TESTIMONY OF MARC ROTENBERG

BEFORE THE

NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES

December 8, 2003

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

---

[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.

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 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

---

[3] *See generally,* Daniel J. Solove and Marc Rotenberg, *Information Privacy Law* 459-60 (2003).
[4] Id. at 472-75.
[5] *Doe v. Chao*, No. 02-1377 (U.S. docketed March 20, 2003).

> 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]

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]

---

[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).

[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.

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 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.

---

[12] 388 U.S. 41 (1967).
[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.

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 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 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

---

[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).

[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.")

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, 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

---

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

[20] Id. at 26.

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 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

---

[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.).

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.

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

---

[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).

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

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 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

---

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

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 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]

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.

---

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

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/

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Docket No. DHS/TSA-2003-1
Interim Final Privacy Act Notice
Aviation Security Screening Records

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

By notice published on August 1, 2003, the Transportation Security Administration ("TSA") established a system of records (DHS/TSA 010 -- Passenger and Aviation Security Screening Records) to support TSA's Computer Assisted Passenger Prescreening System ("CAPPS II").[1] According to TSA, CAPPS II is "intended to conduct risk assessments and authentications for passengers traveling by air to, from or within the United States."[2] Pursuant to the TSA notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by CAPPS II and the new system of records; to request that TSA substantially revise its Privacy Act notice prior to implementation of CAPPS II; and to urge the agency to desist from its recent efforts to obtain personal information concerning millions of air passengers for use in testing the system.[3]

In essence, CAPPS II, as described by TSA in its notice, is a secret, classified system that the agency will use to conduct background checks on tens of millions of airline passengers. The resulting "risk assessments" 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 accomplish 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,

---

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

[2] *Id.* at 45256.

[3] EPIC was assisted in the preparation of these comments by Catherine Harper of the Cyberlaw Clinic at the Stanford Law School Center for Internet and Society.

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.[4]

Introduction

The U.S. Supreme Court has long recognized that citizens enjoy a constitutional right to travel. Thus, in *Saenz v. Roe*, the Court noted that the "'constitutional right to travel from one State to another' is firmly embedded in our jurisprudence."[5] Indeed, TSA Administrator Admiral James Loy has observed that "the founding fathers . . . had mobility as one of the inalienable rights they were talking about."[6] For that reason, any governmental initiative, such as CAPPS II, that conditions the ability to travel upon the surrender of privacy rights requires particular scrutiny.

Given its constitutional implications, and the massive scope of the system (which seeks to collect information about tens of millions of individuals), CAPPS II understandably has been the focus of concern within Congress[7] and the general public. It has also engendered strong opposition abroad, where foreign governments and their citizens have resisted the demands of the U.S. government to provide detailed air passenger data as a condition of flight into the United States. Reflecting those concerns, a resolution was passed at the recent International Conference of Data Protection and Privacy Commissioners in Sydney, Australia calling for "an international agreement stipulating adequate data protection requirements, including clear purpose limitation, adequate and non-excessive data collection, limited data retention time, information provision to

---

[4] 5 U.S.C. § 552a.

[5] 526 U.S. 489 (1999), quoting *United States v. Guest*, 383 U.S. 745 (1966).

[6] Testimony of Admiral James Loy before House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (May 6, 2003) ("May 6 Loy Testimony").

[7] In the recently enacted Homeland Security appropriations bill (H.R.2555), Congress has blocked deployment of CAPPS II until the General Accounting Office ("GAO") studies its privacy implications. The GAO report must be completed by February 15, 2004.

data subjects, the assurance of data subject rights and independent supervision" before such data transfers occur.[8]

Much of the controversy surrounding CAPPS II has centered on the system's secrecy and the lack of public information concerning the manner in which it will assess the security risks particular individuals are deemed to pose, and the types of data that TSA will use to make such assessments. When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and, significantly, required agencies to be transparent in their information practices.[9] The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[10] Adherence to these requirements is critical for a system like CAPPS II.

In recent remarks before the international conference of data protection and privacy officials, the Chief Privacy Officer of the Department of Homeland Security assured the delegates that

> [u]nder the Privacy Act, in concert with the Freedom of Information Act and the E-Government Act, citizens, legal residents, and visitors to the United States have been afforded almost unequalled transparency into the federal government's activities and the federal government's use of personal information about them.[11]

Unfortunately, TSA's CAPPS II Privacy Act notice, along with the agency's responses to Freedom of Information Act ("FOIA") requests and lack of compliance with fundamental E-Government Act requirements, show that the Department and TSA have fallen far short of such transparency in the realm of aviation security.

---

[8] Resolution Concerning the Transfer of Passengers' Data, 25th International Conference of Data Protection & Privacy Commissioners (September 12, 2003) (available at http://www.epic.org/news/Comm03.html).

