, L.A. Times, March 5, 2003.
[12] 18 U.S.C. App.

should make clear it will not consider a successor to the USA PATRIOT Act – such as the draft "Domestic Security Enhancement Act" leaked from the Department of Justice in February 2003 – until such oversight has been completed.

Data Mining and the "Total Information Awareness" Program.

The Pentagon's "Total Information Awareness" program clearly threatens individual privacy. As explained by Senator Richard Shelby, then Vice Chairman of the Senate Select Committee on Intelligence:

> "TIA aspires to create the tools that would permit [intelligence] analysts to data-mine an indefinitely expandable universe of databases. These tools would not be database-specific, but would rather be engineered in such a way as to allow databases to be added to the analytical mix as rapidly as interface software could be programmed . . . ."[13]

As a result, the Pentagon plans to use data mining software and technology to sift through vast amounts of personal information held in an "indefinitely expandable universe" of government and private-sector databases in an attempt to uncover patterns of activity that the software algorithm determines are related to terrorism. Such a program is radically different from a program to encourage greater sharing of intelligence or law enforcement information that is already collected for anti-terrorism purposes, or a program to improve the technological capacity to access data concerning a particular terrorism suspect.

Congress has, for now, placed a moratorium on the domestic use of TIA technology, while allowing research and development of the project to continue. Under the Wyden Amendment to the 2003 Omnibus Appropriations Resolution, the President is required to submit a report providing a detailed explanation of the scope of the program and the program cannot be deployed without Congressional authorization except in the cases of "[l]awful military operations . . . conducted outside the United States" and "[l]awful foreign intelligence activities conducted wholly overseas, or wholly against non-United States persons."

The Wyden Amendment offers Congress an opportunity to fully consider the implications of the mass data surveillance that TIA envisions before permitting such surveillance to go forward. Congress should be particularly skeptical of claims that a surveillance system like TIA will be effective before it permits such deployment. According to the Association for Computing Machinery (ACM), the leading nonprofit membership organization of computer scientists and information technology professionals, "the overall surveillance goals of TIA suffer from fundamental flaws . . . . Technological research alone cannot make a system such as TIA viable."[14]

---

[13] September 11 and the Imperative of Reform in the U.S. Intelligence Community, Additional Views of Senator Richard C. Shelby (Dec. 10, 2002), at p. 41.

[14] Letter to Senators Warner and Levin, January 23, 2003, available at http://www.acm.org/usacm/Letters/tia_final.html

In the meantime, as an alternative to mass, suspicionless data surveillance of the sort programs like TIA envision, the government should consider how to use information technology to better coordinate among agencies the vast quantities of data that is already collected for foreign intelligence and law enforcement purposes. It should also examine carefully what existing information technology could be adapted to automate the accessing of publicly available or – subject to appropriate legal safeguards – privately held data where the government has reason to suspect a particular individual of involvement in terrorism.

Other Information-Sharing Issues Involving Foreign and Domestic Intelligence and Law Enforcement Agencies.

The Homeland Security Act of 2002 provides a number of new authorities to share sensitive information with state officials and officials of foreign governments. Such information includes:

(1) Grand jury information (section 895);

(2) The contents of telephone and electronic communications intercepted by law enforcement officials under criminal or intelligence surveillance statutes (sections 896, 898); and

(3) Foreign intelligence information disclosed to the intelligence community by law enforcement under USA PATRIOT Act authorities (section 897).

Terrorists and terrorist organizations operate in many countries and there is no debate on the need, in general, to share information about terrorist crimes with state and local officials and among many nations' intelligence and law enforcement agencies. Yet intelligence information may also involve rumors, innuendo, and other information of a constitutionally sensitive nature that have nothing to do with terrorist crimes. Congress should encourage sharing of information about terrorist crimes with state and local officials. In circumstances not involving terrorism, intelligence information should not be shared with state and local officials.

Sharing of sensitive information with foreign governments raises a host of civil liberties issues. The most serious concern the potential use of such information by governments who fail to observe even the most basic of human rights. The United States has cooperated in anti-terrorism efforts with a number of governments, such as Syria and Saudi Arabia, whom the State Department reports routinely practice torture.[15] The United States became a party to the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment in 1994. Congress has provided severe criminal penalties for torture, and has extended jurisdiction over offenders without regard to where the torture takes place or the nationality of the offender or the victim.[16]

---

[15] *See* Department of State, Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2002, (March 31, 2003), available at http://www.state.gov/g/drl/rls/hrrpt/2002/

[16] 18 U.S.C. § 2340A.

Congress should seriously consider whether continued sharing of intelligence or law enforcement information with governments that practice torture is consistent with the treaty obligations of the United States. Consider an example where the United States lets Syrian secret police know that it is investigating a Arab American writer, and asks for information Syria may have on that individual, in exchange for a high-level meeting with a top U.S. government official. The Syrian secret police responds by arresting the writer's family and subjecting them to torture, then reporting the information it has extracted to its American counterparts. Such an example would implicate the United States, morally and perhaps legally, in a vile and criminal practice condemned under both American and international law.

At an absolute minimum, Congress should consider requiring, as a condition of receiving any intelligence or law enforcement information, that a country which the State Department has determined practices torture must certify in writing that it will not use torture or other degrading treatment in any case in which it has received such information. Vigorous oversight by this Committee and its Senate counterpart could ensure that, where such promises are not kept, the United States terminates its cooperation with the offending regime. In the absence of such safeguards, the United States risks, in essence, outsourcing torture through intelligence sharing while washing its hands of such criminal activity.

