Order Code RL31289

CRS Report for Congress
Distributed by Penny Hill Press http://pennyhill.com

The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government

Updated March 4, 2002

Marcia S. Smith, Jeffrey W. Seifert, Glenn J. McLoughlin, and John Dimitri Moteff
Resources, Science, and Industry Division

The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government

Summary

The September 11, 2001 terrorist attacks prompted congressional action on many fronts, including passage of the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56. The Act is broadly scoped, and some of its provisions may affect Internet usage, computer security, and critical infrastructure protection.

In the area of computer security, the Act creates a definition of "computer trespasser" and makes such activities a terrorist act in certain circumstances. The Act enables law enforcement officials to intercept the communications of computer trespassers and improves their ability to track computer trespasser activities. It also codifies some elements of U.S. critical infrastructure policy articulated by both the Clinton and George W. Bush Administrations to ensure that any disruptions to the nation's critical infrastructures are minimally detrimental.

Although the Act does not explicitly address electronic commerce (e-commerce), many of the law's provisions may impact it. In particular, Title III responds to concerns that more can be done to prevent, detect, and prosecute international money laundering and the financing of terrorism. Over time, these provisions may affect e-commerce broadly, and electronic fund transfers specifically.

Electronic government (e-government) could be affected by the Act in both positive and negative ways. The intense focus on improving data collection and information sharing practices and systems may contribute to the establishment of government-wide technical standards and best practices that could facilitate the implementation of new and existing e-government initiatives. It could also promote the utilization of secure Web portals to help ensure the data integrity of transactions between the government and citizens and business. However, concern about potential abuses of data collection provisions could dampen citizen enthusiasm for carrying out electronic transactions with the government.

The Act provides law enforcement officials with greater authority to monitor Internet activity such as electronic mail (e-mail) and Web site visits. While law enforcement officials laud their new authorities as enabling them to better track terrorist and other criminal activity, privacy rights advocates worry that, in an attempt to track down and punish the terrorists who threaten American democracy, one of the fundamental tenets of that democracy—privacy—may itself be threatened.

Because of the controversial aspects of some provisions in the Act, particularly regarding privacy, Congress and other groups are expected to monitor closely how the Act is implemented.

Contents

Introduction 1

Computer Security and Critical Infrastructure Protection 2
- Provisions of the USA PATRIOT Act Affecting Computer Security 2
- Provisions Affecting Critical Infrastructure Protection 5
- Policy Issues 6

Electronic Commerce 7
- Provisions of the USA PATRIOT Act Affecting Electronic Commerce . . . 7
- Policy Issues 8

Electronic Government 11
- Provisions of the USA PATRIOT Act Affecting Electronic Government . 11
- Policy Issues 13
  - Knowledge Management 14
  - Ensuring Information Security 14
  - Privacy 15

Internet Privacy: Law Enforcement Monitoring of Internet Usage 16
- Provisions of the USA PATRIOT Act Affecting Internet Privacy 16
- Policy Issues 18

The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government

Introduction

The September 11, 2001 terrorist attacks prompted congressional action on many fronts, including passage of the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. The Act is broadly scoped,[1] and some of its provisions may affect use of the Internet, computer security, and critical infrastructure protection.

The legislation initially passed the Senate (96-1) as S. 1510 on October 11, 2001. The House passed H.R. 2975 (337-79) on October 12. A compromise bill, H.R. 3162, passed the House (under suspension) on October 24 and the Senate (98-1) on October 25. The President signed it into law on October 26 (P.L. 107-56).

The implementation of the Act will be carefully scrutinized. While law enforcement officials heralded the passage of what they regard as necessary provisions for counteracting terrorists and other criminals, civil liberties groups urged caution in passing a new law in an emotionally charged environment. During debate, some Representatives raised concerns about the process used to bring the bills to the floor. In the House, for example, the version of H.R. 2975 as reported from the Judiciary Committee on October 11 (H. Rept. 107-236, Part 1) was replaced by the text of a new bill, H.R. 3801, for the purposes of debate.[2] H.R. 3801 was very similar, but not identical, to S. 1510 as it had passed the Senate hours earlier. Hence, some Representatives felt they had insufficient time to review the legislation they were being asked to vote on. Among the changes in H.R. 3801 was an extension of the sunset period on several of the electronic surveillance provisions from 2 years to 5 years. Some Members had argued for a short sunset period, maintaining that the changes in the law were being made hurriedly. In light of this history, it appears that oversight of the Act's implementation will be of considerable interest to Congress and a broad range of interest groups.

This report summarizes the potential effect of the Act on electronic privacy, security, commerce, and government, and identifies issues that are arising.

---

[1]For a detailed legal discussion of all of the provisions of the Act, see CRS Report RL31200, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, by Charles Doyle, December 10, 2001.

[2]H.R. 3801 was adopted as an amendment in the nature of a substitute to H.R. 2975.

Computer Security and Critical Infrastructure Protection[3]

Every day, persons gain access (or try to gain access) to other people's computers without authorization to read, copy, modify, or destroy the information contained within—webpages are defaced, unwanted messages and pictures are conveyed, information (or money) is stolen, communications are jammed and services denied. The list of perpetrators includes juveniles, disgruntled (ex)employees, criminals, competitors, politically or socially motivated groups, and agents of foreign governments. For the purposes of this report, people who engage in such activities will be called computer trespassers (adopting a term which the USA PATRIOT Act defines, as explained below). The damage computer trespassers can inflict, either knowingly or unwittingly, often goes beyond merely being a nuisance and in most cases rises to the level of a federal crime (pursuant to 18 U.S.C. 1030). It is also conceivable that under certain conditions such actions could be considered a terrorist act or rise to the level of endangering national security by threatening the functioning of the country's critical infrastructure.

