**Pergamon**

Government Information Quarterly 20 (2003) 295–314

**Government Information Quarterly**

# The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act

Paul T. Jaeger*, John Carlo Bertot, Charles R. McClure

*Florida State University, School of Information Studies, Information Use Management and Policy Institute, 101 Shores Building, Tallahassee, FL 32306, USA*

**Abstract**

The collection and analysis of personal information under the Foreign Intelligence Surveillance Act (FISA) has been significantly altered by the U.S.A. Patriot Act, and a proposed enhancement to the Patriot Act would create further changes. This article examines the original intent and scope of FISA, how the Patriot Act has dramatically modified the scope and meaning of FISA, and how the Patriot enhancement, if it were to be enacted into law, would create further significant alterations to FISA. The article explores the impact of these changes on information policy, especially in terms of the collection and analysis of personal information. The implications of these changes to FISA are examined in terms of a number of sources of personal information, including e-government, electronic and transactional records, and libraries. Finally, this article discusses the difficulty in determining the practical effects of these changes to FISA. 

## 1. Introduction

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("Patriot Act"), passed by the U.S. Congress in reaction to the terrorist attacks of September 2001, significantly alters a considerable number of laws, including many related to information policy.[1] The Patriot Act included far-reaching modifications to the Foreign Intelligence Surveillance Act (FISA).[2] A new enhancement of the Patriot Act, entitled the Domestic Security Enhancement Act of 2003, has been drafted by

* Corresponding author. Fax: +1-850-644-4522

*E-mail address:* ptj0956@garnet.acns.fsu.edu (P.T. Jaeger).

0740-624X/03/$ – see front matter 
doi:10.1016/S0740-624X(03)00057-1

the Department of Justice. If it were to became law, it would serve to further expand investigative powers under FISA to collect and analyze information.[3] The changes to the FISA by the Patriot Act, and the potential further changes to FISA that would occur if the Patriot Act enhancement became law, have major implications for information policy.

The passage of the Patriot Act, and other concurrent reactions to the terrorist attacks of September 11, 2001, reflect a decision by the federal government to view security in terms of "the preservation of the security of the homeland."[4] A more expansive approach to security than the United States has previously taken (national security and internal security), homeland security has led to the creation of the Department of Homeland Security, to the alteration of many laws and judicial traditions, and to a virtual abandonment of "Cold War era barriers between foreign intelligence and domestic law enforcement."[5]

Among its many impacts, the Patriot Act modifications of FISA affect the degrees to which and the methods by which law enforcement agencies can collect and analyze personal information. This article examines the evolution of FISA in terms of the collection and analysis of personal information from three perspectives: (1) prior to the passage of the Patriot Act; (2) as it currently is, having been modified by the Patriot Act; and (3) what FISA might be if the draft Patriot Act enhancement legislation became law. This article explores the implications of this evolution by tracing these changes and their impacts on collection and analysis of personal information. By discussing the key policy issues raised by the changes to FISA, this article explores the ramifications of the evolution of FISA to information policy.

## 2. The origins of the Foreign Intelligence Surveillance Act

According to the Constitution, the President has the obligation to "preserve, protect and defend the Constitution of the United States."[6] Over the course of the twentieth century, limited use of electronic surveillance to collect and analyze intelligence information became an accepted element of the executive powers necessary to defend the nation. The frequent use of wiretapping and other forms of electronic surveillance for these purposes began primarily with the administration of Franklin Roosevelt, though he expressed hesitance in authorizing such activities.[7] Each subsequent president tended to echo Roosevelt's apprehensions while expanding gradually the use of electronic surveillance.

The impetus for the Foreign Intelligence Surveillance Act was a result of executive branch abuses of electronic surveillance, most prominently those of Richard Nixon and members of his administration. In 1954, U.S. Attorney General Herbert Brownell ordered the Federal Bureau of Investigation (FBI) to conduct covert, warrantless searches and seizures whenever FBI agents believed national security might be involved.[8] From the McCarthy era to the Nixon administration, federal law enforcement and intelligence gathering agents used highly intrusive electronic surveillance techniques on individuals and groups with little or no relevance to the concerns of national security. The subjects of such investigations included journalists, White House policy advisors, Congressional staff members, at least one member of Congress, civil rights organizations, antiwar protesters, student groups, and the Democratic Party.[9] In reaction to these revelations, the Senate formed the Select Committee to

Study Government Operations with Respect to Intelligence Activities in order to determine an appropriate response.[10] Inspired by the suggestions in a Supreme Court opinion that Congress create separate standards and procedures for surveillance for intelligence purposes and surveillance for criminal investigations, FISA was passed in 1978 after six years of debate and negotiation.[11]

FISA was intended to serve as a "firewall between foreign and domestic intelligence gathering."[12] FISA created a clear distinction between investigative conduct in domestic criminal investigations and in foreign intelligence investigations. By creating this distinction, FISA served to protect the Fourth Amendment rights of U.S. citizens in criminal investigations, requiring probable cause before a search warrant is issued and preserving freedom from unreasonable search and seizure.[13] Under FISA, these Fourth Amendment protections did not apply in full force in foreign intelligence investigations, allowing law enforcement agencies to get court orders for wiretaps and searches with a much lower standard of proof than required in a criminal investigation. Rather than needing to demonstrate probable cause of criminal activity, a FISA order could be issued by demonstrating that the purpose of the investigation was to gather foreign intelligence information.

In the legislative history of FISA, Congress stated warrantless searches "in the name of national security have been seriously abused."[14] To curtail such future abuses, FISA created a complex structure for conducting electronic surveillance, which was limited to foreign powers or their agents for the specific primary purpose of obtaining intelligence information. However, FISA balanced the protection of Fourth Amendment rights of citizens with concerns of national security by still allowing the executive ample ability to engage in foreign intelligence surveillance.