[9] S. Rep. No. 93-1183, at 1 (1974).

[10] *Id*.

[11] Remarks of Nuala O'Connor Kelly Before the 25th International Conference of Data Protection and Privacy Commissioners, Sydney Australia, September 11, 2003 ("Kelly Remarks").

I. TSA Has Thwarted Public Scrutiny Under the Freedom of Information Act

Soon after enactment of the Aviation and Transportation Security Act, Pub. L. No. 107-71, and the creation 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, seeking, *inter alia*, "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.[12] TSA ultimately withheld the vast majority of responsive records on the grounds that they were "pre-decisional" and constituted "sensitive security information" ("SSI") under 49 CFR Part 1520.

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.[13] Upon processing the FOIA request, TSA released records demonstrating that a substantial number of passengers had been misidentified as a result of the agency's "selectee" and "no-fly" lists, but withheld significant amount of material as SSI. In March 2003, EPIC sought TSA records reflecting the agency's assessment of the "potential privacy and/or civil liberties implications of the activities planned or proposed for the CAPPS II project." Upon TSA's failure to respond within the statutory timeframe, EPIC again sought judicial relief.[14] As with the previous FOIA requests, a vast amount of responsive material was withheld.[15]

Most recently, EPIC again found it necessary to seek the court's intervention when TSA refused to expedite the processing of a request for two specific documents -- the Privacy Impact Assessment and the "Capital Asset Plan and Business Case" for the CAPPS II project.[16] EPIC's request for expedition was premised upon the obvious relevance of the requested information to the Privacy Act notice at issue here and the approaching deadline for public comments.

---

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

[13] *EPIC v. Transportation Security Administration*, Civ. No. 02-2437 (D.D.C.).

[14] *EPIC v. Department of Homeland Security*, Civ. No. 03-1255 (D.D.C.).

[15] TSA has not yet fully articulated the basis for its decision to withhold this material; pursuant to court order, it must do so by October 2, 2003.

[16] *EPIC v. Transportation Security Administration*, Civ. No. 03-1846 (D.D.C.).

Although the agency relented after EPIC filed suit, its refusal to voluntarily expedite the processing of the two documents for possible release belies the suggestion that TSA is committed to an open and informed public dialogue on the significant issues raised by the CAPPS II initiative.[17] As we discuss in detail in Sec. III.A., *infra*, TSA's Privacy Act notice indicates the agency's continuing unwillingness to design and implement CAPPS II in an open and transparent manner.

II. TSA Has Not Complied With the Intent of the E-Government Act

As noted, EPIC's most recent FOIA request sought the release of TSA's Privacy Impact Assessment ("PIA") and the "Capital Asset Plan and Business Case" for the CAPPS II project. On September 25, TSA responded to the request and advised EPIC that both documents exist only in draft form and that "final versions . . . are not expected until early 2004."[18] The fact that the PIA and Business Case have not been finalized is significant because their preparation for a system such as CAPPS II is mandated by the E-Government Act and Office of Management and Budget ("OMB") regulations, respectively. The E-Government Act requires that agencies "*shall* conduct a privacy impact assessment . . . *before* . . . initiating a new collection of information that . . . will be collected, maintained, or disseminated using information technology."[19] Likewise, OMB regulations require agencies, when proposing "major" or "significant" information technology projects, to address privacy and security issues in their Business Case submissions and to prepare PIAs.[20]

---

[17] In addition to Ms. Kelly's remarks concerning "transparency," quoted above, other DHS and TSA officials have similarly acknowledged the public's right to know about the CAPPS II project. Most recently, TSA spokesman Brian Turmail was quoted as saying, "The American people have the right to know whether this system will work. We should have a dialogue based on fact and not innuendo." Ryan Singel, JetBlue *Data to Fuel CAPPS Test*, Wired News, September 16, 2003.

[18] 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).

[19] Pub. L. No. 107-347 (December 17, 2002), § 208 (emphasis added).

[20] OMB Circular A-11, part 3, Planning, Budgeting and Acquisition of Capital Assets (July 2000); Memorandum from Joshua B. Bolton, "Implementation Guidance for the E-Government

In his testimony before Congress on May 6, 2003, Admiral Loy stated that "TSA is mindful that privacy protections must be built into the CAPPS II system from its very foundation" and said that the agency was "working to finalize its CAPPS II business case, which will detail how privacy and security are built into the system" and "also will conduct a Privacy Impact Assessment."[21] It is thus surprising to find TSA moving 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."[22] 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.

III. CAPPS II Contravenes the Intent of the Privacy Act

The Privacy Act was intended to guard citizens' privacy interests against government intrusion. 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."[23] 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.[24]

Act of 2002" (August 1, 2003) (available at http://www.whitehouse.gov/omb/memoranda/m03-18.pdf).

