In this short series of articles, I will look 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.

The bulk of this brief summary is based on the excellent, detailed analysis of the law provided by the Electronic Privacy Information Center (EPIC) in its extensive report on specific issues in this unprecedented set of changes in the powers of search and seizure granted to law enforcement agencies (LEAs) in the United States.

The USAPA consists largely of amendments to existing laws. In particular, network administrators should be aware that the basis for granting judicial warrants authorizing LEAs to intercept voice and data communications – including electronic mail and Internet usage data – has been greatly expanded.

Specifically, existing legislation (the Wiretap Statute, Title III) already allowed easy authorization of “tap and trace” installations on voice and data networks to intercept phone numbers (the numbers, note – not the conversations or data transfers) helpful in determining the physical location of suspects. I write “easy authorization” because such warrants did and do note requires showing probable cause that an individual or group of people were involved in specific named crimes. An officer of a LEA simply affirms under oath that such a wiretap would be useful in an investigation.

The low standard of proof made perfect sense when Title III governed disclosure of phone numbers and only phone numbers. However, USAPA has changed the nature of the information that can be gathered without changing the nature of the process through which a warrant is obtained. Specifically, the changes to Title III authorized by USAPA now include all forms of data related to Internet communications. EPIC writes, “The full impact of this expansion of coverage is difficult to assess, as the statutory definitions are vague with respect to the types of information that can be captured and are subject to broad interpretations. The fact that the provision prohibits the capture of "content" does not adequately take into account the unique nature of information captured electronically, which contains data far more revealing than phone numbers, such as URLs generated while using the Web (which often contain a great deal of information that cannot in any way be analogized to a telephone number).”

Network administrators will have to think about the implications of this change. Under the simple assertion of interest because of an investigation and entirely without having to show any evidence whatsoever that there is a substantive basis for probably cause to grant this breach of privacy, a representative of a LEA can demand access to the full flow of information moving through your Internet equipment. I suggest that you discuss this issue with your corporate attorneys to be sure that you understand exactly how you will have to respond to LEA officials if they show up at your door with a warrant issued as a result of Title III changes authorized by the USAPA.
For further reading:

Full text of the USAPA  
http://www.epic.org/privacy/terrorism/hr3162.html and also 
http://www.epic.org/privacy/terrorism/hr3162.pdf


EFF Analysis Of The Provisions Of The USA PATRIOT Act That Relate To Online Activities (Oct 31, 2001).  
http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.php

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

http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e>

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.