Under FISA, a surveillance warrant generally required the approval of the Attorney General and of a Foreign Intelligence Surveillance Court (FISC). If the subject under surveillance was a U.S. citizen, the warrant was required to include a minimization plan to ensure that reasonable steps were taken to only intercept information related to the investigation. Any information gathered about a U.S. citizen under FISA was of extremely limited use in any other law enforcement investigations and could only be used with the permission of the Attorney General.

The FISC was designed to prevent misuses of powers under FISA by mandating the judicial supervision of intelligence activities within the United States. "The FISC began life as a reform, an attempt to put a judicial check on executive abuse of wire-tapping and surveillance."[15] The majority of actions taken under FISA must get the approval of these special courts, theoretically creating a monitoring system to prevent inappropriate uses of FISA investigations. In practice, however, the judicial review provision in FISA has not provided much active oversight, as virtually no applications have been denied.[16] Between 1979 and 1999, FISC courts granted 11,883 FISA warrants and rejected none.[17] Furthermore, despite numerous different legal arguments being raised against FISA, courts "universally have found the statutory provisions constitutional."[18]

FISC hearings are nonadversarial, with only a Department of Justice presentation of the application for a warrant. The evidence, files, and records of the proceedings are sealed and remain secret to even the subject of the warrant in almost all cases.[19] As a result, it is possible for an individual, who is facing criminal charges based on information gathered with a FISA

Table 1
Selected Laws Related to Information Policy Affected by the Patriot Act & the Proposed Patriot II

| Patriot Act | Proposed Patriot II |
|---|---|
| Cable Communications Policy Act | Classified Information Procedures Act |
| Communications Act of 1934 | Electronic Communications Privacy Act |
| Computer Fraud and Abuse Act | Fair Credit Reporting Act |
| Electronic Communications Privacy Act | Federal Pen Register and Trap and Trace Statute |
| Fair Credit Reporting Act | Federal Wiretap Act |
| Family Education Rights and Privacy Act | Foreign Intelligence Surveillance Act |
| Federal Pen Register and Trap and Trace Statute | Freedom of Information Act |
| Federal Wiretap Act | National Security Act of 1947 |
| Foreign Intelligence Surveillance Act | Right to Financial Privacy Act |
| Right to Financial Privacy Act | USA Patriot Act |

warrant, to be unaware of the true nature of the charges and evidence. If an application for warrant were to be denied, it can be appealed by the Department of Justice for a review by a panel of FISC judges.[20] The highly secretive nature of the FISC hearings and their actions serves to complicate the study of the application of FISA.

## 3. FISA as modified by the Patriot Act

The Patriot Act makes changes to a wide range of statutes as diverse as the Antiterrorism and Effective Death Penalty Act,[21] the International Emergency Powers Act,[22] and the Trade Sanctions Reform and Export Enhancement Act.[23] A significant number of statutes altered by the Patriot Act relate directly to information policy (see Table 1), including the Communications Act of 1934,[24] the Computer Fraud and Abuse Act,[25] the Electronic Communications Privacy Act,[26] the Fair Credit Reporting Act,[27] and the Family Education Rights and Privacy Act,[28] and the Federal Wiretap Act.[29] Few statutes are as altered fundamentally by the Patriot Act as FISA.

The Patriot Act makes tremendous changes to FISA, though the ways in which the Patriot Act modifies FISA are clearer at this point than the impacts of these alterations over time. The exact meanings of many elements of FISA after the Patriot Act have created a large volume of legal scholarship devoted to trying to discern the meanings of the changes to FISA.[30] The Patriot Act alters many established laws by adding, removing, or changing words and sections, requiring that each piece of altered legislation "be reevaluated in the courts and reinterpreted by the agencies that must implement" these laws.[31] Further complicating the matter is that much of the wording of the Patriot Act is "disturbingly vague."[32] As a result, the ultimate extent of the impact of the Patriot Act on FISA remains somewhat uncertain.

The ways in which the Patriot Act modifies FISA regarding the collection and analysis of personal information, however, are clear (see Table 2). These changes alter investigations under FISA both of foreign citizens and of U.S. citizens. Some of the most significant relevant alterations by the Patriot Act to the collection and analysis of information under FISA are:

Table 2
Selected Impacts of the Patriot Act & the Proposed Patriot II on the Collection and Analysis of Personal Information under FISA

| Patriot Act (Section of Act) | Proposed Patriot II (Section of Draft) |
|---|---|
| Intelligence need only be a "significant" purpose of an investigation (§ 218) | Expanded definitions of "foreign powers" (§§ 101–102, 111) |
| Records now include any tangible thing that could contain information (§ 215) | Subject of investigation need not be violating federal law (§ 102) |
| The secrecy clause prevents discussion of investigations (§ 215) | Immunity for private entities that voluntarily provide information (§ 313) |
| Expanded use of roving wiretaps, pen registers, and trap and trace devices (§§ 206–207, 214, 216) | Simplified access for investigators to credit and financial information (§§ 126, 129) |
| Surveillance of electronic and voice mail communications (§§ 209–210) | Increased Attorney General powers to authorize warrantless FISA investigations (§§ 103–104) |
| Increased sharing of information from investigations between agencies and levels of of government (§ 203) | Prohibition against the use of encryption technologies (§ 404) |
| | Further expansion of information sharing from investigation between government agencies (§ 105) |