[21] May 6 Loy Testimony.

[22] INFORMATION TECHNOLOGY: Homeland Security Needs to Improve Entry Exit System Expenditure Planning, GAO-03-563 (June 2003) (emphasis added).

[23] Pub. L. No. 93-579 (1974).

[24] *Id.*

DHS's Chief Privacy Officer recently touted the protections afforded by the Privacy Act (and the purpose of a notice like the one at issue here), explaining that the law

> provides substantial notice, access, and redress rights for citizens and legal residents of the United States whose information is held by a branch of the federal government. The law provides robust advance notice, though detailed 'system of records' notices, about the creation of new technological or other systems containing personal information. The law also provides the right of access to one's own records, the right to know and to limit other parties with whom the information has been shared, and the right to appeal determinations regarding the accuracy of those records or the disclosure of those records.[25]

The notice published by TSA, however, exempts CAPPS II from nearly all of the Privacy Act provisions Ms. O'Connor Kelly described.[26] As we detail below, the exemptions claimed by the TSA are thoroughly inconsistent with the purpose and intent of the Privacy Act.

As an initial matter, we note that TSA has invoked 5 U.S.C. § 552a(k) as authority for its exemption of specific Privacy Act requirements. The only subsections of that provision that appear to be possibly relevant to the CAPPS II system are (k)(1) and (k)(2). Subsection (k)(1) is applicable only where the system of records is "subject to the provisions of section 552(b)(1) of this section," *i.e.*, if the system contains classified information. While TSA has designated the "Security Classification" of the system of records as "[c]lassified, sensitive,"[27] it is not apparent that *all* information in the system of records warrants (or is entitled to) such classification. For instance, "Passenger Name Records (PNRs) obtained from airlines"[28] clearly are not subject to government classification.

Subsection (k)(2) is applicable only where the system of records is "investigatory material compiled for law enforcement purposes." The subsection provides, however, that

> if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual . . .

---

[25] Kelly Remarks.

[26] Indeed, TSA has invoked exemptions for *all* of the requirements that the Privacy Act permits an agency to invoke.

[27] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45268.

[28] *Id*.

Given that TSA seeks to exempt the CAPPS II system of records from the Privacy Act's access provisions, as we discuss below, it is unclear whether subsection (k)(2) authorizes TSA's action. As such, we urge TSA to specify which subsection(s) of 5 U.S.C. § 552a(k) it is claiming as authority to exempt the system of records from the various Privacy Act provisions it cites.

We also question whether TSA's invocation of exemptions is procedurally and substantively sound. The legislative history suggests it is not:

> Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions [of exemptable categories] then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained." The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information . . . and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.[29]

TSA's notice does not appear to be the kind of "rulemaking" that Congress envisioned. Nor has the agency stated whether, let alone why, it has determined that the application of standard Privacy Act procedures would "seriously damage" the purpose of the system of records. In addition, the application of the claimed exemptions to the *entire* system of records is clearly inappropriate, as it will obviously contain information "which should be legitimately subject to the access, challenge and disclosure provisions."[30] TSA must cure these defects before collecting personal data for inclusion in the CAPPS II system of records.

---

[29] S. Rep. No. 93-3418, at 75 (1974).

[30] *See also* Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28972 (July 9, 1975) ("OMB Guidelines") ("agencies should, wherever practicable, segregate those portions of systems for which an exemption is considered necessary so as to hold to the minimum the amount of material which is exempted").

A. TSA's Notice Evades the Government Transparency that the Privacy Act is Intended to Provide

Under the Privacy Act, government transparency is the rule rather than the exception. TSA has frustrated that intent by exempting the CAPPS II system of records from the requirement that it publish "the categories of sources of records in the system."[31]

The legislative history of the Privacy Act unequivocally demonstrates that government agencies must be open about their information collection practices unless they can show that exceptional circumstances require secrecy. One key objective of the Privacy Act is to ensure that agencies "give detailed notice of the nature . . . of their personal data banks and information systems . . . ."[32] The Senate Report notes that "it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency."[33] In those few instances in which a limited exemption for national security and law enforcement was recognized, the exemption was "not intended to provide a blanket exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information."[34] Rather, the agency must show that the implementation of specific Privacy Act provisions would "damage or impede the purpose for which the information is maintained."[35]

In its authoritative guidance on implementation of the Privacy Act, OMB explained that "[f]or systems of records which contain information from sources other than the individual to whom the records pertain, the notice should list the types of sources used."[36] While "[s]pecific

---

[31] 5 U.S.C. § 552a(e)(4)(I); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

[32] S. Rep. No. 93-1183, at 2 (1974).

