Cybercrime and the U.S. Criminal Justice System: Professor Susan Brenner Summarizes Key Issues

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT


The first article in Volume 3, Part 3: “Cybercrime and the U.S. Criminal Justice System,” is by Professor Susan W. Brenner, JD<http://www.udayton.edu/law/faculty_and_staff/brenner_susan.php> NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law; topics include

- Differences from Civil Justice System
- Basic Institutional Structure
- Relationship between State and Federal Criminal Justice Systems
- Criminal Justice System and Cybercrime
- Glossary
- Extensive references and suggested readings.

Some of key concepts discussed by Professor Brenner that I have picked pretty much by how interesting I found them are as follows:

- Under the Computer Fraud and Abuse Act (18 USC §1030), prosecution at the federal level requires a demonstration of interference with interstate or foreign commerce.
- Violations of copyright, but not of trademarks, are brought only by federal prosecutors.
- Fifth Amendment prohibition of double jeopardy does not preclude re-prosecution at the same level if a mistrial is declared; furthermore, a different level of government (e.g., a state) can prosecute the defendant for the same actions if they are violations of its laws.

One of the most interesting sections in the chapter concerns striking back at hackers – sometimes called hack back. In her sections on affirmative defenses and on hack back, Professor Brenner points out that under current US law, there is no provision for allowing victims of computer trespass to use unauthorized access to the computers and networks of those they believe to be there attackers. As she writes, “… The law does absolve citizens who take the law into their own hands under very limited situations; this is very different from a blanket authorization for online retaliatory behavior. Aside from anything else, such behavior is objectionable because of the [risk] that innocent parties will be targeted for retaliation; the consequences of this risk are particularly intolerable in cyberspace, where it can be impossible to know precisely from which system an attack was launched…. I must add that even if we do know which system is used to launch an attack, we still don't know whether the system is the property of the attacker or merely the property of an innocent victim subverted by the attacker.

Other interesting discussions in the chapter touch on defenses proffered by some people accused of crimes such as launching denial-of-service (DoS) attacks or involved in child pornography: if not the devil, at least a Trojan horse made my computer do it. Lay juries have actually acquitted at least one accused who claimed that malware whose presence was never detected on his
computer was responsible for the DoS attack with which he was charged. Legal scholars, writes Professor Brenner, have argued that such a defense should be dismissed if there is no evidence of malware on the computer involved or if there is no demonstrable proof that malware found on the system is capable of the particular legal trespass involved in the case.

As a long-time teacher of cyberlaw and cybercrime courses, <http://www.mekabay.com/courses/academic/norwich/cj341/index.htm> I was delighted by this chapter and will reference it my courses.

Readers interested in cyberlaw will also appreciate Professor Brenner’s blog, “Cyb3rcrim3”<http://cyb3rcrim3.blogspot.com/> which has many fascinating discussions of cyberlaw.

* * *


Copyright © 2011 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.