For the most part, law enforcement agencies seem to have had adequate tools to investigate, prosecute and penalize these offenses. One area where officials have sought improvement for some time, however, is in streamlining their ability to track computer trespassers, both in real time or after the fact. Prior to passage of the USA PATRIOT Act, procedures required investigators to request court orders, warrants, subpoenas, etc. from a multitude of jurisdictions, since most computer trespassers will route their communications around the world. While the USA PATRIOT Act is directed primarily to improve the ability of the government to detect, prevent, and respond to the kinds of terrorist attacks experienced last September and October, a number of the provisions affect the government's law enforcement surveillance and investigatory powers more generally. Those that directly and indirectly affect the ability of the government to investigate, prosecute, and perhaps deter computer trespassers, whatever their intent, are listed below.

Provisions of the USA PATRIOT Act Affecting Computer Security

- Section 105 expands upon the U.S. Secret Service's National Electronic Crime Task Force Initiative. The U.S. Secret Service has been leading a New York Electronic Crime Task Force that has been held up as a model of success for investigating a variety of electronic crimes, ranging from "cloning" cell phones to denial-of-service attacks against on-line trading companies.[4] The task force includes experts from other government agencies as well as the private sector. Section 105 directs the Director of the Secret Service to develop a national network of such task forces.

---

[3]Written by John Dimitri Moteff, Specialist in Science and Technology Policy, CRS Resources, Science, and Industry Division.

[4]See: The Cyber-Mod Squad Set Out After Crackers. Computerworld, June 19, 2000, pp. 44-45.

- Section 202 and Section 217 clarify that law enforcement officials may seek permission to intercept electronic communications of "computer trespassers." Section 202 adds 18 U.S.C. 1030 (computer fraud and abuse) offenses to the list of offenses for which the Attorney General, or other designated officials, may authorize a request for a court order to intercept targeted communications. Section 217 defines a "computer trespasser" as someone "who accesses a protected computer[5] without authorization and thus has no reasonable expectation of privacy in any communication to, through, or from the protected computer." Section 217 also specifies the conditions under which the communications of a computer trespasser may be intercepted. Those conditions are: the owner or operator of the protected computer authorizes the interception; the person acting under color of law is lawfully engaged in an investigation; the person acting under color of law has reasonable grounds to expect the content of the computer trespasser's communication is relevant to the investigation; and the interception acquires only the trespasser's communications within the invaded computer.[6] Prior to the Act, the statute was less explicit in specifying the terms under which a computer trespasser's communications could be intercepted.

- Section 210 expands the information that law enforcement officials may obtain (with appropriate authorization) from providers of electronic communications service or remote computing services regarding a subscriber or customer of those services. The information may now include a subscriber's or customer's means and source of payment. The language is also modified to include information more clearly related to Internet use (e.g. session times and temporarily assigned network addresses). These changes are to improve the ability of law enforcement officials to track the activity and identity of suspects concerning a wide range of offenses, including terrorist activities and those of computer trespassers.

- Section 211 clarifies that in the deregulated telecommunications environment, cable providers that also provide communication services are governed by the same statutes as other electronic communication providers in regard to interception of communications, disclosure of customer records, and application of pen registers and trap and trace devices.[7] Prior to deregulation,

---

[5]A protected computer is defined in 18 U.S.C. 1030 (as amended by the USA PATRIOT Act) as a computer exclusively for the use of a financial institution or the U.S. government, or used by or for either of those, if the offense affects that use; any computer used in interstate or international commerce or communications; or a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

[6]Earlier versions of the bill would have allowed the trespasser's communications to be intercepted wherever they were directed. The Act's more restricted language was a compromise position.

[7]A pen register allows the user to code or decode the dialing, routing, addressing, or signaling information transmitted by an instrument or facility. In terms of computer security, it allows

(continued...)

cable providers followed different rules. Therefore, law enforcement officials now have the same surveillance and investigatory powers in regard to cases involving cable internet services. Information regarding a subscriber's selection of video programming, however, continues to be governed separately.

- Section 216 modifies the authorities relating to use of pen registers and trap and trace devices. As a result of Section 216, a single court order authorizing the use of a pen register or trap and trace device can be used to apply those devices to any computer or facility anywhere in the country. Prior to the Act, authorization had to be obtained in each jurisdiction where the devices needed to be applied. Also, the availability of this authority with respect to computer communications was unclear. It was generally thought that these devices could only be used on telephone equipment.

- Section 220 allows a single court with jurisdiction over the offense under investigation to issue a warrant allowing the search of electronic evidence anywhere in the country. Prior to this, the warrant needed to be issued by a court within the jurisdiction where the information resided.

- Section 808 adds certain computer fraud and abuse offenses to the list of violations that may constitute a federal crime of terrorism. The new provisions apply to: anyone who knowingly accesses a computer without authorization and obtains classified information; and, anyone who knowingly causes the transmission of a program, information, code, or command, and as a result intentionally causes damage to a protected computer. The inclusion of these offenses in the definition of a federal crime of terrorism in Section 2332b(g)(5)(B) relates primarily to who has investigatory authority over the offenses (the Attorney General, in this case). However, by virtue of cross-references in other parts of the Act, including these offenses in the definition of terrorism also affects: the extension of their statute of limitations (Section 809 of the Act); post-release supervision of someone convicted of these offenses under certain circumstances (Section 812 of the Act); and, applicability of the racketeering statutes (Section 813 of the Act). According to Section 809, should these computer offenses result in or create a foreseeable risk of death or serious bodily injury, there is no statute of limitations. Under similar conditions, Section 812 could lead to life-time post-release supervision. The cross-reference to racketeering statutes gives law enforcement officials more tools with which to prosecute computer trespassers.