[33] *Id*. at 74.

[34] *Id*.

[35] *Id*. at 75.

[36] OMB Guidelines at 28964.

individuals or institutions need not be identified," the Act contemplates that general categories, such as "financial institutions" or "educational institutions" should be listed.[37]

Despite the Privacy Act's clear emphasis on transparency and TSA's claimed dedication to preserving individuals' privacy, the agency seeks to avoid the requirement that it inform the public of the sources of information that will feed into the CAPPS II system. TSA does not even attempt to meet its burden of demonstrating that the publication of such basic information about the system would somehow impede its presumed effectiveness.

In the supplementary material accompanying its Privacy Act notice, TSA asserts that it "will not use measures of creditworthiness, such as FICO scores, and individual health records in the CAPPS II traveler risk determination."[38] That assurance rings hollow, however, in light of the agency's stated intention to keep secret the sources of information that will eventually be fed into the system.[39]

TSA's determination that CAPPS II will be exempt from the requirement of publishing categories of sources of records is at odds with specific assurances the agency provided to Congress. When asked about this issue just four months ago, Admiral Loy indicated that such information would, in fact, be disclosed:

> SEN. BYRD: Will the new notice name the precise databases of information that CAPPS II will collect about air passengers?
>
> ADM. LOY: I don't know that we have any reason not to name those in the privacy notice . . . .[40]

---

[37] *Id.*

[38] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267.

[39] This is one of several instances in which assurances contained in the supplementary material accompanying the Privacy Act notice are contradicted by the language of the notice itself. EPIC urges TSA to clarify these apparent discrepancies and to clearly state, for instance, whether the public would be notified if the "categories of sources of records" included in the CAPPS II system were to include, at some time in the future, creditworthiness and health data.

[40] *The Fiscal Year 2004 Appropriations for the Bureau of Customs and Border Security; Transportation Security Administration and Federal Law Enforcement Training Center, Hearing Before the Homeland Security Subcommittee of the Senate Appropriations Committee*, 108th Cong. (May 13, 2003) (testimony of Admiral James Loy).

If TSA cannot articulate any reason to exempt CAPPS II from publishing categories of sources of records, it should not exempt the system from that requirement. The Privacy Act does not permit such secrecy unless an agency can demonstrate that it is absolutely necessary for reasons of national security and law enforcement.

B. TSA's Notice Fails to Provide Meaningful Citizen Access to Personal Information

In its notice, TSA has exempted CAPPS II from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them. The Privacy Act provides, among other things, that

- an individual may request access to records an agency maintains about him or her;[41] and
- the agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access.[42]

In lieu of the statutory, judicially enforceable right of access provided by the Act, TSA has established the "CAPPS II Passenger Advocate," apparently to act as a sort of ombudsman, to receive and process requests for access. According to the supplementary information accompanying TSA's notice, "passengers can request a copy of *most* information contained about them in the system from the CAPPS II passenger advocate."[43] The formal notice section, however, states that "[a]ll persons may request access to records containing information *they* provided," which presumably would include only the name, address, and telephone number given to an airline when making a travel reservation.[44] In addition, the notice provides that the system of records "may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual."[45] Such limited, discretionary access to information

---

[41] 5 U.S.C. § 552a(d)(1). Individuals may seek judicial review to enforce the statutory right of access provided by the Act. 5 U.S.C. § 552a(g)(1).

[42] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).

[43] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45267 (emphasis added).

[44] *Id*. at 45269 (emphasis added).

[45] *Id*.

is an inadequate substitute for the access provisions set forth in the Privacy Act, and TSA offers no explanation why such restricted access is necessary in the context of CAPPS II.

TSA's "passenger advocate" acting as middleman is no substitute for the judicially-enforceable access rights provided by the Privacy Act. TSA's notice states that access to one's personal information may be obtained "by sending a written request to the CAPPS II Passenger Advocate" and that "to the greatest extent possible and consistent with national security requirements, such access will be granted."[46] No time guidelines are specified for the procedure. However, TSA explains that "in most cases, the response to a record access request will very likely be that no record of the passenger exists in the system" because records are maintained for too short a time, although "[t]he duration of data retention" for non-U.S. persons "is still under consideration," and "[e]xisting records obtained from other government agencies, including intelligence information, watch lists, and other data will be retained for three years, or until superseded."[47]

As a practical matter, therefore, the only information a passenger can access is the information he provided to the airlines himself. Moreover, even this information may not be accessible, as that information will likely be destroyed in the time it takes a passenger to contact the passenger advocate. In most cases, a passenger will be unable to gain access to records about him kept by the agency, and, in many cases, he will not even be able to learn that a record pertaining to him exists. In fact, the only indication a passenger may have that the government is keeping records about him is if he is given extra scrutiny at the security gate (or, of course, detained and arrested there). TSA's weak access provisions are in direct conflict with the purposes of the Privacy Act, which sought to provide citizens with an enforceable right of access to personal information maintained by government agencies.

