Prepared Testimony and Statement for the Record of

Marc Rotenberg, President
Electronic Privacy Information Center

Hearing on

"Security and Liberty: Protecting Privacy, Preventing Terrorism"

Before the

National Commission on Terrorist Attacks Upon the United States

December 8, 2003
Russell Senate Office Building 253
Washington, DC

Thank you for the opportunity to testify today before the National Commission. My name is Marc Rotenberg and I am President of the Electronic Privacy Information Center, a public interest research organization based in Washington, DC.

We appreciate the work of the Commission and the convening of the hearing today on Security and Liberty. You have asked us to provide information that is pertinent to a full consideration of how the government can best ensure security, protect privacy, and utilize technology while identifying potential terrorists.

The statement is divided into four parts. In part one, I trace the important developments in privacy law in the United States, focusing in particular on the Privacy Act of 1974 and the federal wiretap law. Both laws reflect significant efforts to safeguard privacy even as the government sought to make use of new techniques for creating databases and monitoring private communications.

In part two, I look at the concept of Privacy Enhancing Techniques, as the term was generally understood before 9-11. My central point is that privacy techniques did not generally arise in the context of larger proposals for surveillance. In the few cases where they did, there was significant public opposition.

Part three considers systems of surveillance after 9-11. I discuss EPIC's opposition to the Total Information Awareness program and the passenger profiling system known as "CAPPS II." I also describe some of the problems that have already been uncovered in one watch list system.

Finally, in part four I make several specific recommendations. My main conclusion is that a significant expansion of the investigative abilities of the executive branch without corresponding checks and balances would fundamentally change the structure of our constitutional form of government.

I. Privacy Protection in the United States

For a full consideration of the issues before the Commission concerning privacy, it is vitally important to understand the development of privacy law in the United States and the very significant efforts that have occurred, particularly in the last few decades, to ensure privacy protection in the modern era.

The right of privacy as against the government is grounded in the Fourth Amendment to the United States Constitution. That amendment responded to the specific experience of the general warrants and the writs of assistance that gave the British colonial authorities the ability to enter homes, seize possessions, and search through papers without any basis. The drafters of the Bill of Rights clearly intended to limit the ability of government to conduct such searches.

When evaluating the conduct of a government search or the use of the evidence obtained, courts continue to look to the language of the Fourth Amendment and the previous decisions of other courts to determine whether the government's conduct is lawful. To understand the Fourth Amendment properly, it is important to realize that it is not simply an abstract judgment about whether a particular search is justified: the Fourth Amendment also reflects institutional arrangements central to the operation of the United States government. Critical to this arrangement is the establishment of an independent judiciary that has the ability to evaluate the government's claims to conduct searches and acts as a counterbalance to the investigative authority of the executive branch.

When we look at countries around the world, one of the first questions that is asked to determine the health of a democracy is whether there is a vital and independent judiciary that stands apart from the government.[1]

I make this point here, because much of the discussion about the expansion of government surveillance authority post 9-11has failed to recognize that under our form of government, there are critical checks and balances that must be respected. Several of the legislative proposals adopted since September 11 have reduced the role of the judiciary and given the government greater authority to conduct surveillance with less judicial oversight.[2]

The Fourth Amendment is the starting point for the discussion of privacy protection in the United States, but it is not where the story ends. Both the courts and the Congress have sought to establish new safeguards for privacy as technology has evolved.

Government Databases and the Privacy Act of 1974

The question of how the government should best use information technology and still safeguard privacy is not a new problem. Beginning in the 1960s, the Congress considered the question of how to regulate the new technology then being adopted by the federal government for the management of government programs. It was apparent that the automation of government records would continue to accelerate and that the adoption of this technology would make the management of government programs, including the activities of law enforcement agencies, more efficient. It was also clear that there were widespread concerns about the development of Big Brother databases.[3] These concerns were across party lines, across geographic region, and across economic class.

After extensive hearings and careful consideration of how best to protect privacy in an era of automated information systems, Congress passed the Privacy Act of 1974. It

---

1 *See generally*, U.S. Department of State, "Country Reports on Human Rights Practices" (2002), available at http://www.state.gov/g/drl/rls/hrrpt/2002/.

