Legal Memorandum
Published by The Heritage Foundation
No. 16
March 23, 2005

Data Protection: Safeguarding Privacy in a New Age of Technology

Paul Rosenzweig and Alane Kochems

Since September 11th there has been a great deal of attention on the use of new technologies to perform risk assessments. Two such risk assessment programs, Secure Flight and the proposed, but never implemented, Terrorism Information Awareness (TIA), attempt to analyze information and identify threats to American security. These initiatives raise legitimate concerns about the effectiveness of the technologies and the potential for abuse of civil liberties. Although these technologies could be useful tools for government and private sector security initiatives, many people still are apprehensive about their potential legal, political, and civil liberties implications.

Methods exist for ensuring that the data collected by such programs can be secured. Several standards are available for data protection technologies. Data holders should also manage access to the protected information. After looking at the technology side, we consider the legal and policy implications of using such technology.

Data Protection Technologies

As risk assessments become more popular and the volume of data collected by such programs increases, individuals will attempt to gain unauthorized access to the data and the systems on which they reside. Attempts to penetrate protected systems usually involve some combination of technology and social engineering. To counter such tactics, the government and other organizations should consider multiple

Talking Points

- When designed with proper procedures and safeguards and combined with oversight, technology can provide a reasonable balance between security and privacy.
- The mere implementation of new laws and systems to combat terrorism does not automatically diminish privacy. Rather such laws and practices frequently involve substituting one type or level of privacy intrusion for another.
- Not all data protection technologies will work for every situation—nor should they. The greatest policy challenge is finding the most effective uses of the specific data protection technology—both for liberty and security—not in labeling the collection of information as evil.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/lm16.cfm

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

safeguards to achieve information security. The first is to use accepted industry standards to design a strong information security plan. The second is to protect the data with cryptography to the extent practicable. The third involves ensuring that people authorized to access the data have permissions for access only to data that they need.

Gaining Access to Protected Systems and Data

Individuals seeking unauthorized entry into a computer network will often engage in significant reconnaissance before attempting entry. They may, for instance, scan the target's Web sites and query online databases to find out additional information about the organization or its employees. A target's Web site can provide useful information such as contact information, corporate culture and idioms, product names, business partners, and any of the target's mergers or acquisitions. The individual can also scan list servers for questions that give more information about the network. For instance, the target's systems administrator could post a question to a security-related listserv that includes the types of hardware or software the target is using. Google or other search engines may provide additional information on the target or individual employees. "Whois" records are another resource, listing the names and contact information of employees responsible for network security and operations. Once the individual has this background information, the hacker can then use "social engineering" to fill in missing information like passwords.

Social engineering usually involves the hacker manipulating the human tendency to trust, with the goal of accessing valuable systems and the information residing on them.[1] There are a variety of social engineering tricks for collecting passwords. These include impersonating a new employee or an angry manager who needs a password immediately; claiming to be an employee who needs to gain access to the system remotely; or pretending to be the systems administrator and requesting passwords from employees. Still others may pose as legitimate customers of information providers and secure confidential information through a simple ruse.[2]

There are other techniques for acquiring unauthorized access to networks. Some are as simple as visiting the target's company parking lot and looking for vanity tags on cars. Someone's password may be similar to the vanity tag. Other, more technical, methods include war dialing, where the individual systematically tests the target's phone numbers and extensions to locate unprotected modems, and scanning the network for unprotected ports.[3] If not properly secured, infrared and wireless networks may also be vulnerabilities.

As long as the government and private companies continue to collect vast amounts of information about people, there will be individuals attempting to access it. Entities that store valuable information must be vigilant as hackers' tactics and methods will continue to evolve and change.

Standards for Data Protection

To protect its data and systems, every organization should have a well-conceived and implemented security policy. Such a policy allows for a systematic approach to security that minimizes the chance of overlooked vulnerabilities. The optimal information security policy should be based upon generally accepted public standards used in combination to best meet each company's needs. These public standards (some designed for specific industry sectors) have been articulated in the

1. See Sarah Granger, "Social Engineering Fundamental, Part I: Hacker Tactics" (last updated Dec. 18, 2001), available at *www.securityfocus.com/infocus/1527*.
2. For instance, see Bob Sullivan, "Database Giant Gives Access to Fake Firms," *MSNBC News* February 14, 2005, at *www.msnbc.com/id/6969799* (February 22, 2005) and Rachel Konrad, "At Least 700 Have Identities Stolen," Associated Press, February 19, 2005, at *http://story.news.yahoo.com/news?tmpl=story2&u=/ap/20050219/ap_on_bi_ge/choicepoint_identity_theft* (February 22, 2005).
3. See John Leyden, "Crackers Favor War Dialing and Weak Passwords," *The Register*, April. 26, 2002, available at *www.securityfocus.com/news/379*.