---

[46] *Id*.

[47] *Id*.

C. TSA's Notice Fails to Provide Meaningful Opportunities to Correct Inaccurate, Irrelevant, Untimely and Incomplete Information

Companion and complementary to the right to access information is the right to correct it. TSA's notice establishes a system that provides neither adequate access nor the ability to amend or correct inaccurate, irrelevant, untimely and incomplete records. The agency has exempted the CAPPS II system from the Privacy Act requirements that define the government's obligation to allow citizens to challenge the accuracy of information contained in their records, such as:

- an agency must correct identified inaccuracies promptly;[48]
- an agency must make notes of requested amendments within the records;[49] and
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records.[50]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[51]

Instead of the judicially enforceable right to correction set forth in the Privacy Act,[52] TSA has established its own, discretionary set of procedures for passengers to contest the accuracy of their records. TSA's notice states that "[a] passenger who, having accessed his or her records in this system, wishes to contest or seek amendment of those records should direct a written request

---

[48] 5 U.S.C. § 552a(d)(2)(B), (d)(3).

[49] 5 U.S.C. § 552a(d)(4).

[50] 5 U.S.C. § 552a(f)(4).

[51] H.R. Rep. No. 93-1416, at 15 (1974).

[52] 5 U.S.C. § 552a(g)(1).

to the CAPPS II Passenger Advocate."[53] Further, "[i]f the matter cannot be resolved by the CAPPS II Passenger Advocate, further appeal for resolution may be made to the DHS Privacy Office."[54] Notably, TSA reserves the right to alter even these minimal, discretionary procedures: "These remedies for all persons will [be] more fully detailed in the CAPPS II privacy policy, which will be published before the system becomes fully operational."[55] In addition, "DHS is currently developing a robust review and appeals process, to include the DHS privacy office."[56]

The notice provides TSA the discretion to correct erroneous information upon a passenger's request, but does not obligate the agency to do so. Significantly, there would be no right to judicial review of TSA's determinations. This correction process offers a token nod to the principles embodied in the Privacy Act, but does not provide a meaningful avenue to pursue correction and is subject to change at TSA's whim. Furthermore, the agency presents no explanation why judicially-enforceable Privacy Act correction procedures would be inappropriate in the context of CAPPS II. Denying citizens the right to ensure that the system contains only accurate, relevant, timely and complete records will increase the probability that CAPPS II will be an error-prone, ineffective means of singling out passengers as they seek to exercise their constitutional right to travel.

D. TSA's Notice Fails to Assure Collection of Information Only for "Relevant and Necessary" Use

Incredibly, TSA has exempted CAPPS II from the fundamental Privacy Act requirement that an agency "maintain in its records only such information about an individual as is relevant and necessary" to achieve a stated purpose required by Congress or the President.[57] TSA does not even attempt to explain why it would be desirable or beneficial to maintain information in the CAPPS II system that is irrelevant and unnecessary, although it apparently intends to do so.

---

[53] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

[54] *Id*.

[55] *Id*.

[56] *Id*.

[57] 5 U.S.C. § 552a(e)(1); Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45269.

Such open-ended, haphazard data collection plainly contradicts the objectives of the Privacy Act and raises serious questions concerning the likely impact of the CAPPS II rating process on millions of law-abiding travelers.

In adopting the Privacy Act, Congress was clear in its belief that the government should not collect and store data without a specific, limited purpose. The "relevant and necessary" provision

> reaffirms the basic principles of good management and public administration by assuring that the kinds of information about people which an agency seeks to gather or solicit and the criteria in programs for investigating people are judged by an official at the highest level to be relevant to the needs of the agency as dictated by statutes . . . . This section is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary[.][58]

As OMB noted in its Privacy Act guidelines, "[t]he authority to maintain a system of records does not give the agency the authority to maintain any information which it deems useful."[59]

The Privacy Act's "relevant and necessary" provision thus seeks to protect individuals from overzealous, arbitrary and unnecessary data collection. It embodies the common sense principle that government data collection is likely to spiral out of control unless it is limited to only that information which is likely to advance the government's stated (and legally authorized) objective. Like TSA's other deviations from customary Privacy Act requirements, the "relevant and necessary" exemption will serve only to increase the likelihood that CAPPS II will become an error-filled, invasive repository of all sorts of information bearing no relationship to its stated goal of increasing aviation security.