- Section 814 increases the penalties for certain computer fraud and abuse offenses. The penalty for a first offense of causing the transmission of a program, information, code or command that intentionally causes damage to a protected computer increases from 5 years to 10 years. The penalty for a

---

[7](...continued)
the law enforcement official to identify the address to which a computer trespasser is sending a message. A trap and trace device allows the user to identify the source of a wire or electronic communication. In terms of computer security, it allows the law enforcement official to identify the address from which the computer trespasser is sending a message.

second such offense or a second offense of intentionally gaining unauthorized access to a protected computer and, as a result, recklessly causing damage is increased from 10 years to 20 years. Also, it is now an offense to attempt to commit these offenses. This section also redefines "damage." Damage is now defined as: i) loss to one or more persons during any 1-year period aggregating at least $5,000 in value; ii) modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; iii) physical injury to any person; iv) a threat to public health or safety; v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security. Item "v" is new. Also, item "i" is rewritten. Prior to this, it was not clear whether the $5,000 threshold was per person affected or the total value of damages caused to all people affected. The new language clarifies that it is the latter. Finally, the Section also modifies the language in 18 U.S.C. 1030 regarding civil suits. This includes new language that says victims suffering damages resulting from an offense listed in section 1030 may not sue under this section for negligent design or manufacture of hardware, software, or firmware. This is a broad immunity that protects manufacturers should any design or manufacture problem lead to damages, including, one would expect, security vulnerabilities which are a common problem in trying to make information systems more secure.

- Section 816 authorizes the expenditure of $50 million to develop and support regional cybersecurity forensic capabilities. There are already a number of computer forensic laboratories established. This would encourage the establishment of additional ones. In addition to assisting federal authorities to investigate and prosecute computer crimes, the laboratories are to train federal, state and local officials in computer forensics, to assist state and local officials in investigating and prosecuting state and local computer offenses, and to share expertise and information on the latest developments in computer forensics.

Provisions Affecting Critical Infrastructure Protection

Since information networks (including the Internet) are considered critical infrastructures, the above sections are also relevant to this discussion. However, there are two additional provisions that affect the protection of other critical infrastructures more generally.

- Title VII is entitled Increased Information Sharing for Critical Infrastructure Protection. However, the lone section in the Title (Section 701) really addresses a set of illegal activities much broader than attacks on critical infrastructures. There exists, within the Department of Justice, a Bureau of Justice grant program that helps establish information sharing systems between federal, state, local and non-profit entities for the purpose of identifying, targeting, and removing criminal conspiracies that cross jurisdictional boundaries. These information sharing systems are to include a number of capabilities, such as rapid information retrieval and systematized updates. Section 701 would add that the information sharing system be secure. The

Section also adds multi-jurisdictional terrorist conspiracies to the list of activities tracked by the information sharing system.

- Section 1016 puts into statute elements of the critical infrastructure policy that have been articulated by both the Clinton and the Bush Administrations.[8] That is, to ensure that any physical or virtual (i.e. computer-induced) disruption of the nation's critical infrastructures be rare, brief, geographically limited, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States. The section defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The Section also establishes a National Infrastructure Simulation and Analysis Center. The Center is to support related counter-terrorism, threat assessment, and risk mitigation activities. In particular the Center is to model and analyze the large-scale complexity of critical infrastructures, and use those models and analyses to train authorities in incident response, to recommend changes in system designs or protections, and to provide recommendations to policymakers. The Center is to receive data from state and local governments and the private sector to assist in developing its models. The Section also authorizes the appropriation of $20 million through the Department of Defense's Defense Threat Reduction Agency to support activities at the Center.

Policy Issues

Many of the provisions related to the surveillance and investigatory powers of law enforcement have raised concerns within the privacy and civil liberties communities. These are discussed in more detail later in this report. Some of the provisions do not necessarily grant law enforcement officials more power in practice, but clarify that those powers exist and put them on a sounder basis. Many observers believe that the most important changes affecting law enforcement officials are those provisions allowing for nationwide warrants, court orders, etc. to facilitate the tracking of computer trespassers. In the case of investigating offenses after the fact, these provisions may save more resources than time. However, in cases where officials are trying to track computer trespassers in real time, time is of great importance and the provisions should be that much more effective. In regard to increasing the penalties for computer trespassers, there is some debate about whether doing so will have the hoped for deterrent effect.[9] Others suggest that, deterrence

---

[8](1) The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, May 22, 1998. (2) President George W. Bush, Executive Order 13231—Critical Infrastructure Protection in the Information Age. Federal Register. Vol. 66. No. 202. October 18, 2001.

[9]See: Attorneys Debate Making Cybercrime Laws Tougher. Computerworld, November 20, 2000, p. 16.

aside, increasing penalties better reflects the seriousness of the offenses.[10] The Act primarily strengthens law enforcement's tools to police what many believe is a network ill-designed for security. Aside from the provision to develop a National Infrastructure and Analysis Center, none of the provisions relate to providing for or ensuring more secure systems.

Electronic Commerce[11]

The convergence of computer and telecommunications technologies has revolutionized how we get, store, retrieve, and share information. Commercial transactions on the Internet, whether retail business-to-customer or business-to-business, are commonly called electronic commerce, or "e-commerce." Since the mid-1990s, commercial transactions on the Internet have grown substantially.[12] A January 2002 study by the Pew Internet and American Life Project found that overall, 29 million American shoppers made purchases on-line during the fourth quarter of 2001, spending an average of $392, up from $330 in the fourth quarter of 2000. A quarter of all Internet users did some shopping on the Internet last year, up from one-fifth of Internet users in 2000.

Provisions of the USA PATRIOT Act Affecting Electronic Commerce

The USA PATRIOT Act does not address e-commerce directly;[13] however Title III of the Act, International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, addresses concerns of policymakers that, in the wake of the September 11 terrorist attacks, more can be done to prevent, detect, and prosecute international money laundering and the financing of terrorism. Title III contains three subtitles with provisions that address international money laundering, voluntary disclosure by U.S. banks of suspicious financial activity, and the bulk smuggling of currency across U.S. borders and counterfeiting.

- Subtitle A, International Counter Money Laundering and Related Measures, has among its many provisions requirements that U.S. financial institutions do more to prevent and detect money laundering actions.. It requires that

---

[10]Ibid.

[11]Written by Glenn J. McLoughlin, Specialist in Technology and Telecommunications Policy, CRS Resources, Science, and Industry Division.