- **The expansion of the circumstances under which surveillance can occur.** Instead of requiring that gathering information about foreign intelligence activities be *the* purpose of a FISA investigation, it now needs to be a *significant* purpose—only one of a number of purposes. This change erases much of the distinction between the standards necessary to receive a court order for wiretaps or searches for FISA and for criminal investigations, allowing many FISA investigations to occur that simply would have been disallowed prior to the Patriot Act. Without this distinction, the original intent of FISA to protect the Fourth Amendment rights of U.S. citizens nearly evaporates, as the lower standards to get a court order and the far more intrusive methods usable under FISA can be applied in any investigation that might relate tangentially to foreign intelligence. The Patriot Act, however, does assert that investigations should not be conducted upon U.S. citizens solely on the basis of protected First Amendment activities. It is unclear how this provision can be applied meaningfully in light of the remaining provisions of the Patriot Act.
- **The greatly expanded definition of records that can be searched and obtained in FISA investigations.** Before the Patriot Act, the records that law enforcement agencies could collect and analyze under FISA were limited to specific pieces of information, such as hotel registrations, car rentals, and storage unit rentals. Under FISA as modified by the Patriot Act, investigators can collect and analyze a wide range of records that include "any tangible thing (including books, records, papers, documents, and other items)."[33] This difference is enormous, allowing for an investigation to tap into virtually any form of information in any format related to the subject of the investigation.
- **The secrecy clause.** Section 215 of the Patriot Act places a prohibition on disclosing any information about a FISA investigation, except as necessary to produce information that has been requested by a law enforcement agency using a FISA order. As a result,

individuals or organizations that have been ordered to produce records under FISA are unable to even acknowledge the existence of the order.

- **The expressed ability to conduct surveillance on electronic and voice mail communications.** While FISA focused previously on oral and wire communications, the Patriot Act allows investigations to also examine the contents of emails, as well as dialing, routing, and signaling information in emails. Voice mail messages are now types of communication that can be collected by law enforcement agencies under FISA.
- **The extension of the use of roving wiretaps.** Rather than applying to multiple communication devices regularly used by a suspect, a roving wiretap under FISA is now a multipoint wiretap, following the suspect to any wire or electronic communication device that they may use for any sort of communication. The Department of Justice does not have to demonstrate the suspect actually uses a particular device for the wiretap to occur.
- **The extension of the uses of pen registers and trap and trace devices in FISA investigations.** Rather than needing to demonstrate that the line or device in question has been actively used in communications related to intelligence activities, law enforcement agencies can now use pen registers and trap and trace devices with only a showing that some information related to an investigation might be obtained. The Patriot Act makes pen registers and trap and trace devices usable for both wire and electronic communications, where previously only wire communications had been specified. A pen register and trap and trace device order now follows the suspect throughout the United States. Previously, an investigator had to obtain a separate order for each district that the suspect entered.
- **The dramatic alterations to the relationships between agencies that collect intelligence information and other law enforcement organizations.** The Patriot Act alters FISA to allow information obtained in a FISA investigation to be shared with any government investigative agency, law enforcement agency, or attorney.

These changes are significant and in many ways re-envision FISA and how it functions.

Many surveillance activities considered historically beyond the scope of law enforcement in the United States were included in the Patriot Act.[34] "At the time of its passage, even many key legislators seemed to have little idea of the laws governing electronic surveillance, both before the Patriot Act and following it."[35] It is worth noting that little comment was made regarding these changes from members of the federal legislature. One of the few members of Congress to question these provisions, Senator Patrick Leahy, suggested that the Patriot Act "enters new and uncharted territory by breaking down traditional barriers between law enforcement and foreign intelligence."[36]

The differences in FISA as a result of the Patriot Act seem to be facilitating a considerable increase in FISA investigations. In 2002, there were a total of more than 1,000 FISA warrants issued, which is a dramatic increase from previous levels.[37] This proliferation of FISA investigations under the new Patriot Act modifications have the potential to generate criminal charges unrelated to intelligence gathering, both for subjects of FISA investigations and for the people who have interacted with those subjects. It is now conceivable that, as a result of the increased ability to share information gathered in FISA investigations with other law

enforcement agencies, that people who know subjects of FISA investigations could face criminal charges for unrelated (i.e., nonintelligence activities) that were discovered in the course of a FISA investigation, while the subject of the investigation faces no charges at all.

## 4. The future of FISA

The Department of Justice has been working to create an expansion of the Patriot Act that is entitled the Domestic Security Enhancement Act of 2003. The draft legislation, already commonly called "Patriot II," has not been introduced in Congress as of this writing, and the future of its provisions is unknown. Even if the draft legislation or any of its constituent provisions are never introduced into Congress, the content of the draft legislation is highly revealing about how the Department of Justice would like to continue to expand the scope of FISA investigations. Patriot II, which contains more than 100 proposed changes to existing law, would increase many government powers beyond the boundaries created by the Patriot Act (see Table 2). The Patriot II's provisions include the establishment of a DNA database of people (including U.S. citizens and resident aliens) with suspected ties to terrorism, the provision of complete immunity for federal agents who conduct illegal searches, and the forced expatriation of any U.S. citizen who helps a terrorist organization. The latter provision is especially curious, as it has no requirement of an expression of intent to renounce citizenship and no explanation of the threshold of cooperation necessary for this provision to apply. Unlike all other grounds for expatriation, such as obtaining citizenship in another country or joining a foreign army, this provision for presumptive loss of citizenship is neither intuitive nor the result of foreseeable action. For example, what happens to the individual who donates money to a seemingly legitimate charity, such as for an orphanage located in a nation that is an ally of the U.S., which is later discovered to be funneling money to terrorists?