2 Consider the expanded use of the Foreign Intelligence Surveillance Act, the increasing use of national security letters, and the provisions of the PATRIOT Act that provide courts with only minimal review of the governments applications to conduct searches.

3 *See generally*, Daniel J. Solove and Marc Rotenberg, *Information Privacy Law* 459-60 (2003).

is the most comprehensive privacy law in the United States and the law that regulates the collection and use of personal information by the federal government.[4]

Just by way of illustration of the ongoing significance of the Privacy Act, last week the Supreme Court heard arguments in a Privacy Act case concerning the appropriate standard for determining damage awards.[5] There was no dispute about the essential purposes of the Act. The courts have long recognized the central role that the Privacy Act plays in safeguarding the privacy rights of Americans.

The Privacy Act is a complex law and I will not go into all of the details today. But I would like to point out three of the central findings from that legislation. In 1974, the Congress said that:

- The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies.

- The opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protection are endangered by the misuse of certain information systems

- In order to protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use and dissemination of information by such agencies

The issue was raised during the consideration of the Privacy Act, as it has been raised since 9-11, whether technology could provide sufficient safeguards to protect privacy when government makes use of information. Jerome Weisner, who was the President of MIT and had served as the first science advisor to President Kennedy, cautioned against this approach. He said in 1971 that

> There are those who hope new technology can redress these invasions of personal autonomy that information technology now makes possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be provided by new inventions. They must be provided by the legislative and legal systems of this country. We must face the need to provide adequate guarantees for individual privacy.[6]

---

4 Id. at 472-75.

5 *Doe v. Chao*, No. 02-1377 (U.S. docketed March 20, 2003).

6 *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the House Comm. on the Judiciary*, 92d Cong., 1st Sess. Part I, 761-774 (1971) (testimony of Jerome B. Wiesner, provost elect, Massachusetts Institute of Technology).

Even in the 1970s, the leading scientific experts understood that legal safeguards would be necessary to protect privacy.

Electronic Surveillance and the Federal Wiretap Act

Efforts to create new safeguards for government databases occurred at approximately the same time that the United States was considering how best to regulate electronic surveillance. In 1967, the Supreme Court issued opinions in two important privacy cases that have shaped the law of electronic surveillance up to the present day.

In *Katz v. United States*,[7] the Court was asked to consider whether the use of electronic surveillance required a warrant under the Fourth Amendment. This was not the first time the Supreme Court had confronted the issues. Back in the 1920s, the Court had said that, applying traditional notions of physical trespass, what the government could obtain outside the boundaries of the home would not require a warrant.[8]

By 1967, the law of electronic surveillance had become very confusing. The Court relied on the notion of physical trespass to distinguish between those cases in which a warrant was required and where it was not. In one case, the Court held that no warrant was required because there had been no physical penetration of the suspect's apartment.[9] However, in a similar case, the Court held that there was a warrant requirement because the "spike mike" had crossed the baseboard of the targeted premises.[10]

In *Katz*, the Court held that a warrant was required when the police conducted surveillance of a telephone call made at a public payphone even though the conversation could be easily recorded by means of a tape recorder hidden in the booth. The Court said that, "privacy protects people, not places." In a concurring opinion, Justice Harlan said that the right way to understand the reasonable expectation of privacy would be to consider whether the individual had a subjective expectation of privacy and whether that expectation of privacy is one that society is prepared to recognize.[11]

The second significant case that the Supreme Court would consider in 1967 was *Berger v. New York.*[12] This case has never had quite the same high profile as *Katz*. No case could. But *Berger* was a remarkable opinion. In that case, the state of New York had enacted a law to limit the use of electronic surveillance by the police. The issue before the Court was whether the state of New York had done enough to safeguard critical Fourth Amendment interests. The Court said no. Implicit in the Fourth Amendment were strict limitations on the duration of surveillance and the scope of surveillance. To permit

---

7 389 U.S. 347 (U.S. 1967).

8 *Olmstead v. United States*, 277 U.S. 438 (1928).

9 *Goldman v. United States*, 316 U.S. 129 (1942).

10 *Silverman v. United States*, 365 U.S. 505 (1961).

11 389 U.S. 347, 361.