[12] For statistics and other data on e-commerce, see: CRS Report RL30435, *Internet and E-Commerce Statistics: What They Mean and Where to Find Them On the Web*, by Rita Tehan. Other sources include: [http://www.idc.com], [http://www.abcnews.go.com], [http://www.forrester.com], [http://www.emarketer.com], and [http://www.cs.cmu.edu]. It is important to note that some measurements of e-commerce, particularly data reported in the media, have not been verified.

[13]It is important to note that while no provisions of the USA PATRIOT Act of 2001 explicitly address e-commerce, many provisions throughout the law may have an impact on e-commerce. See: CRS Report RL31200, op. cit., for a discussion of the complete law.

financial institutions provide greater monitoring and due diligence concerning certain foreign financial activities, including wire transfers, interbank accounts, and correspondent accounts involving foreign financial institutions.

- Subtitle B, Bank Secrecy Act Amendments and Related Improvements, amends previous law by revising immunity and liability provisions for financial institutions which might disclose suspicious activities and persons to the federal government, including those which may constitute an "underground" system of financial transactions.

- Subtitle C, Currency Crimes and Protection, provides new penalties for bulk cash smuggling in and out of the United States as well as counterfeiting activities.

Many of the provisions in Title III do not go into effect until regulations are promulgated.[14]

Policy Issues

Upon signing the USA PATRIOT Act, President Bush said "this legislation gives law enforcement officials better tools to put an end to financial counterfeiting, smuggling and money laundering." The President added: "We're making it easier to seize the assets of groups and individuals involved in terrorism."[15] Among the many provisions in Title III, law enforcement officials point to two of the Act's objectives—establishing new standards and requirements for increased cooperation by financial institutions when responding to federal government requests for information; and extending the federal jurisdiction over non-U.S. financial institutions in money laundering—as particularly vital to U.S. counter-terrorism efforts.[16]

However, some have raised concerns that Title III (as well as other provisions) may have a broader scope than many of its supporters intend.[17] While many are concerned that the civil liberties of individuals may be compromised if law enforcement officials extend their reach, Title III may also have implications for a wide range of e-commerce activities. It is unlikely that the Act will immediately affect retail e-commerce (e.g., online catalogue orders) or business-to-business e-commerce (e.g., the use of the Internet for inventory ordering and management). While these

---

[14]See: CRS Report RL31208, *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, Title III of P.L. 107-56,* by M. Maureen Murphy.

[15]President Signs Anti-Terrorism Bill. Office of the Press Secretary. The White House. October 26, 2001.

[16](1) Attorney General Ashcroft Directs Law Enforcement Officials to Implement New Anti-Terrorism Act. Office of Public Affairs. U.S. Department of Justice. Washington, D.C. October 26, 2001. (2) Support for Anti-Terrorism Act of 2001 (Letter to Attorney General John Ashcroft). International Association of Chiefs of Police. Alexandria, VA. October 2, 2001.

[17]Philon, Roger. First Thoughts on the New Money Laundering Act. Current Issues. The Cato Institute. Washington, D.C. December 6, 2001. [http://www.cato.org]

forms of e-commerce are growing very rapidly, to date they have not been identified as being particularly susceptible to misuse by terrorists. Retail e-commerce and business-to-business e-commerce require verifiable information between parties that may include names, addresses, credit card numbers and other information, and can be traced relatively easily. However, some observers have not ruled out terrorists using existing e-commerce exchanges to facilitate their activities in the future.[18]

The more common method of using e-commerce for illicit and terrorist purposes is through financial transactions. For example, the terrorists involved in the September 11 attacks reportedly used wire transfers routinely to fund their activities in the United States. Most money transfers, even relatively small amounts transferred as money orders by firms like Western Union, Money Gram, and other smaller companies, are done electronically. There is no need to establish a bank account or fill out credit reporting forms, identification requirements are minimal, a money wire firm's outlet may be located in a supermarket or drugstore and staffed by store employees, and it can take less than fifteen minutes to send money around the world.[19] The USA PATRIOT Act addresses wire transfers and money orders by requiring, among other provisions, the registration of all money order agents by December 31, 2001, and increasing the criminal penalties for those who knowingly conduct or assist in transferring money that is intended to promote or support an illegal activity. These provisions not only cover the physical transfer of money for these purposes, but electronic transfers as well.[20]

Larger financial institutions which conduct much of their business electronically—and therefore are part of the e-commerce business sector—are also affected by the USA PATRIOT Act. Among the provisions affecting large multinational financial corporations are increased authority for U.S. law enforcement officials to gain access to institutions' records and data bases; due diligence by U.S. financial institutions concerning money laundering by non-U.S. persons; enhanced standards for correspondent accounts held by U.S. banks; and prohibition of correspondent accounts with shell banks (banks which have no physical presence in their chartering country).[21]

Critics contend that the USA PATRIOT Act will not prevent nor prohibit the types of activities that terrorists engaged in before September 11. While U.S. money order and wire transfer firms will have greater reporting responsibilities and tighter restrictions under the Act, the sheer volume of transactions, many under $3,000, is enormous—in 2000, Western Union alone did 89 million wire transfers of money. Particularly in the Middle East a significant amount of money is transferred or

---

[18]For two views on how extensive the reach of the USA PATRIOT Act may be, see: (1) Philon, Roger. Two Kinds of Rights Current Issues. The Cato Institute. Washington, D.C. December 6, 2001 [http://www.cato.org]. (2) Chidi, George, Jr. 'Patriot Act' Aids Law Enforcement. Network World, November 5, 2001. [http://www.nwfusion.com/news/2001/1105carrier.html].

[19]Timmons, Heather. Terrorist Money By Wire. Business Week, November 5, 2001, p. 94.

[20]Subtitle A.