E. The Broad "Routine Uses" of CAPPS II Data will Exacerbate the System's Privacy Problems

TSA's notice identifies six categories of "routine uses" of the information that will be collected and maintained in the CAPPS II system of records.[60] These include anticipated

---

[58] S. Rep. No. 93-3418, at 47 (1974).

[59] OMB Guidelines at 28960.

[60] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45268.

disclosure to a broad range of individuals and entities, such as "Federal, State, local, international, or foreign agencies or authorities . . . contractors, grantees, experts, or consultants . . . airports and aircraft operators."[61] As we have shown, the information that would be disclosed is likely to include material about individuals that is not "relevant and necessary" to any legitimate aviation security requirements. Nor would such information be subject to a meaningful and enforceable process to ensure that it is accurate, relevant, timely or complete. The broad dissemination of CAPPS II information that TSA anticipates underscores the need for full transparency (and resulting public oversight) and judicially-enforceable rights of access and correction.

Related to the breadth of the routine uses is the issue of "mission creep" -- the tendency of government agencies to expand the use of personal information beyond the purpose for which it was initially collected. Admiral Loy discussed the issue in Congressional testimony, stating that "mission creep, if you will, is one of those absolute parameters that . . . I am enormously concerned about and we will build such concerns into the privacy strategy that we will have for CAPPS II."[62] Three months before the notice was published, Admiral Loy assured Congress that CAPPS II was designed as an aviation security tool, and not as a law enforcement tool.[63]

Despite those assurances, the CAPPS II system already contains a carve-out for a purpose beyond its original mission. The notice states that "[a]fter the CAPPS II system becomes operational, it is contemplated that information regarding persons with outstanding state or federal arrest warrants for crimes of violence many also be analyzed in the context of this

---

[61] *Id.*

[62] May 6 Loy Testimony.

[63] *Id*. Admiral Loy stated:

> [w]e are not searching [the National Crime Information Center database] as part of the . . . data that we're looking at . . . . [A]t the moment we are charged with finding in the aviation sector foreign terrorists or those associated with foreign terrorists and keep[ing] them off airplanes. That is our very limited goal at the moment. . . . [E]ven as heinous as it sounds, the axe murderer that gets on the airplane with a clean record in New Orleans and goes to Los Angeles and commits his or her crime, that is not the person we are trying to keep off that airplane at the moment.

system."[64] While the government clearly has a legitimate interest in apprehending accused felons, there are innumerable reasons why it may want to locate particular individuals. Such uses of CAPPS II data, however, are plainly beyond the authorized scope of TSA's mission of ensuring aviation security. It is crucial that TSA define the purpose of CAPPS II, at the outset, more strictly and limit the use of collected information to its core mission.

F. Testing of CAPPS II Should Not Proceed Until TSA's Notice is Revised

While we welcome TSA's assurance that "[a] further Privacy Act notice will be published in advance of any active implementation of the CAPPS II system,"[65] we note the agency's statement that "[w]ith the publication of this notice, internal systems testing will begin, using this System of Records."[66] According to the agency, "[d]uring these tests, TSA will use and retain [Passenger Name Record] data for the duration of the test period."[67] 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 in the testing process.[68] 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 articulated no reason 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.

---

[64] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45266.

[65] *Id*.

[66] *Id*. at 45265-45266.

[67] *Id*. at 45267.

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

Conclusion

For the foregoing reasons, EPIC believes that TSA must revise its Privacy Act notice for the CAPPS II system to 1) ensure greater transparency through the establishment of a non-classified system; 2) provide individuals enforceable rights of access and correction; 3) limit the collection of information to only that which is necessary and relevant; and 4) substantially limit the routine uses of collected information. Further, development of the system should be suspended until TSA prepares a final Privacy Impact Assessment, discloses it to the public and receives public comments. Finally, the agency should not acquire personal information, even for testing purposes, until it has revised its Privacy Act notice as suggested above.

Respectfully submitted,

David L. Sobel
General Counsel

Marcia Hofmann
Staff Counsel*

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009
(202) 483-1140

** Bar admission pending*

FAXED

COMMITTEE ON THE BUDGET

COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON CAPITAL MARKETS, INSURANCE AND GOVERNMENT SPONSORED ENTERPRISES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

COMMITTEE ON SCIENCE
SUBCOMMITTEE ON RESEARCH
SUBCOMMITTEE ON SPACE AND AERONAUTICS

COMMITTEE ON SMALL BUSINESS
(ex officio, 107th Congress)

Congress of the United States
House of Representatives

DENNIS MOORE
Third District, Kansas
www.house.gov/moore

431 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-1603
PHONE: 202-225-2865
FAX: 202-225-3507