12 388 U.S. 41 (1967).

the state to conduct broad electronic surveillance, even subject to state law, would violate the principles set out in the Fourth Amendment. In that case, Justice Clark wrote for the Supreme Court, "This is no formality that we require today, but a fundamental rule that has long been recognized as basic to the privacy of every home in America."[13]

The *Katz* and *Berger* decisions led the Congress in 1968 to establish comprehensive federal regulation for electronic surveillance in the United States, including both wiretapping and electronic bugs. The safeguards created by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 were extensive.[14] Extensive reporting requirements were established. The courts were given a critical role in overseeing the use of this authority. Clear remedies were created for violations.

Now it is probably worth saying a few words about the historical context of these events. At the same time that the Court announced these two sweeping decisions, the United States faced enormous challenges both at home and abroad. The war in Vietnam was accelerating. There was widespread civil protest in the United States. The United States faced adversaries in both the Soviet Union and China. A presidential candidate was assassinated in 1968, as was a great civil rights leader. Still, the Court and the Congress worked to establish strong privacy safeguards for communications in the United States.

Since passage of the federal wiretap act, Congress has also taken important steps to update the law. In 1986, the Congress extended wiretap protection to electronic communications, including the emerging use of email and computer-based communication services. The Electronic Communication Privacy Act of 1986 reflected a Congressional intent to ensure that the safeguards established by the federal wiretap act in 1968 would be carried forward into the new era.[15]

Today, the laws regarding electronic surveillance, both wire interception and electronic bugging, are among the most comprehensive in the world. There are elaborate requirement to obtain a warrant for the content of electronic communications. There are significant reporting requirements that make it possible to evaluate the effectiveness of electronic surveillance as an investigative method. Courts routinely report on the cases in which electronic surveillance has been authorized, including the duration of the surveillance, the basis for its use, and the outcome in the case.

The history of the Privacy Act of 1974 and the federal wiretap law is critical to understand the impact of the proposals that have been made since 9-11 to extend the government's surveillance authority. Invariably, these proposals represent a significant diminishment of the rights that Congress has previously established and the safeguards created in law to protect against abuse.

Thus, when we talk about the impact on privacy of the various new proposals to extend government surveillance, we are really discussing the impact on our current legal

---

13 388 U.S. 41, 63 (1967).

14 See 18 U.S.C. 2510 et seq.

15 See 18 U.S.C. 2701 et seq.

protections and the Fourth Amendment principles on which modern privacy law is based. In my view, much that has happened since 9-11 has diminished the Fourth Amendment freedoms of the United States.

II. Technology and Privacy

Before we consider the specific problems raised by the use of technology for profiling, tracking, monitoring and data mining, it is important to recognize that technology has a critical role to play in safeguarding the country against future terrorist acts. Technology can enable the rapid translation of intercepted communications. It can make airplanes more secure. It can provide better screening methods for cargo and containers entering the United States. It can assist first responders to act more effectively when a tragedy occurs.

In each of these examples, the government must make decisions about cost and effectiveness, but there is no inherent trade-off between measures that promote security and those that preserve liberty.

The issue that you are considering today focuses on a narrow category of technological deployment and that is how best to use information technology to identify individuals that may pose a specific threat to the United States. This is a far more complex problem. It necessarily involves subjective judgments. It is easy to construct a device that can determine whether a person is carrying a gun before he boards an airplane. It is much more difficult to construct a device that can probe his thoughts and determine his intent to commit a crime.

Since 9-11, there has been a great deal of interest in what might be described simply as "privacy friendly surveillance." By this phrase, I intend no disrespect for those who have pursued these projects. It is somewhat reassuring that many of the agencies and government officials have made clear the need to address privacy concerns as new programs are pursued. Nonetheless, it is very important not to lose sight of the underlying goal that is driving the funding of these projects and the research that is being pursued.