Many of the provisions of Patriot II would further expand government intelligence gathering powers under FISA, making it even easier to obtain FISA orders and making searches and wiretaps under FISA even more expansive. As with the Patriot Act, the changes to FISA by Patriot II would change FISA investigations of U.S. citizens and of foreign citizens. Specific issues in the draft of Patriot II related to collecting and analyzing personal information under FISA include, but are not limited to:

- **An expansion of the definition of "foreign power" under FISA.** This provision would enable terrorist organizations and individuals or "sleeper cells" unaffiliated with a terrorist organization or foreign government to be treated as foreign powers for investigative purposes. Terrorist organizations and anyone thought to be affiliated with them, regardless of legal status or residence (including U.S. citizens), would not receive any of the FISA protections normally accorded to U.S. citizens.
- **Elimination of the requirement that the subject of a FISA investigation be engaged in activities that may be a violation of federal law.** Under Patriot II, FISA investigations could occur so long as the suspect might be gathering intelligence information of any sort for any reason. These changes increase greatly the number of people about

whom law enforcement agencies could collect and analyze personal information in FISA investigations.

- **Further sharing of information obtained in a FISA investigation.** Patriot II would alter the requirement that information obtained in a FISA investigation be shared only with the approval of the Attorney General. Under Patriot II, the sharing of information could be approved by other members of the Department of Justice, leading to much greater sharing of personal information between intelligence agencies and law enforcement organizations. Patriot II also contains provisions that would greatly simplify the procedures for getting judicial approval to collect personal financial information, including credit reports.
- **The provision of immunity from civil liability to any private entities, such as businesses, and their personnel that voluntarily provide personal information about customers to law enforcement agencies.** This provision would potentially provide law enforcement agencies with a means to collect tremendous amounts of personal information with none of the procedural protections that FISA would otherwise provide.
- **The creation of criminal sanctions for failure to comply with a FISA order.** This provision would provide the FISC with specific powers to punish individuals or organizations that fail to produce records or install pen registers or trap and trace devices in cooperation with a FISA investigation.
- **An expansion of the Attorney General's role in approving FISA investigations.** Patriot II would increase the Attorney General's powers to authorize FISA investigations without FISC approval by allowing for investigations up to a year when the surveillance is of communication between foreign powers. Patriot II also would strengthen the Attorney General's abilities to issue FISA investigations without approval of FISC by giving the Attorney General unlimited authority to authorize warrantless FISA investigations when Congress declares war. These provisions serve to further reduce the ability of the FISC to monitor intelligence-gathering activities.
- **A stated extension of electronic devices to include any multifunction devices.** Patriot II would make it clear that a FISA order would include interception of all types of communication functions of which a particular multifunction device, such as a Palm Pilot or a Blackberry, is capable. This provision would also permit any noncommunication information retrievable from a multifunction device to be collected and analyzed, regardless of whether the information is related to the communications.
- **The creation of a prohibition against the use of encryption technology to conceal criminal activity.** This provision would add a minimum of five years imprisonment to a conviction if encryption technology was "knowingly or willfully" used "to conceal any incriminating communication or information" related to a felony.[38] This provision, though with the stated intent to limit use of encryption technology in the commission of crimes, certainly has the potential to create a chilling effect on the use of standard computer security programs.

The passage of Patriot II, as the Department of Justice has drafted it, would expand the number and scope of FISA investigations, resulting in unprecedented levels of collection and

analysis of personal information in intelligence investigations. The provisions of Patriot II, even if they remain merely draft legislation, raise many interesting questions of great importance to information policy, particularly about the collection and analysis of personal information.

## 5. Key policy issues

As revealed by the discussion above, the modifications of FISA by the Patriot Act, and the proposed further modifications by Patriot II, have significant implications for information policy. One area in particular that raises many issues is the collection and analysis of personal information under FISA. It is not known exactly how much of an effect these issues will have, partially due to the relatively recent passage of the Patriot Act. Further, little is known about the applications of the Patriot Act, due to the secrecy clause and the secretive nature of the FISC courts, with much of the available information being what law enforcement agencies are willing to disclose.[39] There is no doubt, however, that the Patriot Act is currently having a significant impact on the collection and analysis of personal information under FISA and that this impact would substantially increase if the provisions of Patriot II were to become law.

Given the extensive range of issues raised about the collection and analysis of personal information by the Patriot Act, an article will only be able to focus on certain issues. This discussion is largely focused on the relevant issues related to electronic and transactional records, as these issues could have sizeable implications for many areas of information policy, including e-government. While much of the discussion of the Patriot Act's impacts focus on individual rights, many of the elements extend to groups (e.g., memberships, affiliations) and organizations (e.g., federal, state, and local government agencies; libraries; book stores; and nearly any organization that maintains records of some type).

### *5.1. E-government*

According to the Bush Administration, e-government "is about using technology to its fullest to provide services and information that is centered around citizen groups" and is a means through which to "eliminate redundant systems and significantly improve the government's quality of customer service for citizens and businesses."[40] In this view, e-government strategies are those with which government can achieve economies of scale through integrated systems that provide citizen-centered services and resources.

There are many forms of e-government that include:

- **Intra-agency,** in which units within an agency might engage in a variety of automated and online processes such as electronic purchasing/procurement;
- **Intragovernment,** in which an agency such as the Federal Bureau of Investigation and the Immigration and Naturalization Service could engage in a number of electronic data sharing and information services;
- **Intergovernment,** in which federal, state, and local agencies engage in the sharing of information and other services/resources. For example, law enforcement agencies have

integrated finger print databases and other investigative tools that cut across levels of government;

- **Intersector,** in which government agencies and nongovernmental entities share a variety of resources. For example, the Department of Defense and its various contractors engage in a number of electronic transactions, as do government agencies that outsource various functions (e.g., payroll). This also includes the range of sales, such as of surplus goods or seized items, by the government to citizens and businesses (http://www.firstgov.gov/shopping/shopping.shtml).
- **Government-citizen,** in which citizens engage in actual government services and/or resources electronically. Examples of such services/resources might be renewing a driver's license, accessing the Library of Congress' American Memory digital collection (http://memory.loc.gov/), and posting comments to agency requests for public comment (e.g., when the Federal Communications Commission issues a Notice for Proposed Rulemaking).