[21]CRS Report 31208, op cit, p. 4.

exchanged by *hawla*, a remittance system outside of, and running parallel to, the banking system. Whether the USA PATRIOT Act can be effectively applied to terrorists' use of *hawla* is not clear. Some also question whether the time and cost to track large portions of electronic commerce conducted through *hawla* will prove to be an efficient use of government and private sector resources.[22]

Others contend that large U.S. financial institutions may also expend significant time and resources to comply with the Act without providing any assistance in the war against terrorism. According to Ellen Zimiles, a partner in KPMG's forensics practice, a large U.S. bank spends $10 million per year to fight money laundering—and the Act may add to that cost, as well as adding new costs for brokers, insurers, and others connected with the financial industry.[23] According to another expert, a U.S. bank typically has one million to five million ATM transactions daily, and 100,000 wire transactions per day. U.S. financial institutions will likely have to address how they will balance increased security provisions, broader access to their accounts by law enforcement officials, and ensuring customers that the privacy and integrity of financial accounts will not be compromised by compliance with the Act.[24]

Abroad, many U.S. financial institutions and multinational organizations routinely transfer currency internally and externally, often crossing national borders. These institutions and corporations often engage in routine short-term lending or borrowing to balance accounts or to finance projects. There are several established mechanisms and procedures for these transactions. The London Interbank Offering Rate (LIBOR) is an overnight lending rate by which multinational corporations electronically borrow or lend money to balance their accounts. The LIBOR is set by the largest banks, and the transactions are usually made with "Eurodollars."[25] These transactions occur on a daily basis and range in the trillions of dollars. There is no indication that any U.S. institutions using the LIBOR to settle accounts have aided or abetted terrorist activities. Still, these transactions could fall under the USA PATRIOT Act. If U.S. law enforcement officials begin to examine accounts, or even seize funds, under the Act, how might multinational corporations react– may they even attempt to avoid compliance to the Act? Will foreign banks and governments acquiesce to U.S. actions?

---

[22]Timmons, Heather. Western Union: Where the Money Is—In Small Bills. Business Week, November 26, 2001, p. 40.

[23]McNamee, Mike, et. al. A Hard Slog for Financial 'Special Forces.' Business Week, November 26, 2001, p. 39-41.

[24]Ibid.

[25]"Eurodollars" are not the same as the new European currency, the Euro. Eurodollars are those dollars which are outside of the United States and used in business transactions, usually in denominations of $100,000 to $1,000,000. The term comes from the 1940s, when large amounts of U.S. dollars were pumped into European economies as part of the Marshall Plan. These dollars were so attractive as a medium for conducting business that they became a part of the European, then global, process of conducting business. See: Ritter, Lawrence S., William L. Silber, and George F. Udell. *Principles of Money, Banking and Financial Markets. (Ninth edition)*. Reading, MA, Addison-Wesley, 1997, pp. 116-117; 137-138; 220-221; 573.

Still, it is important to note that, to date, most (if not all) of the concerns raised by critics, other than those of costs of compliance, have been hypothetical. There have been no reported widespread law enforcement intrusions into financial institutions' databases, nor have there been any reported e-commerce or electronic fund transfers disruptions linked to the war on terror since the Act was signed into law. The events of September 11 resulted in a fundamental change in the way the United States views its defense and security. Over time, Title III of the USA PATRIOT Act may affect e-commerce broadly, and electronic transfers specifically. How this Act will affect law enforcement and security efforts in the Internet Age and its actual impact on privacy rights and data integrity remains to be seen.

Electronic Government[26]

A significant component of many of the initiatives regarding the USA PATRIOT Act specifically, and homeland security generally, involves the use of information technology to enhance existing government processes or create new ones. Some of these initiatives may contribute to the growing effort to implement e-government projects by both Congress and the Bush Administration through enhanced data sharing and greater confidence in the security and reliability of the networks. Other initiatives may inadvertently create obstacles by restricting access to information flows and reducing privacy protections.

Provisions of the USA PATRIOT Act Affecting Electronic Government

There are a number of provisions in the USA PATRIOT Act that are relevant to e-government interests. E-government involves using information technology, and especially the Internet, to improve the delivery of government services to citizens, business, and other government agencies.[27] Most of these provisions are independent of one another, reflecting the often disparate and disconnected nature of e-government initiatives. Many of the provisions in the USA PATRIOT Act related to e-government focus on government-to-government (G2G) relationships, both within the federal government, and between federal, state, local, and foreign governments. Fewer of the provisions focus on government-to-business (G2B) or government-to-customer (G2C) interactions. The relevant provisions can be found in titles III, IV, VII, IX, and X, and are briefly discussed in turn.

- Section 361 supercedes Treasury Order Number 105-08, establishes the Financial Crimes Enforcement Network (FinCEN) in statute, and charges the

---

[26]Written by Jeffrey W. Seifert, Analyst in Information Science and Technology Policy, CRS Resources, Science, and Industry Division.

[27]For a broader discussion of e-government concepts and issues, see CRS Report RL31057, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, Jeffrey W. Seifert; CRS Report RL30745, *Electronic Government: A Conceptual Overview*, by Harold C. Relyea; and CRS Report RL31088, *Electronic Government: Major Proposals and Initiatives*, by Harold C. Relyea.

bureau with, among other things, establishing a financial crimes communication center to facilitate the sharing of information with law enforcement authorities. This section also requires FinCEN to maintain a government-wide data access service for information collected under anti-money laundering reporting laws, information regarding national and international currency flows, as well as information from federal, state, local, and foreign agencies and other public and private sources.

- Section 362 seeks to enhance cooperation between the federal government and the banking industry by directing the Security of Treasury to establish a "highly secure network" in FinCEN to enable financial institutions to file reports required by the Bank Secrecy Act and receive alerts regarding suspicious activities electronically.

- Section 403 emphasizes interagency data sharing and technology standards development. It authorizes appropriations to enable the State Department and the Immigration and Naturalization Service (INS) to access the Federal Bureau of Investigation's (FBI) National Crime Information Center's Interstate Identification Index (NCIC-III) database. It also directs the National Institute of Standards and Technology (NIST) to "develop and certify a technology standard that can be used to verify the identity of persons applying for a United States visa or such persons seeking to enter the United States pursuant to a visa for the purpose of conducting background checks, confirming identity, and ensuring that a person has not received a visa under a different name or such person seeking to enter the United States pursuant to a visa."

