About
Membership
Government Affairs
Respondent Coop
Information on Demand
CMOR e-Newsletter
What Is Research?
Contact Info

Government Affairs

CMOR :: GA Articles :::

Anti-Spyware Legislation Advances in Congress
By Howard Fienberg
June 2007

The House recently advanced two competing approaches to combat spyware. Through the erosion of respondent trust, spyware presents a significant threat to research activities online. Furthermore, when written broadly, legislative measures to combat this activity threaten legitimate online research activities.

On May 10, 2007, the House Energy & Commerce Committee passed H.R. 964, the "Securely Protect Yourself Against Cyber Trespass Act" (the SPY Act). Then, on May 22, 2007, the full House passed H.R. 1525, the "Internet Spyware (I-SPY) Prevention Act."

What is spyware?
Spyware is malicious software that surreptitiously installs itself on a computer via the internet. Sometimes it is secretly bundled with free software available for download from Internet sites that offer music sharing, videos, weather data, games and screen savers. Once it gains access to a user's computer or laptop, spyware allows a third party to track a user's personal information. Spyware called "adware" tracks a user's web surfing or online shopping, allowing marketers to send that user unsolicited but related ads. Other kinds of spyware can steal one's passwords, credit card or social security numbers, or financial account information.

Experts estimate the cost of spyware to businesses and consumers at more than $1 billion. A 2004 study by America Online and the National Cyber Security Alliance found 80% of test group computers sported spyware – and 89% of those computers' users were unaware of it's presence.

CMOR's concern
Through the erosion of respondent trust, spyware presents a significant threat to research activities online. Furthermore, legislative measures to combat this activity threaten legitimate online research activities, when written broadly.

Although the Federal Trade Commission (FTC) has sued several purveyors of spyware, the Department of Justice has prosecuted several others, and both federal agencies insist that they have existing authority to handle the problem, Congress feels the need to enact specific and restrictive legislation.

H.R. 964 – The SPY Act
The SPY Act prohibits most commonly known unfair or deceptive spyware acts and practices, and the collection of personal information from a computer (via a spyware or adware program) without notice or consent before the first execution of any information collection program (opt in). The program must also allow the user to easily remove or disable the spyware and must contain a function that identifies the information collection program.

The Act would be administered by the FTC, which could collect civil fines of up to $3 million for violations with "actual knowledge or knowledge fairly implied on the basis of objective circumstances". It would also preempt state spyware statutes and provide an exemption for law enforcement and good faith activities.

The SPY Act would define "personally identifiable information" as the following:

- first and last name
- home or other physical address
- email address
- telephone number
- social security number, tax identification number, passport number, driver's license number, or any other government-issued identification number
- credit card number
- any access code, password, or account number, other than an access code or password transmitted by an owner or authorized user of a protected computer to the intended recipient to register for, or log onto, a Web page or other Internet service or

a network connection or service of a subscriber that is protected by an access code or password

- date of birth, birth certificate number, or place of birth of an individual except in the case of a date of birth transmitted or collected for the purpose of compliance with the law.

The House Energy & Commerce Committee passed H.R. 964 on May 10. Presuming it passes the full House, it will be the third time this legislation has passed the House (it has died without Senate action twice already).

CMOR's Interest in the SPY Act
Over the last several years, CMOR has been most concerned with the provisions relating to tracking cookies. If Congress banned cookies, many of the measurement infrastructures used by research companies to measure online audiences and media would be threatened. Thanks to CMOR's ongoing efforts, the House Energy & Commerce Committee amended the SPY Act clarifying the distinction between innocuous tracking cookies that are part of the basic functioning of most websites, and those that are stored on a user's hard drive to collect personal information (thus acting like spyware).

The bill also demands an FTC report, 6 months following the promulgation of final regulations, to "examine the extent to which cookies are or may be used to transmit to a third party personally identifiable information of a computer owner or user, information regarding web pages accessed by the owner or user, or information regarding advertisements".

H.R. 1525 – The I-SPY Prevention Act
The I-SPY Prevention Act imposes fines or imprisonment of up to five years for certain acts associated with spyware. Rather than attempting to define what illicit software is, the bill would make it a crime to copy computer code on a machine without authorization if doing so divulges "personal information" about a user or "impairs" a computer's security. The keys to violating the Act are the use of spyware in pursuance of other Federal crimes, or spyware activities and practices intended to defraud or deceive.

H.R. 1525 defines "personal information" as first and last name; home or physical address; email address; telephone number; social security number, tax ID number, drivers license number, passport number, "or any other government-issued identification number", or a credit card or bank account number or any password or access code associated with them.

This is the third time that the House has passed the Act. It now awaits action in the Senate.

CMOR's Interest in the I-SPY Prevention Act
Unlike the SPY Act, the I-SPY Prevention Act appears to more effectively target deceptive spyware. Although tracking cookies are not specifically mentioned or defined, there is a possibility that cookies could be included in the scope of the Act. Therefore, CMOR will be working with Senate staff to ensure that the interests of the research profession are protected.

State Spyware Laws
Twelve states currently have spyware laws. For detailed information on these laws, spyware restrictions in the European Union, and how researchers can ensure compliance with them, CMOR recommends the CMOR Compliance Guide (http://www.cmor.org/cg).

Disclaimer: The information provided in this message is for guidance and informational purposes only. It is not intended to be a substitute for legal advice. CMOR advises all parties to consult with private legal counsel regarding the interpretation and application of any laws to your business.

"Shielding the Profession"