The point is significant because much of the work in the field of technology and privacy before 9-11 focused on how technology could enable stronger privacy protection without the expectation of any form of surveillance. This could include, for example, new techniques for electronic voting that would provide security and privacy without any risk of surveillance by a third party. It could include anonymous payment schemes that would extent familiar notions of small-cash transactions to the electronic environment, or techniques to ensure that anonymous speech, a right safeguarded by the First Amendment, would be preserved in the online world.[16]

There were two significant exceptions to the general effort to develop new systems for privacy before 9-11 without large systems of surveillance. These were the

---

16 *See, e.g.*, Herbert Burkert, "Privacy-Enhancing Technologies: Typology, Critique, Vision," in Philip E. Agre and Marc Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press 1997).

key escrow encryption scheme and the Carnivore system. Both were widely opposed by the public and subject to great debate in Congress.

The key escrow encryption scheme, also known as "Clipper," was an attempt to enable law enforcement to intercept and decode private electronic communications by requiring that a copy of all encryption keys that encoded private message be maintained by the federal government. The proposal was strongly favored by the National Security Agency and the law enforcement community that believed that it would be necessary to ensure rapid government access to information sought in the context of an investigation.

But a wide-ranging series of studies on the Clipper encryption scheme eventually concluded that it would do more harm than good. The key escrow scheme would create new vulnerabilities that did not previously exist. The National Research Council concluded that it would be a mistake to establish the key escrow system. [17] Significantly, the current Attorney General, then Senator Ashcroft, had expressed concern about key escrow encryption precisely because it gave the government this extended investigative capability. [18]

I suspect that similar problems will arise with proposals now under consideration to escrow identity. The storage of data about individuals with the expectation that the information will only be disclosed in certain, limited circumstances necessarily creates new vulnerabilities. There is also the enormous technical challenge in trying to ensure that only the necessary information will be disclosed.

This problem arose in the second pre-9-11 effort to establish new systems of surveillance that attempted to safeguard privacy. Carnivore was an investigative technique developed by law enforcement to automate the process of segregating the information obtained in an electronic environment that the government had the lawful authority to obtain from the information that the government could not properly obtain. For example, if the government was seeking real-time access to communications that were transmitted through a particular Internet Service Provider, the government might want the ability to review all electronic messages traveling through that particular ISP, but it would have the legal authority to retain the messages of only the person who was the target of the investigation.

Carnivore, which was later renamed DCS-1000, was the proposed solution to this problem. But documents obtained by EPIC revealed that in fact Carnivore provided access to information beyond the scope of the warrant. And at his confirmation hearing,

---

[17] National Research Council, Cryptography's Role in Securing the Information Society (1996).

[18] *See, e.g.*, Kevin Poulsen, "Justice pick is pro-crypto," Security Focus News, Jan. 2001 (In 1997 Ashcroft opposed an FBI-supported bill that would have mandated a "key recovery" scheme in the U.S., under which all encryption keys would be escrowed with a government agency and made available to law enforcement officers with court authorization. "Our citizens should be able to communicate privately, without the government listening in," Ashcroft said in a 1997 statement opposing the bill. "That is one of our most basic rights and principles.")

the Attorney General pledged a "a thorough review of Carnivore and its technical capabilities."

At this point, I simply intend to point out that before 9-11 there was hardly any positive discussion about the development of techniques that would enable massive surveillance while attempting to safeguard privacy. Privacy techniques were generally understood as those that would permit people to do what they wish to do – send an email, buy a product, cast a vote – with some assurance that their privacy would be safeguarded. The two proposals that were actually part of larger surveillance plans, though also incorporating some privacy concern, were highly controversial. The Congress and the President rejected key escrow encryption and Carnivore was facing a thorough review by the Attorney General of the United States.

III. Systems of Surveillance

Since 9-11 there have been many new systems put in place to monitor and track both people and activities in the United States. It would take volumes to describe fully the new systems for tracking financial transactions, international investigations, entry and exit, visa applications, and more. In a brief that we will submit to the Supreme Court later this month in a case that concerns the compelled disclosure of identification, we focus on several key systems, including the National Crime Information Center (NCIC), the Multi-State Anti-Terrorism Information Exchange (MATRIX), the United States Visitor and Immigrant Status Indicator Technology System (US-VISIT), the Transportation Worker Identification Credential (TWIC), and the Driver And Vehicle Information Database (DAVID). The brief explores the full range of personal information that may soon become available to law enforcement agents when they make a routine stop on the street.