All of these forms of e-government are transaction-based. As such, they generate electronic records of each transaction –from website accesses to searches conducted on websites to requests for information to files viewed and downloaded, applications submitted, and so forth. In other words, every citizen's electronic interaction with government creates a record; so too would any intra- and interagency/government/sector interaction. There are several key questions that this situation forces:

1. Are these *records* under FISA as modified by the provisions of the Patriot Act?
2. To what extent does the Patriot Act's language regarding records (Section 215)
    a. negate government agency (federal, state, local) and nongovernment organizations privacy statements?
    b. require the reconsideration of government agency (federal, state, local) records management policies?
    c. require government agencies to begin maintaining and supplying records to law enforcement agencies that prior to the Patriot Act were either not maintained or were destroyed under various agency records disposal procedures?

The language regarding records and the authorities vested in law enforcement agencies is unclear and makes it difficult to provide answers to these questions with certainty.

Title 44 of the United States Code defines a record as:

> Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them.[41]

With this definition, web log and other e-government transactional records fall under the official definition of an agency record. The National Archives and Records Administration

(NARA) established in 1995 its *General Records Schedule 20* that provides guidance for agencies regarding electronic records that fall under the purview of administrative/transactional systems records. Schedule 20 states that agencies can delete/destroy "Electronic files and hard-copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use...when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes."[42] From this, NARA enables agencies to determine their own management process regarding system transaction-based files.

Moreover, it is important to note that records as defined above:

- Span formats and can include paper/print, electronic, and voice (e.g., voicemail);
- Reside in numerous technologies such as paper files, individual and networked computers, PDAs, and phones/phone systems; and
- Vary in ownership, as individuals can maintain their own records (i.e., on a personal computer), organizations can maintain records on individuals (i.e., Social Security contributions maintained by the Social Security Administration), and organizations can maintain work product records about the organization (administrative and operational).

Thus, the scope of records maintenance and issues that emanate from the authority vested in law enforcement agencies through the Patriot Act's records access rights (Section 215) are quite substantial. It is unclear at this time just how far law enforcement agencies can go in terms of records requests through the Patriot Act. Moreover, through the more restrictive FISA changes as discussed above, it is likely that the public will not know the extent to which law enforcement agencies are engaging in various records requests or from whom such requests are being made.

### *5.2. Nonagency records*

A number of organizations maintain the same types of records in similar formats as federal agencies –inventory, purchasing, personnel, and many others. For example, libraries maintain records of their holdings (inventory, known more often as an online public access catalog or OPAC) that they permit users to browse and access in a number of ways. Libraries also engage in a number of value-added services such as enabling users to borrow selected material from the library, request that a book be delivered to a particular library branch, issue a call for a book that is checked out at the current time, ask real-time online reference questions from librarians, or access electronic collections maintained by the library (e.g., digitized content, documents, etc.). Thus a library is a rich source of records such as:

- Holdings and collections contents;
- Browsing and searching the OPAC by patrons;
- Specific requests by patrons of material that the library holds (or might request through interlibrary loan);
- Specific material that a patron borrows from the library –a circulation record that also references the patron borrowing database maintained by libraries that may contain a substantial amount of information regarding the particular patron; and

- Patron use of online resources, particularly if such resources require the use of a userid/password (most often the patron's library card number).

The Patriot Act overrides pre-September 11, 2001 restrictions on law enforcement access to library records, one of many potential sources for records containing personal information.

In the case of libraries, there is evidence of law enforcement agencies visiting libraries and removing material from library holdings. In Ohio, for example, agents visited the Bluffton County Public Library and removed the *Allen County Hazardous Materials Emergency Plan* from a noncirculating collection. The agents replaced the document with a letter that informed patrons who wished to view the document that they could do so at the Allen County Homeland Security Office with "proper identification."[43] In this instance, agents reviewed the library's holdings records and deemed the material inappropriate for unrestricted public access. As a result of the secrecy clause of the Patriot Act, the number of occurrences of items being removed from library collections nationally is unclear.

### *5.3. Transaction logs*

Based on the combination of factors that include the increased provision of web-based services, the nature of systems log data and the ability to reveal personal information, Freedom of Information Act/Electronic Freedom of Information Act requests, and the administrative burden of maintaining various log files, federal agencies began developing records management policies regarding systems log files in general and web log files in particular. The Defense Technical Information Center (DTIC), for example, developed a web log policy in 1997 that required web site managers to destroy their web server log files after 60 days.[44] DTIC's current privacy and security policy still reflects this (see Fig. 1), but in light of the Patriot Act, it is not inconceivable that the Federal Bureau of Investigation (FBI), for example, could request from DTIC all of its web site transactional logs that would contain data as shown in Fig. 2. Another example of an agency privacy statement is that of the National Library of Medicine (NLM) (see Fig. 3). It contains similar language to the privacy statement of DTIC, but goes into more depth to include NLM's stance on cookies and the use/reuse of user-provided data.

More specifically, transaction logs of various types can contain any of the following data:

- Date/time of transaction;
- User identification, which may take the form of a specific user if a login is required or other identifying information such as an IP address from the initiating terminal (e.g., computer, PDA) which may or may not be linked directly to a specific user;
- Documents accessed and/or downloaded;
- Searches conducted, including the actual search string entered by the user;
- Hardware/software used by the user to access information such as operating system and browser type and version;
- Prior web location of users (referring site), through which can be traced the last website at which users were before entering an agency's website; and

*Privacy and Security Notice*

1. This World Wide Web (WWW) site is provided as a public service by the Defense Technical Information Center (DTIC®).

2. Information presented on this WWW site is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with the National Archives and Records Administration's General Records Schedule 20 *(Electronic Records)*.

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward them to us: bcporder@dtic.mil.