Gramm-Leach-Bliley Act (GLBA),[4] the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[5], and the International Organization for Standardization's (ISO's) 17799.[6] The GLBA standard, which is intended to protect consumers' personal financial information that is held by financial institutions, identifies 296 specific issues to be considered in 15 broad areas. HIPAA covers consumers' private information in a health care context and identifies 20 control areas with 329 discrete issues relating to data/system security.

ISO 17799 is a non-industry specific, international code of practice. The ISO describes the code's purpose as offering "guidelines and voluntary directions for information security management. It is meant to provide a high level, general description of the areas currently considered important when initiating, implementing or maintaining information security in an organization."[7] It has two parts: ISO 17799, which is a code of practice, and BS7799-2, which contains security management system specifications. This standard is intended to serve as a single reference for determining the types of controls needed for the majority of situations in which information systems are used in industry and commerce. ISO 17799 identifies 10 control areas for implementation: (1) establishing organizational security policy; (2) organizational security infrastructure; (3) asset classification and control; (4) personnel security; (5) physical and environmental security; (6) communications and operations management; (7) access control; (8) systems development and maintenance; (9) business continuity management, and (10) compliance.

Organizations that collect and store data must carefully choose the standards that best fit their individual needs. An appropriate, reliable standard allows for a systematic review of information security policies and systems to better protect valuable systems and data.

Protecting Data with Cryptography

In the United States, the National Institute of Standards and Technology (NIST) establishes the standards for government agencies wishing to encrypt their data.[8] If properly implemented, cryptography (the technology for keeping information secure) provides very strong data protection. With cryptography, a person can know everything about the cryptographic tool except the key and still be unable to decipher the enciphered information. Cryptography is therefore a powerful data protection tool because it allows an organization to focus on protecting just the key instead of vast amounts of information.

There are two types of algorithm keys: symmetric and asymmetric. With symmetric algorithms the encryption key and decryption key are identical. To use this type of algorithm, the sender and receiver must decide in advance what the key will be. If the key becomes known, then anyone with the key can access the encrypted information. Symmetric ciphers are typically used because information can be enciphered and deciphered relatively easily and quickly.

4. For more information, see "Financial Privacy: The Gramm-Leach Bliley Act," available at *www.ftc.gov/privacy/glbact/*.
5. The text of the law is available at *http://aspe.hhs.gov/admnsimp/pl104191.htm*. The final security rule can be found at *http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2003_register&docid=fr20fe03-4.pdf*.
6. The ISO's product description and ordering information is available at *www.iso.ch/iso/en/prods-services/popstds/informationsecurity.html*.
7. *International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management: Frequently Asked Questions*, Nov. 2002, available at *http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf*.
8. The NIST Computer Security Resource Center (*http://csrc.nist.gov/*) provides information on all of its program areas including cryptographic standards and applications; security testing; security research and emerging technologies; security management and guidance; and outreach, awareness and education. NIST's standards for government entities that want to use cryptography to protect their data are detailed and technical. They cover public key, hashing, and symmetrical key cryptography. Instead of attempting to review every cryptography tool as it becomes available, NIST has certified nine commercial labs to test new programs and provides a list on its Web site of the validated programs.

Asymmetric or public key algorithms have different encryption and decryption keys. In addition, the decryption key cannot usually be determined from the encryption key within a reasonable period of time. With this type of algorithm, only the decryption key must remain secret. Security for such a system is higher, but the ease of use is comparatively less.

Cryptography can provide authentication, integrity, nonrepudiation, and confidentiality. In this context, authentication means that it is impossible for someone to impersonate someone else. Integrity involves being able to verify that the data have not been modified, and nonrepudiation prevents a person from denying having sent or accessed the information. Encryption can also enhance confidentiality for stored data. The greatest problem for cryptography, however, is lost keys, and the concomitant necessity for ways to recover the key—for data without a key are utterly lost. If data are being transmitted, losing the key or data is less of a concern because either can be resent. In order to counter the possibility of lost keys, there must be systematic key management and a backup system for keys and data. Yet this backup system for recovery is often the loophole and source of greatest insecurity in the system.

