

The Impact of the USA PATRIOT Act on Records Management

The impact of the USA PATRIOT Act on a particular records manager or records management program depends largely on the industry in which it operates

Cristine S. Martins, Esq. and Sophia J. Martins, Esq.

With 16 of its provisions, including several key ones, set to expire at the end of the year, the USA PATRIOT Act – enacted in 2001 in reaction to the worst terrorist attack in U.S. history – is the subject of much media attention and heated discussion. The controversy, however, has done little to explain the legislation’s impact on records and information management (RIM), dispel the myths surrounding what certain provisions of the act actually do, or shed light on how information professionals can comply with its provisions in their working environments.

While the PATRIOT Act does not necessarily have a direct impact on RIM in all industries, it has a profound impact in certain key sectors. Communications providers – including many cable, phone, and Internet

providers – as well as banking and financial institutions, libraries, and even precious metals, gems, and jewelry dealers have all had their business recordkeeping affected to some degree by this law.

Key Provisions

Among the provisions of the act that have had an impact on RIM in various

sectors of the U.S. economy are the following:

- *Section 204* – allows stored voice mail communications to be obtained by a search warrant rather than by having to meet the more stringent wiretap requirements. However, messages on an answering machine tape are not accessible through this provision.
- *Section 210* – expands the type of information that an electronic communications provider must disclose. This could include records of session times and duration, temporarily assigned network addresses, and means of payment, and it is not limited to investigations of suspected terrorist activity.
- *Section 211* – makes cable companies that provide telephone or Internet services subject to exist-

At the Core

This article

- ▶ examines key provisions of the USA PATRIOT Act that affect records management
- ▶ reviews recent court decisions and the way the act has been applied
- ▶ discusses how records and information management professionals can comply with the act in their working environments

ing laws that cover telecommunications providers and Internet service providers (ISPs). This directly affects records managers who work for cable providers, where the impact of the PATRIOT Act has been strongly felt.

- *Section 215* – allows the government to seek a court order to obtain personal records such as library, financial, phone, travel, and medical records. This is done by amending the Foreign Intelligence Surveillance Act and is based on a much lower probable-cause standard than that for a regular warrant. Section 215 will expire at the end of 2005 unless renewed by Congress and is one of the most highly publicized in the media.
- *Section 216* – applies telephone monitoring laws to Internet traffic, including e-mail, Web page, and Internet protocol addresses. This applies to computers just about everywhere, including public libraries, which has made this a major talking point in the media and a hotly contested issue.
- *Section 314* – provides for information sharing among financial institutions and between the government and financial institutions. Part of the tougher anti-money laundering rules, this provision allows a broader spectrum of communication than ever before.
- *Section 319(b)* – amends Section 5318 of Title 31 of the U.S. Code to include a “120-hour rule.” This provision requires that a financial institution must produce records relating to “any account opened, maintained, administered, or managed in the United States” upon request from an appropriate federal banking agency. This section also provides instruction on maintaining foreign bank records.
- *Section 326* – requires that financial institutions verify a person’s identi-

ty when that person seeks to open an account and to maintain records of the information used in such identification, amending Section 5318 of Title 31, U.S. Code.

- *Section 505* – allows the government to seek personal records with no judicial approval through the

The ALA has issued a resolution against the PATRIOT Act and offers information on its Web site on how libraries can respond to requests for information under the act.

use of an administrative subpoena. This provision does not expire at the end of 2005 and has been used many times since 2001. It was, however, struck down as unconstitutional by a New York Federal District Court in September 2004. The case is currently awaiting appeal.

Key Provisions as They Relate to Specific Sectors

Sections 215 and 216 – Libraries

The opposition to Sections 215 and 216 is quite vocal. The American Library Association (ALA) has come out strongly against government access to library loan or library computer information. The ALA has issued a resolution against the PATRIOT Act and offers information on its Web site on how libraries can respond to requests for information under the act. Through its Office for Intellectual Freedom, the group offers free legal advice for libraries served with PATRIOT Act information requests that do not have their own legal counsel.

However, it is unclear if these sections have ever been used to gain access to library loan records. In fact, there is no case where Section 215 was used to access an individual’s library records. Because this provision is due to expire at the end of 2005 unless renewed by Congress, it will undoubtedly be in the news as the debate over renewal heats up.

Section 314 – Financial Institutions

The banking industry is greatly affected by PATRIOT Act provisions relating to stricter anti-money laundering regulations and reporting duties. In September 2002, the U.S. Treasury Department issued new rules effectively implementing the act’s new requirements. Among them were provisions for federal law enforcement agencies investigating terrorist or money-laundering activity to submit an information request to the Treasury Department. In turn, Treasury can solicit information from financial institutions. The investigating agency needs only “credible evidence” of terrorist or money laundering activity.

The financial institution that receives an information request from the Treasury Department has an obligation to search its records and respond. Under the final regulations, the search encompasses the following

New Bills Aim to Restore Rights under USA PATRIOT Act

Sen. Russ Feingold (D-Wis.) has introduced three bills aimed at protecting civil liberties that he says were taken away by the USA PATRIOT Act, the anti-terrorism measure passed shortly after September 11, 2001.

Feingold – who was the only senator to vote against the PATRIOT Act – reintroduced the Library, Bookseller, and Personal Records Privacy Act, the Reasonable Notice and Search Act, and the Computer Trespass Clarification Act. All are intended to fix specific portions of the PATRIOT Act that Feingold criticized before voting against it in October 2001.

The Library, Bookseller, and Personal Records Privacy Act is designed to protect the privacy of citizens with no connection to terrorism by more carefully defining the ability of the government to obtain library, bookstore, medical, and financial records and other sensitive materials under the PATRIOT Act while still allowing the FBI to follow up on legitimate terrorism leads.

The Reasonable Notice and Search Act revises the PATRIOT Act authority to delay notice of the execution of search warrants – so-called "sneak and peak" provisions – and requires the attorney general of the United States to submit to Congress every six months a report concerning all of the requests for delayed notice warrants.

The Computer Trespass Clarification Act limits the amount of warrantless surveillance of authorized computer users allowed under a provision of the PATRIOT Act that was designed to permit computer owners to seek the assistance of the government in combating unauthorized hackers.

"These bills are appropriate fixes to a number of the USA PATRIOT Act's most problematic provisions, which members of both parties are working to correct," Feingold said. "The civil liberties we enjoy as Americans define our nation as the freest on earth, and I will continue to work to protect those freedoms while keeping our country safe from terrorism."

At the time of this writing, all three bills had been read twice and referred to the Committee on the Judiciary.

On April 5, 2005, Feingold also joined Senators Larry Craig (R-Idaho), Dick Durbin (D-Ill.), Mike Crapo (R-Idaho), John Sununu (R-N.H.), and others in reintroducing the Security and Freedom Ensured (SAFE) Act. This act also seeks to amend several controversial provisions of the USA PATRIOT Act, including placing limitations on the use of surveillance, the issuance of search warrants, and the compelled production of personal records. There is strong bipartisan support for the act, which, its sponsors say, will safeguard the rights of Americans without impeding law enforcement's ability to fight terrorism.

for each named suspect:

- any current account maintained
- any account maintained during the preceding year
- any transaction conducted on the suspect's behalf
- any funds transmittal that the financial institution records as required under law or that it records and maintains electronically in which the suspect was either transmitter or recipient during the preceding six months

In addition, the regulations require that each financial institution maintains adequate procedures to preserve confidentiality. Where adequate procedures to protect, preserve, and ultimately produce the information are expected, records management comes into play. Records managers in the banking sector are very familiar with the multitude of recordkeeping requirements already placed on them by several federal agencies and, as a result, most financial institutions already have well-developed records management policies and systems. However, since the PATRIOT Act was enacted, the requirements have been further tightened, and all financial institutions should already have reviewed their policies and procedures to ensure compliance with the Treasury Department's new rules.

The PATRIOT Act also specifies, in Section 314(b), that financial institutions may share information with one another for the purpose of identifying terrorism or money laundering suspects. According to Carl A. Fornaris and Alan B. Horn's *GT Alert* article, "New USA PATRIOT Act Regulations that Apply to Banks, Broker Dealers, and Other Financial Institutions," information sharing is allowable provided that

- the financial institution submits a notice to the Treasury Department, effective for a one-year period, as prescribed by the new regulations

- before sharing information, the financial institution takes “reasonable steps” to verify that the other financial institution with which it intends to share information has submitted the same notice to the Treasury Department
- the financial institution maintains the shared information as confidential
- the financial institution submits a new notice for information after the anniversary of the filing of the initial notice

If they have followed the rules on filing notice of information sharing and maintained the shared information as confidential, both financial institutions are protected from liability for sharing information or for failing to notify the entities about whom information was shared.

The act, while creating some new standards and requirements, does not appear to have created the same controversy in this industry or in the media, although some articles on the new identification requirements have been published.

One criticism of the PATRIOT Act’s changes to bank recordkeeping has been that it will cost smaller institutions more time and money to update their systems to comply with the new rules. Actually, this might be true no matter the size of the institution. Citigroup, for example, reportedly had to resort to using pen and paper to record additional customer identity information required under the PATRIOT Act when its computer systems were not updated in time for the act’s required implementation deadline.

Section 505 – Communications Industry

ISP records pose challenges to Section 505 – which allows the gathering of personal records from a third party without disclosing that a search of the records took place – and has implications for records managers in the communications industry. In a case

involving records of a personal account identified only as “John Doe” that were subpoenaed from an ISP in order to preserve the Federal Bureau of Investigation’s examination, U.S. District Judge Victor Marrero declared Section 505 unconstitutional. He asserted that Section 505 violates the Fourth Amendment because it deters

In addition to adjusting some retention policies to comply more easily with information requests, some companies have had to add staff to keep up with Section 505 subpoenas...

judicial challenge to government searches. Marrero also found that, by banning disclosure of the release of the records to the account holders, Section 505 also violates the First Amendment as a prior restraint on free speech.

Although this case involved an ISP, the provision could also be applicable

to phone records and other personal records kept about individuals by third parties. Voice over Internet protocol (VOIP) technology may fall under this heading as well as other kinds of electronic communications.

The final disposition of this case could greatly impact the number and type of government subpoenas that records managers in the communications sector receive and may have implications for other industry sectors as well.

One effect that has already been seen is that more subpoenas mean are increasing workloads for records managers. Cable companies that offer Internet services, in particular, have had to change recordkeeping practices in order to comply with the new standards. This is principally because of differences in the way that requests for cable TV subscriber versus cable Internet subscriber information requests are handled under the PATRIOT Act. The amount and kind of information required to be provided is much greater for Internet subscriber data than it is for cable TV subscriber information. Keeping the two realms separate is a challenge for records managers responding to information requests.

In addition to adjusting some retention policies to comply more easily with information requests, some companies have had to add staff to keep up with Section 505 subpoenas as well as with information requests made under older laws.

Title III – Jewelry Industry

As part of the act’s anti-money laundering goal, Title III includes amendments to the anti-money laundering provisions of the Bank Secrecy Act (BSA). It defines what a “dealer” in precious metals, stones, or jewels is and what records such entities are responsible for keeping. With the potential for precious commodities to be used in money laundering activities to fund terrorism, dealers must create policies

and procedures to curtail these activities and to ensure compliance with the reporting requirements of the BSA, as amended by the Patriot Act.

Management Response to the PATRIOT Act

Some companies have responded to increasing legislation – The PATRIOT Act, the Sarbanes-Oxley Act, and others – by forming separate compliance departments or groups, often within the existing financial department. Sometimes these compliance groups work well with the existing records management groups and sometimes not. Corporate culture and the function of the groups involved are influential factors in applying any new law to an existing records management program.

New legislation often precipitates a review of existing systems conducted by the records management staff, internal compliance groups, or outside consultants. Whatever the situation, existing records policies and systems must be analyzed in light of the new laws that may affect them. Documentation of program analysis and changes to the existing records management policies and/or systems should be as detailed as possible.

The PATRIOT Act's Future

Much of the publicity surrounding the PATRIOT Act relates to sections that appeal to public interest, such as the search of library loan or computer information without the library patron's knowledge or consent. While important and widely discussed in the media, this is a relatively small issue as it relates to the act as a whole and has never been used in a real-world case in the years since the act was passed.

Many of the more complex, industry-specific issues, such as increased access to banking and Internet data, have not been discussed in any real detail in the media. Only time will tell whether the long-term effects of the PATRIOT Act are desirable or not.

Court cases, such as the one in New

York dealing with the specifics of Section 505, will clarify the limits and boundaries of the act further and should be watched carefully with an eye toward compliance by records managers in affected sectors of industry. If the New York District Court finding that Section 505 is unconstitutional is upheld, potentially all administrative subpoenas issued under Section 505 would be null and void. If, however, the higher court overturns the lower court's findings, Section 505 will continue in force.

It is also possible that the higher

court might find some middle ground that could change the way Section 505 is used without invalidating it completely.

In addition, Congress could step in to enact a new version of Section 505 that might be better tailored to pass constitutional scrutiny while allowing for the broader power the administrative subpoena currently enjoys.

Whatever the outcome, records managers in the communications industry should keep a careful eye on developments in order to best comply with the final decision on Section 505. ■

Cristine S. Martins, Esq., is an attorney, librarian, and President of Martins Consulting, a New York-based information management firm. She is co-author of The Sarbanes-Oxley Act: Implications for Records Management, published by ARMA International. She may be contacted at cris@crismartins.com.

Sophia J. Martins, Esq., is an attorney and former public library director. She is currently a reference law librarian at Touro Law Center in Huntington, New York. She may be contacted at sophiam@tourlaw.edu.

References

American Library Association. "Resolution on the USA PATRIOT Act and Related Measures that Infringe on the Rights of Library Users." Available at www.ala.org (accessed 1 March 2005).

Doyle, Charles. "Libraries and the USA PATRIOT Act." CRS Report for Congress. 26 February 2003. Available at www.ala.org/ala/washoff/woissues/civilliberties/theusapatriotact/CRS215LibrariesAnalysis.pdf (accessed 1 March 2005).

Fornaris, Carl A. and Alan B. Horn. "New USA PATRIOT Act Regulations That Apply to Banks, Broker Dealers, and Other Financial Institutions." *GT Alert*. September 2002. Available at www.gtlaw.com/pub/alerts/2002/horna_09d.asp (accessed 1 March 2005).

Harlin, Kevin. "Banks Drafted to Fight Terror." *Times Union*. 5 October 2003.

Maiello, Michael. "Citigroup's Low-Tech USA PATRIOT Act Solution." *Forbes.com*. 8 September 2003. Available at www.forbes.com/2003/09/08/cz_mm_0908citi.html (accessed 1 March 2005).

Patel, Purva. "Security: 9/11 Law Burdens Smaller Banks." *Detroit Free Press*. 6 October 2003. Available at www.freep.com/money/business/bank6_20031006.htm (accessed 1 March 2005).

Powell, Eileen Alt. "USA PATRIOT Act Affects Financial Industries, Customers." *New Haven Register*. 6 October 2003.