Source: http://www.dtic.mil/dtic/privacy.html

Fig. 1. Defense Technical Information Center (DTIC) Website Privacy Policy.

- Specific actions of a user for each access to a website/system (known as threading).

The above are only illustrative and other types of data are possible to collect through log files. In addition, by combining log files with other data sets, it is possible to determine, for example, the specific location from where a session initiated (through IP address registration data and other tracing techniques).

As a specific example, the authors accessed a number of different agency websites while conducting research for this article. For example, the authors accessed the White House website (http://www.whitehouse.gov); conducted searches for e-government policy documents, statements, and material; accessed selected documents; and downloaded some presentations made by various government personnel regarding federal e-government efforts. This research process generated, minimally, the following log transactions:

- Web site access;

**xxx.yyy.com - - [28/Jan/1997:00:00:01 -0500]**
**"GET /sitename/news/nr012797.html HTTP/1.0" 200 16704**
**Mozilla 3.0/www.altavista.digital.com**

**xxx.yyy.com (or 123.123.23.12)** -- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (....**com**) the requester is coming from a commercial address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

**[28/Jan/1997:00:00:01 -0500]** -- this is the date and time of the request

**"GET /sitename/news/nr012797.html HTTP/1.0"** -- this is the location of the requested file

**200** -- this is the status code - 200 is OK - the request was filled

**16704** -- this is the size of the requested file in bytes

**Mozilla 3.0** -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages

**www.altavista.digital.com** -- this indicates the last site the person visited, which indicates how people find this site
Requests for other types of documents use similar information. No other user-identifying information is collected.

Source: http://www.dtic.mil/dtic/privacy-sample.html

Fig. 2. Sample web log data.

- Referring website (from where we entered the site, for example, Google or FirstGov);
- Search string;
- Search results list and accessed links from the search hits;
- Specific page accesses; and
- Any documents downloaded.

Moreover, these log transactions contained the day/time, IP address, operating system, and other identifying information as described above.

In the case of citizen-government interaction, such transaction capturing would be multiplied by a factor of however many government-sponsored sites citizens access and use. Plus, user access and transaction records would be created across sectors and levels of government any number of times depending on how an agency created, maintained, operated, and managed its various systems. Finally, it may be the case that each citizen-government interaction generates a number of "behind the scenes" systems interactions that involve various intra- and interagency data sharing applications.

The National Library of Medicine (NLM) provides this Web site as a public service. We do **not** collect personal information about you when you visit our Web sites unless you choose to provide that information to us.

*Information Collected and Stored Automatically*

Of the information we learn about you from your visit to NLM Web sites, we store only the following: the IP address from which you access the Internet, the date and time, the Internet address of the Web site from which you linked directly to our site, the name of the file or the words you searched, and the browser used to access our site. This information is used to measure the number of visitors to the various sections of our site and identify system performance or problem areas. We also use this information to help us expand the coverage of the sites and to make the site more useful. NLM periodically deletes its Web logs.

*Cookies*

A "cookie" is a small file that a Web site transfers to your computer's hard disk allowing our server to "remember" specific information about your session. While visiting certain NLM sites you may occasionally encounter a Web page that employs cookies to make it easier to use the dynamic features of these Web pages. The cookie and the information about your session will be destroyed automatically shortly after you close your browser-it is not permanently stored on your computer. You can set your browser to disable cookies or prompt you before a cookie is accepted. If you do not want to receive cookies, you will still be able to use the NLM sites, but will be unable to use cookie-dependent features.

*Personally Provided Information*

If you choose to provide us with personal information by sending an email, or by filling out a form with your personal information and submitting it through our Web site, we use that information to respond to your message and to help us provide you with information or material that you request. If provided, personally identifiable information is maintained in a database that is regularly purged. Third party contractors may have access to this information in order to provide an initial response to your question or comment. These contractors are held to strict policies to safeguard the information and provide the same level of privacy protection as guaranteed by NLM. On occasion, we may conduct a study concerning the types of questions sent to us. These studies help us to improve our Web sites in order to make them more responsive to the needs of our users. We do not give, share, sell, or transfer any personal information to a third party unless required by law.

*Links to Other Sites*

Some NLM Web sites, such as MEDLINEplus, provide links to other Internet sites that provide health information. Once you link to another site, you are subject to the privacy policy of the new site.

*Security*

The U.S. Government maintains this site. For site security purposes and to ensure that this service remains available to all users, we use software programs to monitor traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Causing damage to federal computer systems is a violation of U.S. law and is subject to criminal prosecution in federal court. In the event of authorized law enforcement investigations, and pursuant to any required legal process, information from these sources may be used to help identify an individual.

Source: http://www.nlm.nih.gov/privacy.html

Fig. 3. National library of medicine website privacy statement.

## 6. Future impacts and challenges

To a large extent, many of the policy issues identified in relation to the collection and analysis of electronic and transactional records are hypothetical. There is no evidence to suggest that law enforcement agencies are requesting that agencies revise their privacy statements or records management practices, nor is there any evidence that shows that law enforcement agencies are visiting systematically various organizations and/or agencies to request that they maintain web log files, provide those log files to selected agencies, track specific users through particular systems, or insert various tracking capable cookies on user client computers.

The most pressing issue is, however, that the public does not actually know whether law enforcement agencies are engaging in any of these activities, and if they are, to what extent and in what setting they are doing so. Third party research (e.g., through surveys and other types of data collection) that attempts to answer such questions could potentially put both those who conduct the study and those who participate in the study in legal jeopardy, as the Patriot Act (Section 215) prohibits the public disclosure of law enforcement activities (e.g., a librarian cannot disclose that law enforcement officials visited the library or what transpired during such a visit).

Because of this secrecy clause, unless government agencies choose to disclose such information, it is likely the case that the public will never know the extent to which law enforcement agencies request records containing personal information from various organizations. As a result, the public will not know the extent to which agencies are engaging in information collection, analysis, and sharing activities within and across agencies as well as across levels of government and sectors.