I would be pleased to provide the Commission with a copy of the brief after it is filed. At this point, I would like to focus on the two most prominent systems that have been proposed for tracking and data mining since 9-11 – Total Information Awareness (TIA) and the Computer Assisted Passenger Prescreening System (CAPPS II).

Total Information Awareness

One of the most ambitious proposals for tracking and surveillance was certainly Admiral Poindexter's plan for Total Information Awareness. The Total Information Awareness program was ambitious in several respects. First, the proponents believed it would extract useful information from the multitude of database, including public and private record systems that could include medical information, financial information, credit reports, travel records, telephone records, and more.

Second, TIA's proponents were willing to support new research to establish data collection methods. For example, the Office of Information Awareness proposed to fund research in "human identification at a distance." According to OIA, a nationwide identification system would be of great assistance to such a project by providing an easy means to track individuals across multiple information sources.

There were some projects underway within the Office of Information Awareness that could help protect public safety and would not necessarily raise significant privacy concerns. These includeded projects on rapid language translation that would enable better use of open source materials that are obtained by the federal government as well as electronic communications that are lawfully intercepted.

But the primary focus of the work within the OIA which came to be known as Total Information Awareness was clearly the proposal to expand significantly the ability to capture and process data about individuals. Not surprisingly, this plan produced a sharp response from both the public and the Congress. Many viewed it as the technology that would make possible extensive domestic spying in the United States. Eventually, the Congress suspended funding for the program. Admiral Poindexter had failed to resolve several key questions:

First, it was never clear how the Pentagon proposed to establish adequate privacy safeguards. The backers of Total Information Awareness said at the beginning that since this was simply a research project, the policy and legal implications would have to be addressed by the agencies that used the systems. But certainly a government agency that proposed to make available to others such sophisticated surveillance capabilities has some responsibility to determine whether such techniques could be lawfully deployed.

So, the Total Information Awareness proponents then took the position that it would comply with all appropriate privacy safeguards. A report to Congress earlier this year reflected OIA's intent to comply with applicable privacy laws.[19] But the report also revealed the full extent of the Department of Defense's desire to exempt itself from most of the obligations within the Privacy Act. Indeed the listing of exemptions to the Privacy Act that would apply in the use of TIA was considerably longer than the list of privacy laws that the Department of Defense would follow.[20]

Admiral Poindexter also expressed interest in supporting privacy techniques that might enable selective revelation of information relevant to a particular investigation once judicial authority was obtained. In fact, one of the final acts of Admiral Poindexter was to provide significant funding for work in this field. But it still remains unclear whether such techniques could be made to work. Based on the previous experience with key escrow encryption and Carnivore, there is at least some basis for skepticism.

CAPPS II

Another program that has received significant public attention is the Computer Assisted Passenger Prescreening System. CAPPS is "intended to conduct risk assessments and authentications for passengers traveling by air to, from or within the

---

19 DARPA, "Report to Congress Regarding the Terrorism Information Awareness Program," May 20, 2003.

20 Id. at 26.

United States."[21] In essence, CAPPS II is a secret, classified system that the TSA will use for background checks on tens of millions of airline passengers. The results will determine whether individuals will be subject to invasive searches of their persons and belongings, or be permitted to board commercial aircraft. TSA will not inform the public of the categories of information contained in the system. It will include information that is not relevant and necessary to its stated purpose of improving aviation security. Individuals will have no judicially enforceable right to access information about them contained in the system, nor to request correction of information that is inaccurate, irrelevant, untimely or incomplete. In short, it is precisely the sort of system that Congress sought to prohibit when it enacted the Privacy Act of 1974.

I have attached to the statement the complete comments EPIC submitted to the TSA in September of this year based on our review of the system proposal and our consideration of the material made available by the TSA including the Privacy Act notice. I would like to briefly summarize our key objections to the system.

First, we argued that the TSA has resisted public scrutiny of the system and failed to comply with its obligations under the Freedom of Information Act. Soon after the establishment of TSA, EPIC began requesting information from the agency under the FOIA seeking information on the potential privacy impact of CAPPS II and other aviation security initiatives. The first such requests were submitted in February 2002 for "records concerning the development of airline passenger screening/profiling systems." When the agency failed to respond in a timely manner, EPIC filed suit in U.S. District Court.[22] TSA ultimately withheld the vast majority of responsive records because, the agency claimed, they were "pre-decisional" and constituted "sensitive security information."

