Policy and Legal Implications of Spyware and Data Privacy

Federal and state laws and university policies argue for taking a very close look at spyware and researchware as possible threats to data privacy

By **Andrea Nixon**

For years computer viruses have threatened productive use of personal computers, challenging users and support providers to prevent and recover from viral attacks. Now another type of computing malady has begun to enter popular consciousness: spyware.

Typically, analyses of spyware focus on technical issues or provide pointers to resources for detecting and removing unwanted software. Equally important are the legal and policy issues colleges and universities need to consider in assessing institutional responses to spyware on campus. Institutional policies must address both computer usage and compliance with federal and state laws.

Defining Spyware

Defining spyware can be contentious. The Anti-Spyware Coalition has drafted both narrow and broad definitions.[1] The narrow definition refers to tracking software "deployed without adequate notice, consent, or control for the user." More broadly defined, spyware is a synonym for software used to track or capture data, display ads, control a computer, dial modems, modify system software, analyze computer security, or automatically download files. For this article, I use the term spyware in this broader sense.

The arguments about spyware's nature arise from the intended use of the technologies. The Anti-Spyware Coalition's definitions allude to this insofar as they identify both wanted and unwanted uses of each technology associated with spyware. One market research firm, comScore, distinguishes between spyware and "researchware,"[2] asserting that researchware refers to software that collects personal information—including encrypted financial transactions—in a way that gives individuals notice, the choice to opt in, and the ability to uninstall the software. At stake for comScore and other market research firms is whether their techniques are viewed as legitimate and hence whether their software is targeted by antispyware applications.

In defining spyware, it is useful to consider recent use of the term researchware. Researchware is controversial in the higher education community for several reasons. While the term invokes the notion of research, it falls short of research guidelines to which colleges and universities adhere. In other words, market research firms may not have institutional review boards through which they vet research projects. Invocation

of the term research connotes standards in research design that may not be present in the market research process or activities. Also, market research companies' notion of individual consent is not necessarily sufficient in cases where their software culls information from institutionally owned computers.

Whether individuals have the option of giving consent or not, the presence of spyware on institutionally owned computers presents very real problems. What role does individual consent play where multiple people might use a single computer? What are the implications of spyware where confidential or protected data are exposed?

Legal and Policy Implications

Colleges and universities have an array of data stewardship responsibilities, some defined in federal laws governing the protection of records. Student educational records, for example, are protected by the Family Educational Rights and Privacy Act (FERPA). FERPA contains guidelines that establish what type of information, and under what circumstances, may be disclosed to students, guardians, school employees, and other parties.[3] Market research firms do not automatically qualify for access to student records without written permission from affected students, and their software does not meet this standard.

The privacy of medical records is protected under the Health Insurance Portability and Accountability Act (HIPAA), which was designed to provide a baseline of protection for medical records and individually identifiable health information. HIPAA requires patients to sign specific authorization before records can be disclosed to outside businesses for purposes not related to health care. HIPAA also contains specific restrictions and requirements for authorization to use patient information for marketing purposes.[4]

Personally identifiable financial information is protected by the Gramm-Leach-Bliley (GLB) Act, which requires that institutions disclose the parties with whom they share protected data. GLB also gives individuals the right to opt out of having information disclosed to certain third parties.[5] Uncontrolled disclosures of personally identifiable financial information through market research software, for example, presents very real challenges to GLB compliance.

Federal protection is not limited to administrative records. Colleges and universities establish institutional review boards (IRB) to ensure that research on human subjects follows the mandates of federal law. IRB guidelines specifically address the importance of protecting the confidentiality of data about people who are research subjects.[6]

Spyware is problematic in light of all of these federal laws and regulations. Once spyware is installed on computers that have access to protected records—whether stored locally or accessible over a network—a third party potentially has access to these otherwise protected data.

Depending on the location of a college and university, a variety of state laws may apply as well. The state of California's Law on Notice of Security Breach defines a "breach of the security of the system" as

> unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure (California Civil Code 1798.29).

While most colleges and universities are not bound by California state law, federal legislation is being proposed along the same lines (Senate Bill 751, Notification of Risk to Personal Data Act of 2005). Additionally, many institutions have or are in the process of putting together their own notification policies. In this context it is important for institutions to consider the implications of information culling as a potential "unauthorized acquisition of computerized data." Institutions must consider whether this type of disclosure represents sufficient cause to trigger notification of security breaches.

Spyware may present challenges to policies on an institutional level, as well. For example, colleges and universities commonly have policies in place that prohibit campus community members from sharing the passwords to their institutional accounts. Yet, just as spyware may capture an individual's Web-based activities or transactions, it might also capture enterprise credentials such as usernames and passwords.