- Section 405 directs the Attorney General to carry out a study on enhancing the FBI's Integrated Automated Fingerprint Identification System (IAFIS) to improve screening of foreign nationals applying to enter the country.

- Section 413 authorizes the State Department to share, with other countries, information from its visa outlook database for the purpose of investigating or preventing crimes and to "deny visas to persons who would be inadmissable to the United States."

- Section 414 directs the Attorney General to fully implement an "integrated entry and exit data system for airports, seaports, and land border ports of entry," with a particular focus on the use of biometric technology and tamper-resistant documents.

- Section 701 authorizes the Office of Justice Programs to expand information sharing with state and local law enforcement agencies and nonprofit organizations to fight multi-jurisdictional criminal conspiracies. It also calls for the establishment of a secure information sharing system.

- Section 906 emphasizes the potential consolidation of data collection responsibilities by requiring the Attorney General, the Director of Central Intelligence, and the Secretary of the Treasury to submit a report to Congress "on the feasibility and desirability of reconfiguring the Foreign Terrorist Asset Tracking Center and the Office of Foreign Assets Control of the Department

of Treasury in order to establish a capability to provide for the effective and efficient analysis and dissemination of foreign intelligence relating to the financial capabilities and resources of international terrorist organizations." The report is also to examine "to what extent the capabilities and resources of the Financial Crimes Enforcement Center of the Department of the Treasury may be integrated into the capability contemplated by the report."

- Section 1008 also focuses on the potential for data sharing between agencies. It calls for a study directed by the Attorney General in consultation with the Secretary of State and the Secretary of Transportation "on the feasibility of utilizing a biometric identifier (fingerprint) scanning system, with access to the database of the Federal Bureau of Investigation Integrated Automated Fingerprint Identification System, at consular offices abroad and at points of entry into the United States to enhance the ability of State Department and immigration officials to identify aliens who may be wanted in connection with criminal or terrorist investigations in the United States or abroad prior to the issuance of visas or entry into the United States."

- Section 1009 focuses on potential information sharing between federal agencies and airlines. It directs the FBI to study "the feasibility of providing airlines access via computer to the names of passengers who are suspected of terrorist activity by federal officials."

- Section 1012 focuses on enhancing the cooperation between federal and state officials to limit the issuance of licenses to transport hazardous materials in commerce (hazmat licenses). It allows states to request the Attorney General to conduct a background check on applicants using "relevant international databases through Interpol" and other means.

- Section 1015 also focuses on intergovernmental relationships by expanding the scope and lengthening the authorization of appropriations of the Crime Identification Technology Act (P.L. 105-251), which allows the Office of Justice Programs to issue grants to state and local entities to develop integrated information and identification systems.

Policy Issues

The e-government policy implications associated with the USA PATRIOT Act are centered around three primary issues; knowledge management/data sharing, information security, and privacy.

Knowledge Management. Knowledge management (KM) has been defined as "the process through which an enterprise uses its collective intelligence to accomplish its strategic objectives."[28] As the above summary of the relevant provisions suggests, enhanced data sharing and knowledge management techniques

---

[28]Barquin, Ramon C., Alex Bennet, and Shereen G. Remez (eds.). *Knowledge Management: The Catalyst for Electronic Government.* Vienna, VA: Management Concepts, Inc., 2001, p. 5.

are expected to play a significant role in homeland security efforts. Several of the provisions focus on improving access and the sharing of centralized databases by federal, state, and local law enforcement agencies. Some of the provisions also seek to establish a more fully integrated database system for processing and tracking the granting of visas, as well as the entry and exit of foreign nationals in the United States. In many cases these provisions are designed to rectify the problems associated with having multiple, incompatible, and sometimes overlapping databases, which have been identified as one of the contributing factors to the difficulties law enforcement and intelligence agencies have had tracking suspected terrorists.[29] Just as knowledge management has been recognized as an important component of improved homeland security, its proponents argue that knowledge management could play a significant role in e-government initiatives generally. Knowledge management efforts involving e-government have so far encountered a variety of obstacles.[30] Some of these obstacles include creating the appropriate technical and support infrastructure, achieving user "buy-in," and managing the development and use of specialized information. Some have suggested the creation of the position of chief knowledge officers (CKOs) at the agency, department, and/or federal level to facilitate the execution of specific knowledge-intensive projects and support larger government reform efforts. The success of knowledge management/data sharing efforts in the homeland security area could affect the adoption of these proposals.

Ensuring Information Security. Heavy reliance on centralized databases with wider access by more actors (both governmental and non-governmental) will require careful attention to data protection and the authentication of users. One way this may be achieved is through the use of public key infrastructure (PKI) encryption systems.[31] PKI systems are generally considered the most reliable means to ensure the security of online transactions.[32] However, implementing a PKI system can be a very difficult, time consuming, and expensive process. Moreover, in the case of federal e-government projects, the PKI systems used by different departments and agencies would need to be interoperable in order to realize the efficiencies hoped for, and convenience necessary, to achieve the desired citizen usage levels. So far, no such standards have been established.

The challenge of establishing a large scale PKI system raises many issues. Some of these include the lack of federal interoperable standards, the feasibility of

---

[29]Porteus, Liza. FBI Official Laments Restrictions on Information Sharing. Government Executive Magazine, January 23, 2002. [http://www.govexec.com/dailyfed/0102/012302td1.htm].

[30]Caterinicchia, Dan. Cultural Changes Trumps Technology. Federal Computer Week, January 7, 2002, p. 21.

[31]A PKI is a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. Certificate and registration authorities can be managed either by third party organizations or through in-house personnel.