Effective Reforms of the Intelligence Community Need Not Compromise Civil Liberties

Controversy over specific policy changes with serious implications for civil liberties should not be permitted to obscure the lessons of September 11 for the intelligence community. While the full report of the Joint Inquiry of this Committee and its Senate counterpart have not yet been made public, the findings and recommendations of that investigation have illustrated a number of serious shortcomings in the handling of intelligence information prior to the September 11 attacks.

Almost without exception, the findings and recommendations of this Committee and its Senate counterpart do not concern any lack of legal authority to collect intelligence information or to share intelligence information before September 11, 2001 that was corrected as a result of the USA PATRIOT Act. Some of the most dramatic intelligence failures included:

(1) The CIA's failure to add the names of two Al Qaeda terrorists, Khalid al-Mihdhar and Nawaf al-Hamzi, who became known in early 2000, to existing government watchlists for eighteen months – after they had entered the United States (finding 5.b);

(2) The failure of FBI headquarters to take further steps to follow up on reports from its field offices concerning possible efforts by Osama bin Ladin to send members of Al Qaeda to train in American flight schools (finding 5.e);

(3) The failure of FBI headquarters personnel to seek a warrant pursuant to its existing authority under the Foreign Intelligence Surveillance Act to search the laptop computer of Zacarias Moussaoui, the alleged "20th hijacker" (finding 5.f); and

(4) The failure of the National Security Agency (NSA) to translate intercepted communications from September 8 to 10, 2001 that indicated an impending terrorist attack until after September 11, 2001 (finding 5.j).

None of these failures suggest a need for expanded powers. In the Moussaoui case, the Joint Inquiry specifically found that "personnel at FBI headquarters . . . as well as agents in the Minneapolis field office, misunderstood the legal standard for obtaining an order under FISA." Still, the Administration has asked Congress to change the law – asking for a legal fix to a bureaucratic problem.

The intelligence community's inability to "connect the dots" prior to September 11 was the result of a number of significant problems, but it appears that a lack of legal authority was not one of them. As a result, if Congress opts for the easy solution of changing the law, rather than for the hard solution of continued public oversight and pressure for reform of the intelligence community, our security as well as our civil liberties will be at risk. Likewise, building new, complex, expensive and untested surveillance technologies simply ignore the real needs for better exploitation of basic information technology by the intelligence community.

Some of the Joint Inquiry's recommendations, such as the recommendation to consider created a separate domestic intelligence agency, clearly raise civil liberties concerns. However, the majority of these recommendations do not, or even provide civil liberties benefits. The ACLU strongly encourages this Committee to press the Administration to fully implement the following recommendations for reform of the intelligence community:

(1) **More reliance on human sources.** While not without civil liberties concerns, it is plain that, despite massive electronic surveillance, the intelligence community lacked basic information about the operation of Al Qaeda prior to September 11. Developing human sources in terrorist organizations like Al Qaeda is difficult and dangerous, but desperately needed. While government agents should leave lawful protest groups alone, they should infiltrate terrorist organizations where there is reasonable suspicion of criminal activity. Terrorist groups easily meet this simply test, which protects national security by identifying those groups that pose a threat. Terrorists do not announce their plans at public political meetings and are savvy enough to avoid disclosing their plans in electronic communications they know are monitored.

(2) **Utilize existing information technology to "connect the dots."** Rather than chase some pie-in-the-sky "Total Information Awareness" program, Congress must ensure both that there is adequate funding for basic information technology

within the intelligence community and that personnel are trained to use that technology to the fullest.

(3) **Provide sufficient incentives to recruit a diverse and skilled workforce of intelligence analysts, particularly those skilled in foreign languages.** The information collected by the intelligence community under its existing powers does no good for national security unless it is translated and analyzed in a timely fashion, yet resources have not been adequate to attract and retain sufficient numbers of highly skilled intelligence analysts with skills in languages like Arabic, Hindi, and other Asian languages. The Joint Inquiry's many creative recommendations for such incentives should be fully implemented.

(4) **In depth training of all national security personnel, and continuing legal education for FBI lawyers.** If Congress tries to solve a bureaucratic problem – such as a lack of understanding of the Foreign Intelligence Surveillance Act – with a legal solution, it is bound to fail. Instead, the government must be able to better use its existing legal powers. In order to use them, government lawyers must understand them.

(5) **A thorough review of excessive secrecy.** The Joint Inquiry asked Congress to "consider the degree to which excessive classification has been used in the past and the extent to which the emerging threat environment has greatly increased the need for real-time sharing of sensitive information." Excessive classification – not civil liberties protections – almost certainly represents the greatest barrier to effective information sharing. Oversight of excessive classification has largely been regarded as an issue of interest for historians and archivists. The CIA's overly aggressive hoarding of information was a contributing factor to the intelligence failures that lead to September 11. Congress should be far more aggressive in demanding that the Administration justify its secrecy decisions, and should ask pointed questions about why President Bush's new Executive Order – which reverses a presumption against classification without good reason[17] – moves in the opposite direction.

Conclusion

Securing the freedom of the nation requires polices that ensure safety and protect civil liberties. Government policies that ask Americans to give up essential liberties for freedom present a false and dangerous choice. The lessons of September 11 show us how intelligence reforms can be implemented without compromising civil liberties.

America can become more safe while remaining free.

---

[17] Further Amendment to E.O. 12958 (March 25, 2003); *See* Adam Clymer, *U.S. Ready to Rescind Clinton Order on Government Secrets*, N.Y. Times, March 21, 2003.