9410 SANTA FE DRIVE, #101
OVERLAND PARK, KS 66212
PHONE: 913-383-1012
FAX: 913-383-2088

500 STATE AVENUE, #176
KANSAS CITY, KS 66101
PHONE: 913-621-0832
FAX: 913-621-1633

647 MASSACHUSETTS ST., #212
LAWRENCE, KS 66044
PHONE: 785-843-0313
FAX: 785-843-3268

MIAMI COUNTY
PHONE: 913-294-4122

May 28, 2002

SENT BY FAX: 202-267-5047

JANE F. GARVEY
ADMINISTRATOR
FEDERAL AVIATION ADMINISTRATION
800 INDEPENDENCE AVENUE SOUTHWEST
WASHINGTON DC 20591-0004

Re: [redacted] b6

Dear Ms. Garvey:

I was recently contacted by one of my constituents who travels frequently and has been subjected to extensive and thorough searches before boarding every flight.

This young man, whose travels are job related, realized the searches were not random. b6 Upon contacting the FAA Intelligence, we were told that his name, [redacted] is the alias of a known terrorist. However, according to FAA Intelligence, the known terrorist is about 20 years older that my constituent.

It is my understanding that the "Watch List" which the FAA Intelligence furnishes to the airlines contains only the names of known or suspected terrorists. Are other physical identifiers or a date of birth/age information included on the "Watch List"? Inclusion of this information might reduce the unnecessary time and inconvenience of conducting searches that contribute nothing to security.

I would appreciate your consideration of adding the birth date or age information to the names listed on the "Watch List" if this information is not already included. This would improve the efficiency of the airport screeners and alleviate some of the inconvenience to passengers. Thank you.

Very truly yours,

DENNIS MOORE
Member of Congress

000215

DM:kc

JACK QUINN
30TH DISTRICT, NEW YORK

COMMITTEES:

TRANSPORTATION AND INFRASTRUCTURE
CHAIRMAN, SUBCOMMITTEE ON RAILROADS
SUBCOMMITTEE ON AVIATION
SUBCOMMITTEE ON HIGHWAYS AND TRANSIT

VETERANS' AFFAIRS
SUBCOMMITTEE ON BENEFITS

CHAIRMAN, NORTHEAST MIDWEST COALITION
CHAIRMAN, STEEL CAUCUS EXECUTIVE COMMITTEE

TSA

Congress of the United States

House of Representatives
Washington, D.C. 20515-3230

PLEASE RESPOND TO:

WASHINGTON OFFICE:
2448 RAYBURN BUILDING
WASHINGTON, DC 20515
(202) 225-3306
FAX: (202) 226-0347

MAIN OFFICE:
403 MAIN STREET
SUITE 240
BUFFALO, NY 14203-2199
(716) 845-5257
FAX: (716) 847-0023

SATELLITE OFFICE:
1400 JEFFERSON AVENUE
BUFFALO, NY 14208
(716) 886-4076

August 30, 2002

Mr. Quentin Burgess
Acting Administrator for Government Affairs
Federal Aviation Administration
800 Independence Ave SW, Rm 1022
Washington, D.C. 20591-0004

Dear Mr. Burgess,

b6

I have recently been contacted by [redacted] regarding difficulties he has encountered as a professional and private pilot at the airport.

I have taken the liberty of enclosing the correspondence I received relative to this matter, and look forward to your expedited review and response.

b6 b6

[redacted] seeking some identification/clearance that will provide him more easy passage to and from work as a pilot. [redacted] believes his common Pakistani surname has been the cause of these delays. Every assistance afforded him will be appreciated.

Thank you in advance for your attention to this matter. If you have any questions or suggestions, please do not hesitate to contact me in my Buffalo district office.

Very truly yours,

Jack Quinn
Member of Congress

JQ:mc

OFFICE OF THE ADMINISTRATOR
2002 SEP 10 A 10 57
EXECUTIVE SECRETARIAT

RECEIVED

02 AUG 29 AM 9:35

CONG... BUFFALO DISTRICT OFFICE

[redacted] b6

Honorable Jack Quinn
Member of Congress

Dear Mr. Quinn:

I am an American citizen of Pakistan descent and have been living in the United States for almost 25 years.

I am presently employed as an airline pilot and have been so employed for numerous years without incident.

After September 11, and in the last month, I have been stopped twice by airport security because my last name is [redacted] the name [redacted] is in the computer as a person to be checked. The first time I was flying on my own, but because of this problem I was unable to board my plane and had to stay overnight to get clearance. b6 b6

Last week, while in full uniform, I was again stopped for the same reason and delayed for over an hour. As a result, I was almost unable to leave on time and the flight was almost canceled.

I am sure my employer will not put up with this, because if the plane I am supposed to fly is delayed, it could cost the airline a lot of money.

Would you please check with the "Joint Task Force" of the FBI and see if there is anything they can give me so I can clear security without being delayed unnecessarily?