Market research technologies such as comScore's (http://www.comscore.com/method/tech.asp) present acute risks to federally mandated data security rules under FERPA, HIPAA, and GLB. Similar problems may face researchers with respect to IRB guidelines. Additionally, it is possible that third-party access to protected data may run afoul of state law and institutional policies. Individuals who have access to protected data and who consent to the placement of spyware may well be in violation of federal or state law and institutional policies. Breaches of data security can expose institutions to the loss of federal funding or, if state laws are also violated, exposure to damages. The institution may also be compelled to invoke notification procedures mandated by state law. Consequently, it is important for students, faculty, and staff to be aware of the risks associated with spyware.

Preventive Steps

Market research firms such as comScore's Marketscore division claim to have access to the Web-browsing activities of as many as two million people. Some colleges and universities have seen sufficient numbers of connections to Marketscore sites to justify policy statements on this software alone. EDUCAUSE has a collection of resources that address issues associated with spyware in general and a listing of Marketscore policies in particular (http://www.educause.edu/Browse/645?PARENT_ID=741). Institutional policy responses listed vary from working to block all connections to known Marketscore addresses to redirecting requests for Marketscore

Web pages to institutional pages that warn of Marketscore's privacy practices. Some of this variation results from rapid changes that comScore has made to its software. IT security professionals have found themselves in a cat-and-mouse technical game as they work to keep up with shifts in comScore's software.

There are a number of steps that colleges and universities should consider taking to address this particular situation and spyware in general:

- Work to educate the campus community about the data security issues inherent in spyware.
- Prohibit the use of spyware or researchware on computers that have access to protected data, whether institutionally or privately owned.
- Engage faculty and administrators in discussions of the implications of breaches in data security for both institutional and research data.
- Provide antispyware software and training in its use for members of the college or university community.

Spyware presents institutional challenges that exceed the purview of computer security officers. It is important for faculty, students, and administrators to understand the risks associated with spyware and to have ready access to tools that will either prevent its installation or remove it. Institutional policy makers, legal counsel, and technologists alike need to play a role in informing their campus communities about the risks associated with spyware and the potential for security breaches and subsequent damage to the institution. *e*

Endnotes

1. The Anti-Spyware Coalition, Anti-Spyware Coalition Definitions and Supporting Documents, <http://www.antispywarecoalition.org/definitions.pdf> (retrieved September 20, 2005).
2. S. Olsen, "ComScore: Spyware or 'Researchware'?" CNET News.com, December 20, 2004, <http://news.com.com/ComScore+Spyware+or+researchware/2100-1032_3-5494004.html> (retrieved September 20, 2005).
3. U.S. Department of Education, Family Educational Rights and Privacy Act (FERPA), <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html> (retrieved September 21, 2005); and The Catholic University of America, The Office of General Counsel, "Reference Chart: Release of Student Education Records Under the Family Educational Rights and Privacy Act Actions to be Taken by Record Custodian," updated September 2001, <http://counsel.cua.edu/ferpa/resources/recchart.cfm> (retrieved September 21, 2005).
4. U.S. Department of Health and Human Services, "Fact Sheet: Protecting the Privacy of Patient's Health Information," April 14, 2003, <http://www.hhs.gov/news/facts/privacy.html> (retrieved September 21, 2005); and The Catholic University of America, The Office of General Counsel, "HIPAA," June 1, 2005, <http://counsel.cua.edu/HIPAA/> (retrieved September 21, 2005).
5. Federal Trade Commission, "Privacy Initiatives, Financial Privacy: The Gramm-Leach-Bliley Act," <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> (retrieved September 21, 2005); and The Catholic University of America, The Office of General Counsel, "Student Records and Confidentiality of Financial Information: University Obligations and the Gramm-Leach-Bliley Act," <http://counsel.cua.edu/glb/publications/brochure.cfm> (retrieved September 21, 2005).
6. Public Welfare, 45 § 46.111 (2005); R. L. Penslar, "Privacy and Confidentiality," Institutional Review Board Guidebook, 2001, <http://www.hhs.gov/ohrp/irb/irb_chapter3.htm#e4> (retrieved September 21, 2005); and The Catholic University of America, The Office of the General Counsel, "Institutional Review Boards," Summary of Federal Laws: Research, 2004, <http://counsel.cua.edu/fedlaw/Irb.cfm> (retrieved September 21, 2005).

Andrea Nixon (anixon@carleton.edu) is Associate Director of Academic Computing at Carleton College in Northfield, Minnesota, and a member of the EDUCAUSE Security Task Force Policy and Law Working Group, Researchware Working Group, and 20-20 Advisory Committee, and chair of the Advisory Committee on Teaching and Learning.