[32]Robinson, Brian. PKI: A Necessary Evil. Federal Computer Week. September 3, 2001. [http://www.fcw.com/geb/articles/2001/sep/geb-tec2-09-01.asp].

implementation, and high costs.[33] First, the lack of federal interoperable standards raises the question of who would be responsible for developing and promulgating such standards. The National Institute of Standards and Technology (NIST) often works with industry to facilitate and develop technical standards and measurements. However, it is currently unclear what role NIST would play in developing any PKI standards. Assuming the acceptance of the PKI approach, it is also unclear whether the federal government should work to create a standard for its own use, or if it should rely on the development of an industry standard, which may take longer to emerge. Second, large scale, full-featured PKI systems are not common, raising questions regarding the scalability of the technology and the resources needed to accomplish the task. Implementation of such a system would require policy makers to decide if the federal government has sufficient expertise and resources to create a large scale PKI system in-house, or if it will need to be outsourced to one or more private contractors. Third, the largely uncharted nature of such an undertaking and the high costs of PKI systems generally, raises concerns for budget planning and oversight. Proponents of a government-wide PKI system maintain that if these issues can be adequately addressed, the creation of a single government-wide PKI system could promote the utilization of secure Web portals to ensure the data integrity of transactions between the government and citizens and business.

Privacy. In contrast to the two previously discussed issues, the implications of the USA PATRIOT Act on privacy could have a negative effect on e-government initiatives. Surveys have shown that the loss of privacy as a result of e-government is a significant concern among citizens.[34] As mentioned in the earlier section on computer security, the Act expands the type of information that may be collected by law enforcement officials from providers of electronic communications services or remote computing services. It also allows for the issuance of nationwide search warrants to facilitate the tracking of computer trespassers. Concerns about potential misuse of these data collection provisions could dampen citizen enthusiasm for carrying out electronic transactions with the government.

Internet Privacy: Law Enforcement Monitoring of Internet Usage[35]

Until the September 11, 2001 terrorist acts, the Internet privacy debate focused on consumer privacy issues sparked by the collection, use, and dissemination of

---

[33]General Accounting Office, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277, February 2001, p.42.

[34]The Council for Excellence in Government. E-Government: The Next American Revolution, 2001, p. 27.

[35]Written by Marcia S. Smith, Specialist in Aerospace and Telecommunications Policy, CRS Resources, Science, and Industry Division.

personally identifiable information by commercial Web site operators.[36] The practices of law enforcement agencies in monitoring the activities of individuals as they use the Internet for electronic mail (e-mail) or visiting Web sites was an important, but less visible, issue. Congress addressed it primarily in the context of ensuring that the Federal Bureau of Investigation (FBI) did not overstep its authority in using a software program called Carnivore (later renamed DCS 1000).[37] With a court order, the FBI could install Carnivore on the equipment of an Internet Service Provider (ISP) to monitor a suspect's Internet activity, which raised concern about whether the software was sufficiently precise to avoid monitoring the activity of other ISP customers and hence impinging on their privacy.

While Congress remains interested in overseeing the FBI's use of Carnivore, the September 11 terrorist attacks sharpened the debate over how to strike a balance between law enforcement's need to investigate criminals and protecting what most citizens believe to be their "right" to privacy.[38] Congress included provisions in the USA PATRIOT Act that make it easier for law enforcement to monitor Internet activities. Also, many ISPs that opposed law enforcement monitoring of their customers' Internet activity reportedly have been quite willing to assist law enforcement in its search for e-mail and other Internet evidence relating to the attacks.[39]

Provisions of the USA PATRIOT Act Affecting Internet Privacy

Title II of the Act, Enhanced Surveillance Procedures, includes provisions that affect monitoring of Internet activities.

- Section 210 expands the scope of subpoenas for records of electronic communications to include records commonly associated with Internet usage, such as session times and duration.

- Section 211 clarifies that cable companies offering Internet services are subject to 18 U.S.C. ch. 119 (Wire and Electronics Interception and Interception of Oral Communications), 18 U.S.C. ch. 121 (Stored Wire and Electronic Communications and Transactional Records Access), and 18 U.S.C. ch. 206 (Pen Registers and Trap and Trace Devices) in their provision of those services. Cable companies had sought, in particular, to clarify their obligations with regard to release of personally identifiable information about subscribers and whether they were required to notify the subscriber that the information had been requested by a governmental entity as required under the 1992 Cable

---

[36]See CRS Report RL30784, *Internet Privacy: An Analysis of Technology and Policy Issues*, by Marcia S. Smith, for a discussion of those issues.

[37]For information on Congress' actions relative to Carnivore/DCS 1000, see CRS Report RS20035, *Internet Privacy: Overview and Pending Legislation*, by Marcia S. Smith.

[38]See CRS Report RL30671, *Personal Privacy Protection: The Legislative Response*, by Harold Relyea, for a discussion of the evolution of privacy rights in the United States.

[39]Matthews, William. Security Trumps Privacy in New Order. Federal Computer Week, September 24, 2001, p 40.

Act. Under this section, no notification is required, but disclosure specifically does not include a subscriber's video programming choices.

- Section 212 *allows* ISPs to divulge records or other information (but not the contents of communications) pertaining to a subscriber if they believe there is immediate danger of death or serious physical injury or as otherwise authorized, and *requires* them to divulge such records or information (excluding contents of communications) to a governmental entity under certain conditions. It also allows an ISP to divulge the *contents* of communications to a law enforcement agency if it reasonably believes that an emergency involving immediate danger of death or serious physical injury requires disclosure of the information without delay.[40]

- Section 216 adds routing and addressing information (used in Internet communications) to dialing information, expanding what information a government agency may capture, as authorized by a court order, using pen registers and trap and trace devices.[41] The content of any wire or electronic communications is excluded. A court shall enter an ex parte order permitting installation and use of a pen register or trap and trace device if it finds that an attorney for the government or a state law enforcement or investigative officer has certified that the information likely to be obtained is relevant to an ongoing criminal investigation. Law enforcement officials must keep certain records when they use their own pen registers or trap and trace devices and provide those records to the court that issued the order within 30 days of expiration of the order. To the extent that Carnivore-like systems fall with the new definition of pen registers or trap and trace devices provided in the Act, that language would increase judicial oversight of the use of such systems.

- Section 217 allows a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from a protected computer under certain circumstances.

