Don't Participate in Porn2Porn Networks

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

A colleague recently told me that a young relative of his was arrested by the state police in his US home for obtaining and distributing child pornography.

Child pornography is defined as "any visual depiction of sexually explicit conduct involving a minor (persons under 18 years of age)…. Federal law prohibits the production, distribution, importation, reception, or possession of any image of child pornography."< http://www.justice.gov/criminal/ceos/subjectareas/childporn.html >

In a 2001 paper< http://www.cyber-rights.org/documents/us_article.pdf >, "Governing Pornography & Child Pornography on the Internet: The UK Approach"(in *Cyber-Rights, Protection, and Markets: A Symposium. University of West Los Angeles Law Review* 247:275) from Yaman Akdeniz, LLB, MA, PhD, then of the CyberLaw Research Unit of the Faculty of Law at University of Leeds< http://www.law.leeds.ac.uk/research/international-governance/cyberlaw-research-unit/ > (and also the Founder and Director of the Cyber-Rights & Cyber-Liberties organization< http://www.cyber-rights.org/ >), Dr Akdeniz points to two UK laws particularly concerned with prosecuting child pornography (including "pseudo-photographs", which are modified images made to appear to be child pornography):

- Protection of Children Act of 1978
- §160 of the Criminal Justice Act of 1988.

As in the USA, creation, possession, and distribution of such materials are all punishable by law in the UK.

The young man who was arrested protested his innocence; apparently the illegal images were found only in the folders associated with a peer-to-peer (P2P) network that he belongs to. P2P networks such as the early versions of Napster< http://www.napster.com/ > and Kazaa< http://www.crunchbase.com/company/kazaa > allow (or allowed) users to post files for easy sharing with any other member of the network. Some of the shared files distributed through P2P networks that have been studied intensively are illegal copies of music, videos and software.< http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/archive/download.aspx?id=3190 >

A current example of a server-based equivalent to these P2P networks is Dropbox< https://www.dropbox.com/tour >, which lets a group of people access shared files instantly.

Another quirk is that some inoffensive-looking programs include file-transfer capabilities that most users fail to notice. For example, digsby < http://www.digsby.com/ > is a multiprotocol instant messenger client that integrates e-mail services and social-networking services into a single user interface. However, the terms of service< http://www.digsby.com/tos.php > changed after 2008.12.16 and before 2009.02.26< http://web.archive.org/web/20090226041618/http://www.digsby.com/tos.php > (ascertained using the Wayback Machine) to state that

> "You agree to permit the Software to use the processing power of your computer when it is idle to run downloaded algorithms (mathematical equations) and code within a process. You understand that when the Software uses your computer, it likewise uses your CPU, bandwidth, and electrical power. The Software will use your computer to solve distributed computing problems, such as but not limited to, accelerating medical research projects, analyzing the stock market, searching the web, and finding the largest known prime number. This functionality is completely optional and you may disable it at any time."

When I used Digsby several years ago, I failed to read clause 15 in the Terms of Service and therefore had no idea that the program was silently using my resources for anything at all other than my commands. When I found out, I uninstalled the program in a fit of pique.

The problem for users of any networks that download files to their computers without necessarily providing information about what is being transferred via the users' computers is that the users don't have information about what is being transferred via their computers!

Aside from the risk of malware infection< http://threatpost.com/en_us/blogs/hidden-security-risks-p2p-traffic-062712 >, P2P programs pose serious legal risks for users and for the corporate owners of the equipment being used to support P2P traffic. Joe Dysart write in *Today's Campus*< http://www.todayscampus.com/articles/load.aspx?art=369 > that

> "Many P2P users are being less-than-careful about the folders that get shared when they install a P2P program and are unwittingly disseminating all sorts of personal, sensitive and potentially damaging data over the web.
>
> "The Committee staff did its own investigation," says U.S. House Rep. Henry Waxman, who chairs the House's Committee on Oversight and Government Reform. "We used the most popular P2P program, LimeWire, and ran a series of basic searches. What we found was astonishing: personal bank records and tax forms, attorney-client communications, the corporate strategies of Fortune 500 companies, confidential corporate accounting documents, internal documents from political campaigns, government emergency response plans and even military operation orders."
>
> Worst case scenario for a university: a staff member using P2P software could inadvertently download a child porn image coded with a clandestine file name and never know it until it was too late, says Pasquale Giordano, president and COO of SafeMedia, a company that specializes in P2P blocking technology.

Readers would do well to either avoid P2P technology or to monitor the contents of files being transferred through these networks to ensure that they are not inadvertently contributing to crimes and inadvertently ending up being arrested.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *