USA PATRIOT and You (2)
by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, I am looking at some of the implications of the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001” (USA PATRIOT Act, or USAPA) for network administrators.

Following along the analysis I began summarizing in the previous article, the Electronic Privacy Information Center (EPIC) notes several other changes in existing laws that I believe will affect how network administrators have to comply with demands for wiretaps.

One change that may please many network administrators is that suspected violations of the Computer Fraud and Abuse law (18 USC 1030) can now be used as a basis for obtaining a wiretap under Title III. It may be easier now to get rapid response to a report of intentional unauthorized access to any federal-interest computer in the USA (i.e., to any system owned or used by government departments or agencies, financial institutions, credit-reporting agencies or by some contractors working under contract for such entities).

Another section (204) of the USAPA amends existing laws to permit access to stored voice-mail “through a search warrant rather than through more stringent wiretap orders.” [EPIC] Sections 216 and 220 allow surveillance to be extended throughout the United States instead of being limited to a narrow geographic court jurisdiction. This provision will certainly aid law enforcement agencies (LEAs) in carrying out their investigations on the highly mobile and interconnected population of suspects, but it has implications for network administrators too. Heretofore, an organization that objected to the terms of a wiretap or other surveillance order would have to appear in a relatively local court to present its case; now, the court may be on the other side of the country. In cases of problematic justification for court orders, organizations will have to weigh the value of protecting employee and customer privacy against the time and money costs of travel and legal representation in other jurisdictions. Remember too that corporate attorneys may not be licensed to practice in distant jurisdictions, leading to additional costs for local attorneys.

One of the most controversial changes authorized by the USAPA is in section 213, where LEAs are authorized to delay notification of their search and seizure procedures. In addition, when the FBI demands records (or any other “tangible things”) under court order, section 215 includes language that specifically forbids anyone involved in producing those things from revealing the fact that they were demanded and supplied. This rule must be incorporated into the procedures to be followed by network administration personnel to avoid inadvertently breaking the law when complying with FBI requests under these statutes. Some librarians and bookstore owners have been infuriated by this gag order and have taken to posting signs in their facilities that read, “The FBI has not yet demanded records about any of our members’ / customers’ reading habits. Watch for disappearance of this sign.” It remains to be seen whether such measures will be tolerated by the courts.

In summary, the USAPA has wrought significant changes in the laws of surveillance, search and
seizure in the USA and network administrators should be working with their corporate counsel right now to adapt corporate policies to ensure full compliance with these changes. It would be irresponsible to break the law by inadvertence through ignorance of our responsibilities.

The question of whether the USAPA should be renewed after its sunset date of December 31, 2005 is left to the individual reader.

* * *

For further reading:

American Library Association USAPA Reports.  

Computer Fraud and Abuse Act (18 US Code Section 1030).  
http://www4.law.cornell.edu/uscode/18/1030.html


http://www.fepproject.org/commentaries/patriotact.html

* * *

INFOSEC UPDATE 2003 – MONTREAL CANADA – 4-5 & 7-8 August 2003.  See  
http://www.dmcyul.com for details in English _et en français_.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems 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>.

Copyright © 2003 M. E. Kabay.  All rights reserved.

Permission is hereby granted to *Network World* to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.