- Section 220 allows for nationwide search warrants for e-mail instead of requiring separate search warrants for each jurisdiction in which the e-mail may be located, such as at the ISP's location rather than where a crime was committed.

- Section 224 establishes a 4-year sunset period (until December 31, 2005) for many of the Title II provisions, but among the sections excluded from the sunset are Sections 210, 211, and 216.

---

[40]Legislation (H.R. 3482) is currently pending before Congress that would amend this section of the USA PATRIOT Act to lower the threshold of the circumstances under which ISPs may divulge the contents of communications, and to whom they may divulge the contents. For information on current legislative status on that or other Internet privacy legislation, see CRS Report RS20035.

[41]See footnote 6 for an explanation of pen registers and trap and trace devices.

Policy Issues

As noted, the challenge for policy makers is balancing the needs of law enforcement with the desire by the public to maintain its privacy. In the wake of the terrorist attacks, the public appears more willing to make sacrifices in the privacy arena to protect the country against further attacks and bring the perpetrators of the September 11 assault to justice. Criticism of the USA PATRIOT Act from a privacy standpoint has been relatively muted, possibly because of the perception that the public is willing to accept such measures at this time. An October 2001 Harris Poll found that 63% of Americans favored monitoring of Internet discussions and chat rooms, and 54% favored monitoring cellphones and e-mail.[42]

However, privacy advocates worry that, in this emotionally charged climate, Congress is passing legislation that it later will regret. Groups such as the American Civil Liberties Union (ACLU), Center for Democracy and Technology (CDT), Electronic Privacy Information Center (EPIC), and Electronic Frontier Foundation (EFF) urge caution, fearful that, in an attempt to track down and punish the terrorists who threaten American democracy, one of the fundamental tenets of that democracy—privacy—may itself be threatened. The ACLU issued a press release[43] on October 24 stating that it was deeply disappointed with the House passage of H.R. 3162, and, after the bill cleared Congress, vowed to monitor its implementation.[44] CDT's Executive Director said on October 25 that "This bill has been called a compromise but the only thing compromised is our civil liberties."[45] Among CDT's concerns is that Section 216, which is not subject to the sunset provision, allows law enforcement officials to collect information about Internet usage without what CDT considers to be meaningful judicial review.[46]

There are other privacy issues, too. Peter Swire, who served as privacy counselor at the Office of Management and Budget during the Clinton Administration, worries that the Act does not include sufficient provisions to deal with potential abuses by law enforcement of the new authorities granted in the Act.[47] Federal Trade Commission (FTC) Commissioner Orson Swindle has suggested that ISPs relook at their privacy policy statements in the wake of passage of the Act, particularly with regard to ISPs' new authority under Section 212 to voluntarily disclose information.[48]

---

[42]Schwartz, John. Seeking Privacy Online, Even as Security Tightens. New York Times, November 11, 2001, p. 10 Bu.

[43]ACLU press release October 26, 2001 [http://www.aclu.org/news/2001/n102401a.html].

[44]ACLU press release October 24, 2001 [http://www.aclu.org/news/2001/n102601a.html].

[45]CDT press release October 25, 2001 [http://www.cdt.org/press/011025press.shtml].

[46]CDT Policy Post 7.11, October 26, 2001. Available at [http://www.cdt.org].

[47]Swire, Peter. If Surveillance Expands, Safeguard Civil Liberties. Atlanta Journal-Constitution op-ed, October 21, 2001, p 2D. In its final form, the Act includes enhanced sanctions and other measures designed to reduce the risk of abuse, e.g., sections 223 (civil liability), 224 (sunset of some provisions), and 1001 (review of the Department of Justice).

[48]FTC's Swindle: PATRIOT Act May Require Updated ISP Privacy Policies. (continued...)

The FTC oversees how businesses, including ISPs, adhere to their privacy policies. Mr. Swindle also pointed out that it is his understanding that the law does not cover Web sites, only ISPs. He wondered if an online bookseller received many requests for books on, for example, how to make bombs or fly an airplane, "and the name of the purchasers reflected one or another ethnic group, would that be alarming under concern for terrorism? ... It would seem to me that common sense would say that would be alarming but they're not covered by this."[49] John Kamp, an attorney with Wiley, Rein & Fielding, commented that the definitions in the Act were murky and Web sites might be covered, but that "It is clear that this law wasn't designed to go there."[50]

The question of definitions is raised by others, including EFF. In particular, EFF cites the lack of definitions of "content" of e-mails that cannot be retrieved without a warrant, and the term "without authority" in the definition of a computer trespasser.[51] Packets of data that comprise e-mail messages may contain both content and non-content information (such as routing information). The Act allows law enforcement officials access to non-content information, but not to content. Thus this definition could be quite important. Regarding computer trespassers, Section 217 defines a computer trespasser as a person who accesses a protected computer without authorization, but it does not include a person with an existing contractual relationship with the owner or operator of the computer. EFF wants that term to mean only individuals who intentionally break into computers with which they have no relationship.

Some ISPs express satisfaction that guidance issued by the Justice Department implementing the USA PATRIOT Act clarifies that ISPs may use their own tools to obtain information required by law enforcement officials rather than rather than being required to allow the FBI to install software such as DCS 1000. EarthLink executive David Baker called it a "silver lining in what many otherwise describe as a cloud...."[52]

Like the ACLU, most of the privacy advocate groups assert that they will closely monitor how law enforcement officials implement the Act and try to ensure that the law is not misused. Congress may conduct oversight of the Act's implementation, both from the standpoint of the value of providing law enforcement officials with these additional tools to combat crime and terrorism, and in terms of any detrimental consequences that could arise.

---

[48](...continued)
Communications Daily, November 30, 2001, p. 1-2.

[49]Ibid.

[50]Ibid.

[51]EFF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities (Oct. 31, 2001).
[http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html]. The law does define "contents" and "electronic communications" for interception purposes, 18 U.S. C. 2518 (8), (12), although not for pen register or trap and trace device purposes, 18 USC. 3127.

[52]Communications Daily, November 30, 2001, op cit.