Web Filtering and Tracking

by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In response to a recent article about stealth utilities intended to wipe out traces of Web browsing on corporate computers, reader Dave Morris, an active supporter of FREE IT (http://www.freeit.net), an organization supporting open-source software, wrote to me with some interesting comments. The following edited version of our correspondence is published with Mr Morris' permission.

Mr Morris wrote, "I enjoyed this article very much as it does raise some interesting and controversial issues. I guess the position one would take depends largely on whether they are the 'oppressor' or the 'oppressed.'

"While I'm very much an advocate of privacy and personal freedom on one hand, it is also important to recognize the need for controls in certain situations. What is and is not appropriate is certainly subjective unless it is placed in context. If consenting adults wish to enhance their relationship by perusing the numerous titillating and scandalous destinations on the Web from the privacy of their own home, it is certainly their prerogative and their right to do so, as it is their right to protect their privacy by employing whatever means necessary on their own PC to remove the evidence, which could prove embarrassing if they share their PC with other family members.

"However, accessing that same information at the public library or the office is not only inappropriate, it could expose the employer to serious liability issues. The idea of allowing unfettered access to the Internet and then scouring the machine after the fact to uncover evidence of inappropriate use of company assets seems a bit like entrapment to me. Any company with the time and resources to do this could use it more efficiently by employing a content filtering solution that would enforce their appropriate-use policy by denying access to questionable material and reporting access attempts.

"The privacy tool would then be rendered completely ineffective in this environment as there would be no tracks to hide since access is denied. Nonetheless, I agree that stealth privacy software has no place in a corporate network."

I responded as follows: "No purely technological solution will prevent people from violating security policies if that's what they have their mind bent on. For example, it is possible to use anonymizing sites such as http://www.anonymizer.com to mask the destination of one's browsing. Mind you, one could then try to block access to the privacy proxy servers, but you see the point: without monitoring and enforcement, policies are just words on paper. Enforcement can hardly be described as entrapment if there is adequate awareness of the issues and training of employees for compliance with those policies. In any case, 'entrapment' is a term generally reserved for discussions of Fourth Amendment rights in connection with law enforcement personnel's behavior, not corporate security officers working within private networks."

Mr Morris then replied, "I would expand on your statement by saying that those with the will, the expertise, and the determination will eventually find a way to bypass whatever controls are in place. However, those that possess these skills are definitely a minority in most corporate environments.

"Content filtering is as much psychological as it is technological in that it communicates to the end-user that the appropriate use policies are, in fact, enforced and monitored. After attempting to reach a couple of marginal sites and finding them blocked, violators are likely to stop trying if they value their position. Such filtering can be used in conjunction with a policy against installing unauthorized software of any kind on the company's workstations."

Mr Morris added some thoughtful remarks of more general import going beyond issues of network administration:

"In this post-911 America, however, we find our rights to privacy and anonymity eroding as we are subjected to more and more surveillance through video cameras and technologies such as RFID, face-recognition software, biometrics and geographical positioning systems (GPS). The very existence of systems like Carnivore [the FBI tool for monitoring ISP traffic] justifies the need for the type of [privacy-protecting] software you describe. The government, it seems, is making an attempt at omnipresence. The desire to defend our right to privacy and anonymous freedom of speech does not imply guilt of any kind: it is simply an attempt to preserve the principles upon which this country was founded and to limit the government's ability to meddle in our private lives."

* * *

For Further Reading

American Civil Liberties Union < http://www.aclu.org/safeandfree/ >

Electronic Frontier Foundation < http://www.eff.org/ >

Electronic Privacy Information Center < http://www.epic.org >

Fight the Fingerprint < http://www.networkusa.org/fingerprint.shtml >

* * *

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mailto:mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.