In October 2002, EPIC requested information from TSA concerning the agency's creation and maintenance of "no-fly lists." Again, TSA failed to comply with the FOIA's time limits and EPIC filed suit. Eventually, TSA released records demonstrating that a substantial number of passengers had been misidentified because of the agency's "selectee" and "no-fly" lists, but withheld significant amount of material as SSI. The documents that we eventually obtained revealed significant problems with the program.

Second, we object to CAPPS going forward because the TSA has failed to conduct the Privacy Impact Assessment mandated by federal law. EPIC's most recent FOIA request sought the release of TSA's Privacy Impact Assessment for the CAPPS II project. On September 25, TSA said that responsive documents existed only in draft form and that "final versions . . . are not expected until early 2004."[23] The fact that the Privacy Impact Assessment has not been finalized is significant because its preparation for a system such as CAPPS II is mandated by the E-Government Act and Office of Management and Budget regulations.

---

[21] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003).

[22] *EPIC v. Department of Transportation*, Civ. No. 02-475 (D.D.C.).

[23] Letter from Patricia M. Riep-Dice to David L. Sobel, September 25, 2003 (available at http://www.epic.org/privacy/airtravel/pia-foia-response.pdf).

Nonetheless, the TSA proposes to go ahead with CAPPS II before the privacy implications of the system have been fully addressed and disclosed to the public. The General Accounting Office, in a recent report on another DHS information system, noted that "OMB requires that IT projects . . . perform a system privacy impact assessment, so that relevant privacy issues and needs are understood and appropriately addressed *early and continuously* in the system life cycle."[24] CAPPS II has been under development for almost two years; it is clear that TSA has failed to meet its obligation to address the privacy implications "early and continuously," as federal law requires.

Third, we believe that the CAPPS system violates the Privacy Act. The Act was intended to guard citizens' privacy interests against government intrusion. As I described above, Congress found that the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies, and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States." It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.

Although the Chief Privacy officer of the DHS has expressed strong support for the Privacy Act, the notice published by TSA exempts CAPPS II from nearly all of the relevant Privacy Act obligations. We discuss in more detail in our attached comments the specific problems with the CAPPS system regarding compliance with the Privacy Act. Here are the main problems with CAPPS:

1. The CAPPS Privacy Act notice evades the government transparency that the Privacy Act is intended to provide

2. CAPPS fails to provide meaningful citizen access to personal information

3. CAPPS fails to provide meaningful opportunities to correct inaccurate, irrelevant, untimely and incomplete information

4. CAPPS fails to assure collection of information only for "relevant and necessary" use

5. The broad "Routine Uses" of CAPPS II data will exacerbate the system's privacy problems

It was recently reported that TSA is contemplating the issuance of a security directive requiring U.S. airlines to provide the agency with passenger information for use

[24] "Information Technology: Homeland Security Needs to Improve Entry Exit System Expenditure Planning, "GAO-03-563 (June 2003).

in the testing process.[25] Such data acquisition would place in the agency's hands personal information concerning millions of individuals without, as we have discussed, meaningful rights of access or correction. TSA has simply not explained why such rights should not be provided and, as such, even limited use of personal information for testing purposes would raise significant privacy issues. Acquisition of personal data should not proceed until TSA revises its policies and practices to bring them into conformance with the intent of the Privacy Act.

Errors in No Fly Lists

Part of our concern about the operation of the CAPPS system, a dramatically expanded system for tracking millions of air passengers, is based on materials we obtained through the Freedom of Information Act that reveal that the current system for screening air passengers is flawed. As we describe in our web page on this topic, the Transportation Security Administration (TSA), which is now part of the Department of Homeland Security, is authorized by law to maintain a watch list of names of individuals suspected of posing "a risk of air piracy or terrorism or a threat to airline or passenger safety."

EPIC submitted a Freedom of Information Act request in October 2002 to learn more about the operation of the watch list, which reportedly had been used to interfere with the travel of political activists. When the TSA failed to respond to EPIC's request, we filed suit in December 2002. The lawsuit sought, among other things, TSA's criteria for putting people on so-called "no-fly lists" that bar some passengers from flying and subject others to extensive scrutiny, and complaints from passengers who felt they had been mistakenly placed on the list.