[redacted] a very common surname in Pakistan and without a first name it borders on harassment. Could you imagine if you were stopped, questioned for over an hour and almost missing a plane because the name "Quinn" was in the computer? b6

Very truly yours,

[redacted] b6

NM/amp

000241

Memorandum

U.S. Department of Transportation
Transportation Security Administration

Subject: INFORMATION: TSA "Watchlists"

Date: October 16, 2002

Reply to

From: Acting Associate Under Secretary, Transportation Security Intelligence, TSI-1

To: Associate Under Secretary, Security Regulation and Policy

1. **(FOUO) Summary:** Since November 2001, the FAA/TSA "watchlist" has expanded almost daily as Intelligence Community (IC) agencies and the Office of Homeland Security continue to request the addition of individuals to the No-Fly and Selectee lists. [redacted] (b)(5)

(FOUO) Although TSA compiles the lists from requests made by IC agencies, the airline companies are responsible for implementing the security directives (SDs) that support the two lists. [redacted] (b)(5) (b)(2) (b)(3) 1520.7(b) (j)

2. **(SSI) Background:** Between 1990 and September 11, 2001, the FAA issued several Security Directives (SDs) and companion Emergency Amendments (EAs) that identified persons whom air carriers could not transport, because they were determined to pose a direct threat U.S. civil aviation. [redacted] On September 11, 2001, only three of these SDs were in effect, with a total of [redacted] names of individuals that air carriers were prohibited from transporting. (b)(2) (b)(3) 1520.7(b), (c)(j)

(SSI) Early on September 12, [redacted] the FAA issued SD-108-01-06/EA 129-01-05, [redacted] (b)(2) (b)(3) 1520.7(b), (c), (j)

(SSI) In November 2001, [redacted] the FAA assumed full administrative responsibility for the "watchlist" and issued SD-108-01-19. At that time, the three active FAA SD/EAs that had listed names of individuals to be denied transport [redacted] were canceled. [redacted] (b)(2) (b)(3) 1520.7(b), (j)

[redacted] and the SD was broken out into two separate "name lists:" No-Fly and Selectee. SD-108-01-20*** supports the list of persons to be denied transport; this list is commonly referred to as the "No-Fly list." SD-108-01-21*** supports the list of persons whom air carriers are required to "select" for additional security screening prior to boarding the individuals on an aircraft; this list is referred to as the "Selectee list."

3. (FOUO) Discussion:

A. (FOUO) Current Procedures: All individuals placed on the No-Fly and Selectee lists since November 2001 have been added or removed (or moved from one list to the other) based on the request of and information provided, almost exclusively, [redacted] (b)(2) (b)(3) 1520.7(j) (c)

[redacted] Names are removed from the two lists when [redacted] the individual is no longer assessed to pose a threat to U.S. [redacted]

B. (FOUO) Criteria: Since FAA/TSA assumed administrative control of the "watchlist" in November 2001, the placement of individuals on the No-Fly or Selectee lists has been guided by two primary principles: [redacted] (b)(2) (b)(3) 1520.7(c), (j)

[redacted]

(b)(2)
(b)(3)
1520.7(c)
(j)

(FOUO) The essential purpose of the No-Fly list is to prevent the transport of individuals who [redacted] The Selectee list is a less restrictive measure that requires named individuals to be subjected to additional security screening measures before being allowed to board an aircraft. [redacted] TSA's immediate concern is the safety of the flying public.

b(2)
b(3)
1520.7(c)
(j)
b(5)

(FOUO) [redacted]

(b)(2)
(b)(5)
(b)(3)
1520.7(c)
(j)

C. (FOUO) Requirements: [redacted]

b(2)
b(3)
1520.7(c)
(j)

(FOUO) [redacted]

(b)(2)
(b)(3)
1520.7(b)
(j)

[redacted] b(2) (b)(3) 520.7(b) (j)

4. (FOUO) Problems and Recommendations:

A. (FOUO) [redacted] b(2) (b)5) (b)(3) 1520.7(b) (c); (j)

(FOUO) Solution: [redacted] (b)2 (b)(5) (b)(3) 1520.7(c), (j), (L)

B. (FOUO) [redacted] (b)(2) (b)(5) (b)(3) 1520.7(b), (L)

(FOUO) Solution: [redacted]

C. (FOUO) [redacted] (b)(2) (b)(5) (b)(3) 1520.7(b)

[redacted] (b)(2) (b)(5) (b)(3) 1520.7(

(FOUO) Solution: [redacted] (b)(5) (b)(3) 1520.7(

5. (FOUO) Conclusions: [redacted]

continues to receive these requests on a daily basis. [redacted] b(5)

Claudio Manno