While cryptography can protect data, its more valuable role is in authenticating data and messages and demonstrating their integrity. For instance, cryptographic keys can be used to prevent intentional alteration or forgery. Many cryptographic tools now automatically integrate encryption, authentication, and integrity functions, since many individuals have difficulty doing this properly on their own.

Legal and Policy Implications

Technology is both a problem and a solution for the issues posed by enhanced information collection systems. It can facilitate access to and the accumulation of large amounts of data; however, if that access is not properly managed, the information can be misused. When designed with proper procedures and protections and combined with oversight, technology can provide a reasonable balance between security and privacy.

Technology can assist in ensuring both data security and data privacy. Software can allow for different levels of information access between the data owner and the data requester. This means that access is no longer a binary issue ("Can I have access to all of your data, yes or no?"). In addition, the variable access levels help to guarantee as much as possible the privacy of the third party whose data are being examined. If a data owner has a database of suspected terrorists, the owner can giver data requesters different permissions for data access. The data owner could, for example, give the State Department permission to retrieve the names of the top 10 individuals whose information matches at least 80 percent of the search request. The data owner might give a private entity, like an airline, less access. The search results might provide an identification number for individuals who have at least a 90 percent match to the database query. If the private entity (e.g., the airline) wanted more information, it would have to return to the data owner and request the information associated with the specific ID numbers. A third permissioning option would allow or require the data holder to send alerts to governmental entities, like intelligence agencies, when the database retrieves certain search results.

A Way to Think about Data Protection Technologies

There are gradations between the poles of complete anonymity and full identity. Many government transactions can now occur with the disclosure of a minimal amount of personal information. Just as there is a growing understanding of the concept of graduated identification, data protection technologies can provide a spectrum of access solutions for the government. Information databases can be designed to give data requesters the type and amount of information they need, and no more.

Conceptions of liberty are not based on the expectation of absolute privacy, but rather on the assumption that the government will not intrude without good cause. When a criminal or terror investigation is underway, Americans must be able to expect that scrutiny will not be focused on them without a good reason. Most interactions with the

government require more than absolute anonymity, but rarely reach detailed investigation. There must be a continued expectation that the government will ensure that infringements on liberty are commensurate with necessity. Properly implemented data protection technologies allow for authentication, verification, and graduated access. They can help prevent expectations of privacy from eroding by allowing the government to avoid treating full-scale disclosure as the default for all individual interactions.

The mere implementation of new laws and systems to combat terrorism does not automatically diminish privacy. Rather such laws and practices frequently involve substituting one type or level of privacy intrusion for another. Some Americans might prefer a shortened wait in airports if airlines can check their personal information against suspected terrorist watch list databases through limited permission rather than have to endure a longer wait and investigative screening onsite. Not all data protection technologies will work for every situation—nor should they. The greatest policy challenge is finding the most effective uses of the specific data protection technology—both for liberty and security—not in labeling the collection of information as evil.

Data protection technologies can improve the safety of data and prevent abuse. As with all technology, the implementation should be thought out well in advance and designed with the appropriate protocols to ensure privacy. Protocols can be both part of the hardware and the operational guidelines and oversight mechanisms.

Conclusion

In properly determining how best to enhance both liberty and security, it is useful to have some basic principles for assessing data protection technologies. Such a list might include the following:

- The data protection technology should allow for clear audit tracks to prevent data alteration or identify when data have been changed.
- The technology should have a means to provide graduated levels of access to the data.
- The technology should have protocols for enforcing the confidentiality and security of the data.

There are multiple approaches to securing data. One means is following one of the many published information security standards; another is to protect the most sensitive data through encryption. Controlling access to data and making sure that entities only have the appropriate level of access is critical if privacy interests are to be protected in the large data collections within the U.S. government's control. It is possible to balance security and privacy when it comes to data protection, but all of the policies and plans need to be thought out first before any of the data are collected.

—Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University. Alane Kochems is a Research Assistant in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation. This paper is based in part on a roundtable discussion held June 22, 2004, at the Heritage Foundation and co-sponsored by the Center for Democracy and Technology and The Heritage Foundation.