CyberPro

July 2009

Keeping Cyberspace Professionals Informed

WILL 'DEAF LISTENING' TECHNOLOGY CHANGE WIRETAPPING LEGISLATION?

BY ED GUNDRUM, PRESIDIO NETWORKED SOLUTIONS

A Long History of Listening to Conversations

As long as there have been private conversations, people have tried to eavesdrop on them. Ancient Anglo-Saxons who hid in the eavesdrip of another's home to listen in were punished when caught. When conversations moved to the telephone, unregulated wiretapping enabled law enforcement officials to listen in on any conversation they wanted to. Today, wiretapping legislation helps protect the privacy of individuals by requiring court-ordered subpoenas that specify the conditions under which a wiretap may occur, including who can be listened to, for how long and what information must be heard within a specified time period in order for the wiretap to continue.

Wiretapping in Cyberspace

The advent of cyberspace has introduced a variety of new Internet Protocol communications including VoIP, e-mails, instant messages, blogs and social networking. These new means of communication have added complexity to surveillance because they may use open public networks that are less definable, accessible and traceable for law enforcement officials than were the traditional hard-wired telco switching technologies. Blogging and social networking added yet another layer of complexity due to their use of complex Web site http protocols. Pervasive IP communications – such as Blackberries – provide users with IP communications access wherever they travel and therefore create moving targets.

Additionally, each communication record itself has become more complex, with only 30 percent of the volume of some IP communications pertaining to the actual content and associated attributes, while the remaining 70 percent may consist of redundant packet level data, duplicate header information and Internet housekeeping protocols like Domain Name System (DNS).

'Deaf Listening' Technologies Offer New Wiretapping Capabilities

"Deaf Listening" is a term I use to describe applications that provide the ability for machines to capture IP communications in near real time, screen them for specific content and take action on matches and non-matches without human intervention.

Decomposing and converting the complex IP network traffic into more concise and flexible formats such as document-oriented XML enables simple, fast and comprehensive Google-like searches, even with files containing millions of records and occupying peta bytes of storage. By indexing every word within each IP communication, particular keywords or phrases within the content may be searched. IP attributes associated with the each communication (i.e. "From:," "To:," "Date:," "Time:," etc.) further identify the communicator and sources. Removing the unnecessary networking "junk" that accompanies each IP communication and focusing on the content and IP attributes during the conversion to XML allows the overall volume of the IP record to shrink by as much as 80 percent depending on the type of communication. This significant size reduction makes it cheaper to store and preserve files for a longer period of time for so that historical investigations may be conducted.

Conversations that match the search criteria may either be made available for viewing or subjected to additional qualification criteria. Conversations that do not match pre-approved selection criteria can be automatically deleted before they are made available to humans.

If a Tree Falls in the Forest….

George Berkeley, the great philosopher who created the theory of "immaterialism," or objects ceasing to exist once there was nobody around to perceive them, would have probably expressed this high tech version of his 250-year-old theory as: "If a machine records a tree falling in the woods, and that recording is deleted prior to any human hearing it, did the falling tree actually make a noise when it hit the ground?" Similarly in our wiretapping scenario: If a machine listens to a conversation for specific keywords, none are found and the record is deleted before a human sees or hears it, were that person's privacy rights infringed upon?

How Technology May Influence Wiretapping Legislation

A successful wiretap requires first that suspicion is aroused, a legal subpoena is created and the instructions within that subpoena must then be strictly implemented. While lawmaking officials will always require "just cause" for the issuance of a subpeona, "Deaf Listening" technologies may eventually influence the conditions under which a wiretap may proceed.

For example, instead of terminating a wiretap because certain keywords were not heard within a specified amount of time into the wiretap, perhaps new legislation will permit machines to listen to the entire conversation and selectively frame only those portions that pertain to the subpoena. The subpoenas may also include a wider group of suspects because the new wiretapping technology can automatically delete irrelevant conversations before any humans hear them, and therefore the risk of violating an individual's privacy rights are greatly reduced. Finally, the technology may influence the types of communications that may be tapped, including e-mails, Internet searches, VoIP, blogs and social networking. "Deaf Listening" technology is ready today to help meet the challenges of tracking IP communications and to influence new wiretapping legislation. George Berkeley would have certainly enjoyed participating in a debate about how this technology should affect wiretapping legislation.

About the Author

Ed Gundrum is senior manager for Sentry Managed Services at Presidio Networked Solutions and a security subject matter expert for ENISA. He is the former EVP for Dejavu Technologies, Inc., a network eforensics and security vulnerability assessment products company. Gundrum is also the former EMC Director of Telco, Media and Entertainment Solutions and Marketing, where he was responsible for the development, sales and marketing of a leading terrorist tracking solution. He holds a bachelor of arts in computer science from the State University of New York and a master's of business administration in management science from Rochester Institute of Technology. He can be reached at ed_gundrum@comcast.net.