Thus, it may be impossible to conduct a meaningful assessment of the impact and use of the various provisions in the Patriot Act and FISA as outlined above. The inability of policymakers and the public to conduct such assessments and policy analysis limits the application of the system of checks and balances, a key foundation of the U.S. Constitution.[45] Attempts at Congressional oversight of aspects of the Patriot Act and FISA have been marginalized, for example, by the Department of Justice's seeming resistance to respond to a set of questions posed by the Senate Judiciary Committee. In short, there appear to be inadequate checks and balances on the implementation and use of the various provisions in the FISA, and to some degree, Congress has been unwilling or unable to exercise such controls over the Department of Justice.

Perhaps the most important issue at hand is determining how to balance defense against terrorism and protection of individual civil liberties. The government must take adequate steps to protect its citizens from the threat of terrorist attacks, and it must be able to obtain information about potential terrorist activities to help minimize or stop such attacks. At the same time, the government must also protect individuals from excessive intrusion on their privacy and basic civil liberties as guaranteed in the Constitution and the Bill of Rights. Only recently have members of the media, individual citizens, and various organizations become alarmed at what they see as an erosion of civil liberties as a result of these Acts.

Given the extensive range of issues raised by the Patriot Act and its impacts on FISA, there is a need for Congress to reconsider the powers that they gave to the Executive Branch

as a result of the Patriot Act and its changes to FISA. This reassessment should consider implementing policy that:

- Develops procedures for more specific reporting on the use and impact of various provision of the Patriot Act and FISA (e.g., how the new powers under FISA are being employed);
- Provides meaningful Congressional oversight and some checks and balances on the implementation of FISA and Patriot Act provisions;
- Allows more and better public disclosure of instances where FISA and Patriot Act provisions have, in fact, been implemented;
- Considers the removal of the nondisclosure portion of Section 215 in the Patriot Act which makes it impossible to disclose that law enforcement agencies requested certain types of information; and
- Directs that independent study and research be done on the uses, impacts, and policy implications of these laws especially in terms of basic civil liberties as input to a possible revision and updating of the laws.

These are only a beginning set of criteria and concerns that should be considered by Congress in a review of the Patriot Act and its modifications of FISA. Such a review will likely not occur, however, until there is substantial and significant public outcry regarding the implementation of the provisions of these Acts –that is, when people in their daily lives are confronted directly with the FBI or other law enforcement agencies' use of these provisions.

## Notes

1. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S.A. Patriot) Act of 2001*. P.L. 107-56.
2. *Foreign Intelligence Surveillance Act of 1978*. 50 U.S.C. §§ 1801-1829, 1841-1846, 1861-1863.
3. *Domestic Security Enhancement Act of 2003*. Draft legislation generated by the Department of Justice. Available: http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf.
4. Relyea, H.C. (2002). Homeland security and information. *Government Information Quarterly, 19*(3), 213-224, p. 218.
5. Reylea, note 4 above, p. 219.
6. *U.S. Constitution*, article II, 1.
7. Birkenstock, G.E. (1992). The Foreign Intelligence Surveillance Act and standards of probable cause: An alternative analysis. *Georgetown Law Journal, 80*, 843-871. For a detailed tracing of the historical development of executive branch surveillance, *see* Banks, W.C. & Bowman, M.E. (2000). Executive authority for national security. *American University Law Review, 50,* 1-130.
8. Senate Committee on the Judiciary, *Foreign Intelligence Surveillance Act of 1977*, S. Rep. No. 604, 95th Congress, 1st Session 84 (1977).
9. Senate Committee on the Judiciary, note 8 above.

10. Birkenstock, note 7 above.
11. *United States v. U.S. District Court,* 407 U.S. 297 (1972).
12. Osher, S.A. (2002). Privacy, computers and the Patriot Act: The Fourth Amendment isn't dead, but no one will insure it. *Florida Law Review, 54,* 521-542. p. 532.
13. *U.S. Constitution,* Amendment IV. This Amendment guarantees the right of citizens "to be secure in their persons, houses, papers, and effects" and not subjected to "unreasonable searches and seizures." For a search warrant to be issued properly, it must be based on supportable "probable cause" and specifically describe the person, place, and things to be searched or seized. Unfortunately the framers of the Constitution did not thoroughly contemplate the implications of the Fourth Amendment beyond the parameters of criminal investigations, failing to consider issues related to political threats or technology. Banks & Bowman, note 7 above.
14. Senate Reporter No. 95-604, part 1, at 7.
15. Mayer, J.D. (2002). 9-11 and the secret FISA court: From watchdog to lapdog? *Case Western Reserve Journal of International Law, 34,* 249-252. p. 249.
16. Dycus, S. (2002). *National security law* (3rd ed.). New York: Aspen Law & Business.; Reimers, G.F., II. (2000). Foreign Intelligence Surveillance Act. *Journal of National Security Law,* 55-106.
17. Bradley, A.A. (2002). Extremism in the defense of liberty?: The Foreign Intelligence Surveillance Act and the significance of the U.S.A. Patriot Act. *Tulane Law Review, 77,* 465-493.
18. Rackow, S.H. (2002). How the U.S.A. Patriot Act will permit governmental infringement upon the privacy of Americans in the name of "intelligence" investigations. *University of Pennsylvania Law Review, 150,* 1651-1695, p. 1673. Cases that have upheld the constitutionality of FISA in spite of different legal arguments include *United States v. Duggan,* 743 F.2d 59 (2nd Cir. 1984); *United States v. Ott,* 827 F.2d 473 (9th Cir. 1987); *United States v. Pelton,* 835 F.2d 1067 (4th Cir. 1987); and *United States v. Johnson,* 952 F.2d 565 (1st Cir. 1991).
19. Robinson, G.H. (2000). We're listening! Electronic eavesdropping, FISA, and the secret court. *Williamette Law Review, 36,* 51-81.
20. Bradley, note 17 above. The FISC Appeals Court met for the first time in 2002, upholding the Patriot Act's reduction of mitigating measures to protect the rights of U.S. citizens in FISA investigations. United States Foreign Intelligence Surveillance Court of Review, *In re: Sealed Case No. 02-001* (November 18, 2002). Available: http://www.cadc.uscourts.gov/common/newsroom/02-001.pdf.
21. *Antiterrorism and Effective Death Penalty Act.* P.L. 104-132.
22. *International Emergency Powers Act.* 50 U.S.C. § 1702.
23. *Trade Sanctions Reform and Export Enhancement Act.* P.L. 106-387.
24. *Communications Act of 1934.* 47 U.S.C. §§ 151 *et seq.*
25. *Computer Fraud and Abuse Act.* 18 U.S.C. §§ 1030 *et seq.*
26. *Electronic Communications Privacy Act.* 18 U.S.C. §§ 2701 *et seq.*
27. *Fair Credit Reporting Act.* 15 U.S.C. §§ 1681 *et seq.*
28. *Family Educational Rights and Privacy Act.* 20 U.S.C. § 1232g.
29. *Federal Wiretap Act.* 18 U.S.C. §§ 2510 et seq.

