Process Over Presumption:
The Vermont Encryption Key Decision

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

On December 17, 2006, Canadian citizen and legal US resident Sebastian Boucher crossed the US border into Vermont at Derby Line. A US Immigration and Customs Enforcement agent inspected the 30-year-old man’s computer and reportedly found pornography and – significantly for this case – child pornography on the Z: drive. The laptop was seized as evidence and Sebastian Boucher was charged with transporting child pornography across interstate borders. Two days later, when agents tried to access the Z: drive, they found that it was encrypted using PGP.

In the course of 2007, a grand jury issued a subpoena ordering the accused to divulge his PGP encryption key; that subpoena was overruled on November 20, 2007 by U.S. Magistrate Judge Jerome J. Niedermeier. The case has created a wave of impassioned debate in the blogosphere, much of it consisting of abuse hurled at the defendant and contempt heaped upon the judge for letting a child pornographer go unpunished; a typical example of that kind of commentary, complete with original spelling, grammar and punctuation, is “What are they thinking? This is our children. We should do everything to put children pornographers behind bars, along with the pedophiles!!!! They have the laptop already, they have the evidence. This Judge needs to wake up and do the job he was hired to do. ‘My own opinion may the should check on all the people that agree with this decision!’"< http://www.news.com/5208-13578_3-0.html?forumID=1&threadID=33676&messageID=350202&start=0 >


There are some implications of this decision if it is borne out on appeal. First, for corporate security managers, teach all employees what security specialists have been repeating for years: don’t carry sensitive materials across borders and don’t think that encryption will protect your laptop against seizure by border police. We have long known that many countries regard encryption on laptops with suspicion; in France, for example, “…the government has access to private encryption keys, import and export of encryption software are restricted, and strict sanctions are imposed for using cryptographic techniques to commit a crime.”< http://www.privacyinternational.org/article.shtml?cmd%5B5B347%5D=x-347-559537 >

Here are my recommendations for anyone crossing an international border with a laptop computer:

1) Do not carry anything on the computer that you would regret being known to the officials from either side of that border.
2) Be prepared to divulge your decryption key(s) on demand; otherwise be prepared to have your computer seized.
3) Because of the risk of seizure, you must absolutely back up all operational data that you carry on your portable computer before you leave.
4) Make two backups before you leave so that data corruption of portions of either one may be compensated for using the other copy.

Another thought prompted by this interesting development over Fifth Amendment rights is the easy carryover of loathing for a crime and its perpetrators (child pornography and pornographers) into hostility for due process. The person quoted above who was foaming at the keyboard and implying that anyone who supports due process must be a pornographer illustrates a logical error that underlies extreme political discourse: if you disagree with our policies you must support criminals / perverts / our enemies / terrorists. We must steadfastly resist these forces of illogic and refocus the discussion on the arguments at hand. The rants and the _ad hominem_ attacks are dangerous distractions that we can challenge by dragging them into the light of reason.

Finally, I am struck by how poorly some of us in the United States grasp the importance of due process in protecting us from abuse of power. Our revulsion at child pornography and our fear of terrorism make it easy to forget that, unlike the situation in many dictatorships around the world, accusations are not normally permitted to be _ipso facto_ proof of guilt. We insist on fair and open judicial process precisely so that we shall not subject ourselves to rule by the powerful and conviction by emotion. I hope that these principles will return to our country and that we will see habeas corpus restored, secret trials condemned and torture repudiated.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 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.