The documents released, while heavily redacted, provide insight into how the TSA operates the watch list, and raises several questions for further public and Congressional oversight.

The documents establish that the TSA administers two lists: a "no-fly" list and a "selectee" list, which requires the passenger to go through additional security measures. The names are provided to air carriers through Security Directives or Emergency Amendments and are stored in their computer systems so that an individual with a name that matches the list can be flagged when getting a boarding pass. A "no-fly" match requires the agent to call a law enforcement officer to detain and question the passenger. In the case of a Selectee, an "S" or special mark is printed on their boarding pass and the person receives additional screening at security. The TSA has withheld the number of names on each of the lists.

The watch list was created in 1990, with a list of individuals who have been "determined to pose a direct threat to U.S. civil aviation." This list was administered by the FBI before the Federal Aviation Administration and the TSA assumed full

[25] Sara Kehaulani Goo, *TSA May Try to Force Airlines to Share Data*, Washington Post, September 27, 2003, at A11.

administrative responsibility for the list in November 2001. The Transportation Security Intelligence Service (TSIS) currently serves as the clearinghouse for the addition of names to the list. Since the TSA took over, the watch list "has expanded almost daily as Intelligence Community agencies and the Office of Homeland Security continue to request the addition of individuals to the No-Fly and Selectee lists." The names are approved for inclusion on the basis of a secret criteria. The Watchlists memo notes that "all individuals have been added or removed ... based on the request of and information provided, almost exclusively by [redacted]."

There are two primary principles that guide the placement on the list, but these principles have been withheld. The documents do not show whether there is a formal approval process where an independent third party entity is charged with verifying that the names are selected appropriately and that the information is accurate. Furthermore, there is no reference to compliance with the Privacy Act of 1974, which imposes certain record keeping obligations on the agency. There is also no reference to how individuals might take their names off a list - it appears from the FOIA documents that the standard TSA response is to direct individuals to their local FBI offices to clear their names.

As part of the lawsuit, EPIC also received dozens of complaint letters filed by irate passengers who felt they had been incorrectly identified for additional security or were denied boarding. The letters describe the bureaucratic maze passengers find themselves in if they happen to be mistaken for individuals on the list. In one case, the TSA notified a passenger that airlines are responsible for administering the first generation Computer Assisted Passenger Pre-Screening System that flagged the individual as a risk for additional screening and directed the passenger to contact the airline. In another case, an airline said that the CAPPS program is run by the government, and complaints should be directed to the TSA. A local FBI office in New Jersey, at the behest of Congressman Bill Pascrell, wrote to the TSA in August 2002 to ask it to take a woman off the list who was being flagged because of her name's similarity to a wanted Australian man. In an email dated July 2002, an FBI counter-terrorism officer acknowledged that different airlines have different procedures when the passenger's name is a similar to one on the list.

Some of the incidents noted in the complaints reflect passenger inconvenience and frustration with the increased attention individuals receive because their names appear on watch lists. But other complaints are more disturbing, demonstrating real-life implications for passengers singled out for increased security in this way.

In the attached documents you will see the actual communications from members of Congress on behalf of constituents who had been detailed by airline at airports. Representative Moore wrote to the Federal Aviation Administration in May 2002 on behalf of one of his constituents who experienced problems with airport security. Rep. Moore explained that his constituent, who must travel frequently for business, is subjected to vigorous security scrutiny each time he flies because his name matches that of a "known terrorist" twenty years his senior.

Another individual appealed to Representative Quinn for help in August 2002 when he discovered his name is identical to that of a person on a watch list. This man, "an American citizen of Pakistan descent" who has "been living in the United States for almost 25 years," is a commercial airline pilot whose livelihood depends upon being permitted to board airplanes. The individual complained that he had been stopped by airport security twice, and once not permitted to board an airplane he was piloting.

The litany of problems is long, but all point to a lack of transparency and due process in the operation of the watch lists. The attached memo from the TSA suggests further areas of inquiry for the Commission.

International Implications

The problems with CAPPS and the watch lists have also raised difficult issues for the United States as it seeks cooperation with other governments. The United States has asked European air carriers to provide the Passenger Name Records on European air travelers to the United States before departure. The request creates a significant problem under European law because such information would not be routinely disclosed to police authorities in the absence of a specific investigation.

The Europeans have taken significant steps to try accommodate the United States, but strong concerns remain. The problems have been exacerbated by the fact that the TSA has indicated that access to such information could be used for routine criminal investigations.

The demands for information on citizens in other countries is raising a series of similar concerns. For example, the United States Department of Justice, through the Choicepoint firm, has sought voter registry records and motor vehicle records from almost a dozen countries in Latin America. Several of these countries began investigations once the matter was revealed, and alleged that the data transfer violated national law. The investigation and prosecution in Mexico brought an end to Choicepoint's efforts to sell data from that country to the Department of Justice.

These are complex issues that are not easily resolved. But I'd like to draw your attention to this problem because the response of the United States to future threats is also having a significant impact on the privacy rights of individuals in other countries. We are trying to impose new rules on telephone companies and Internet Service Providers c in Europe to enable better surveillance of private communications. We are mandating new biometric-identifiers for people entering the United States. While it may seem expedient to pursue these arrangements now, the diminishment of privacy protections in other countries will have long-term effects.[26]

---

[26] *See generally,* EPIC, *Privacy and Human Rights, An International Survey of Privacy Laws and Practices* (2003).

IV. Recommendations

In evaluating how best to make use of new technology to safeguard the country against future terrorists acts, I urge you to consider the following:

1. Privacy law in the United States has evolved over more than two centuries providing ever-greater protections for individuals. This has occurred even as the United States has faced economic depression, widespread public protests, world war, Presidential assassinations, and adversaries armed with nuclear weapons.

2. Many technologies can reduce the risk of threats to public safety and enable the government to respond when tragedy occurs. But there are specific problems with information technologies for monitoring, tracking, and profiling. The techniques are imprecise, they are subject to abuse, and they are invariably applied to purposes other than those originally intended.

3. Technological safeguards are simply not adequate to protect against abuse. New surveillance authorities require corresponding means of public oversight and accountability. A strong and independent judiciary as well as extensive public reporting is critical for this purpose.

4. The United States will continue to have an enormous influence on how other countries respond to emerging threats. The rule of law, transparency, an independent judiciary, popular elections, and government accountability are not as well established in other parts of the world. We must be careful that our responses do not endanger fragile democracies elsewhere.

There is no simple equation that allows the country to trade privacy rights and freedom for security and safety. Privacy laws both safeguard individual liberty and ensure government accountability. They reflect the essential form of checks and balances on which our form of government is based. Any effort to expand significantly the surveillance capabilities of the executive branch of government without corresponding oversight from the Congress and the judiciary will diminish significantly Constitutional democracy.

Thank you for the opportunity to appear before the Commission. I would be pleased to answer your questions.

ATTACHMENTS

Comments of the Electronic Privacy Information Center, on Department of Homeland Security, Transportation Security Administration, Docket No. DHS/TSA-2003-1 (Aviation Security Screening Records), Interim Final Privacy Act Notice, 68 Fed. Reg. 45265 (August 1, 2003). ["EPIC_CAPPS.pdf"]

Materials concerning air passenger "watch lists," including an internal TSA memo, obtained by EPIC under the Freedom of Information Act ["EPIC_WL.pdf"]

REFERENCES

EPIC, Air Travel Privacy
http://www.epic.org/privacy/airtravel/

EPIC, EU-US Passenger Data Disclosure
http://www.epic.org/privacy/intl/passenger_data.html

EPIC, Foreign Intelligence Surveillance Act
http://www.epic.org/privacy/terrorism/fisa/

EPIC, No-Fly Watch List Documents
http://www.epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html

EPIC, Passenger Profiling
http://www.epic.org/privacy/airtravel/profiling.html

EPIC Terrorism (Total) Information Awareness page
http://www.epic.org/privacy/profiling/tia/

EPIC USA PATRIOT Act
http://www.epic.org/privacy/terrorism/usapatriot/

EPIC Wiretap
http://www.epic.org/privacy/wiretap/