30. For a wide range of stances about the meanings of the Patriot Act provisions related to FISA, *see*: Bradley, note 17 above; Dowley, M.F. (2002). Government surveillance powers under the U.S.A. Patriot Act: Is it possible to protect national security and privacy at the same time? *Suffolk University Law Review, 36,* 165-183; Etzioni, A. (2002). Implications of select new technologies for individual rights and public safety. *Harvard Journal of Law and Technology, 15,* 257-290; Evans, J.C. (2002). Hijacking civil liberties: The U.S.A. Patriot Act. *Loyola University of Chicago Law Journal, 33,* 933-990; Henderson, N.C. (2002). The Patriot Act's impact on the government's ability to conduct electronic surveillance of ongoing domestic communications. *Duke Law Journal, 52,* 179-209; Kerr, O.S. (2003). Internet surveillance law after the U.S.A. Patriot Act: The big brother that isn't. *Northwestern University Law Review, 97,* 607-673; Mayer, note 15 above; Murphy, P. (2002). An examination of the United States Department of Justice's attempt to conduct warrantless monitoring of computer networks through the consent exception of the Wiretap Act. *Connecticut Law Review, 34,* 1317-1352; Osher, note 12 above; Rackow, note 18 above; and Whitehead, J.W. & Aden, S.H. (2002). Forfeiting "enduring freedom" for "homeland security": A constitutional analysis of the U.S.A. Patriot Act and the Justice Department's anti-terrorism initiatives. *American University Law Review, 51,* 1081-1133.
31. Bradley, note 17 above, p. 485.
32. Osher, note 12 above, p. 539. One commentator notes that "there will most certainly be litigation about this bill in the near future." Murphy, note 30 above, p. 1319. Another describes Constitutional challenges to the Patriot Act as "inevitable." Bradley, note 17 above, p. 493.
33. Section 215.
34. Young, M.G. (2001). What big eyes and ears you have! A new regime for covert governmental surveillance. *Fordham Law Review, 70*(6), 1017-1109.
35. Kerr, note 30 above, p. 608.
36. Quoted in McGee, J. (2001, Nov. 4). An intelligence giant in the making; antiterrorism law likely to bring domestic apparatus of unprecedented scope. *Washington Post,* November 4, 2001, at A4.
37. CNN. (2003, March 25). Ashcroft accelerates use of emergency spy warrants: Move concerns some groups, lawmakers. Available: http://www.cnn.com. The total number FISA warrants in 2002, according to the Department of Justice, was 1,228. See Office of the Attorney General. (April 29, 2003). Letter to the director of the Administrative Office of the United States Courts. Available: http://www.fas.org/irp/agenyc.doj/fisa/2002rept.html.
38. Section 404.
39. For example, the FBI has admitted that it is actively using information gained from FISA investigations to pursue criminal prosecution of U.S. citizens who support some organizations. CNN. (2003, May 8). FBI intensifies investigations of Hezbollah, Hamas. Available: http://www.cnn.com.
40. Office of the White House. (2002). About E-gov. Available: http://www.whitehouse.gov/omb/egov/about_backgrnd.htm.
41. 44 U.S.C. § 3301.

42. National Archives and Records Administration. (1995, August). *General records schedule 20, Transmittal 7*. Washington, D.C.: National Archives and Records Administration. Available: http://ardor.nara.gov/grs/grs20.html.
43. "Homeland security agents pull Ohio libraries' haz-mat documents." (2003, April 7). *American Libraries Online*. Chicago, IL: American Library Association. Available: http://www.ala.org/al_onlineTemplate.cfm?Section=April_2003&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25175.
44. Harreld, H. (1998, July 13). GSA: Protect Web users' privacy. *Federal Computer Week*. Available: http://www.fcw.com/fcw/articles/1998/FCW_071398_563.asp.
45. Articles I, II, and III of the Constitution assign specific powers to each of the three branches, creating the separation of powers between the branches and establishing the system of checks and balances. The system of checks and balances is designed to be a "formula against tyranny." Kelly, J.M. (1992). *A short history of Western legal theory*. Oxford: Clarendon Press. p. 278. Sir Winston Churchill praised this system as the "cardinal principle of the American Constitution." Churchill, W. (2001 edition). *The great republic: A history of America* (W.S. Churchill, Ed). New York: Modern Library. (Original work published 1956-1958). p. 224.