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

In my last column, I introduced the issue of crossing United States borders with encrypted data and advised corporate users to think carefully about whether to do so. Today I want to discuss the implications of the _way_ the US Customs and Border Protection (CBP) service is demanding decryption keys from travelers and seizing portable electronic devices.

In February 2008, the Electronic Freedom Foundation (EFF) and the Asian Law Caucus (ALC) sued the US Department of Homeland Security (DHS) for “release of agency records concerning CBP’s policies and procedures on the questioning, search, and inspection of travelers entering or returning to the United States at ports of entry.”

We have now lost the benefits of strong disk encryption when crossing US borders. A bureaucrat can demand our encryption key and seize our computers with no way to prevent the seizure or even to demand (let alone receive) an explanation of that demand. How do we ensure chain of custody if there’s no available documentation, even under court order? How do we ensure protection of confidential corporate data if the rules of investigation are undocumented? Judging by the resistance of the USBCI to demands for information about their investigative process, the border entry points have become a constitutional-protection-free zone.

Corporate information about new products, new marketing plans, new business strategies and even detailed customer records may be worth millions to competitors. Do you really want to entrust such information to people who are _entirely without judicial oversight_? How much do you think an industrial spy would be willing to pay for some of your corporate secrets? For that matter, how much do you think ordinary criminals would be willing to pay for personally-identifiable information on your encrypted – and now decrypted – hard drive? Why would anyone assume that a secret process, closed to judicial or indeed any form of external oversight or control, is necessarily secure and immune to corruption? Faith? Hope? Patriotism defined as subservience to power?

It seems to me that we are experiencing a level of unchecked government intrusion that justifies a corporate policy dictating that employees, whether US citizens or not, should not carry _any_ confidential corporate data at all on their laptop computers unless they feel like having unnamed judicially-uncontrolled agents of the United States government examining company information. Oh – and watch out for your password safe; maybe it would be a Good Thing to wipe that as well if you are uncomfortable handing your bank account access codes to a total stranger.

On a personal note, I think my confidential, PGP-encrypted data might be at risk when I cross the US border. I’m a non-Christian (gasp!) former Canadian (horrors!!) with a name like “Kabay” (Father was “Kabashnikoff” until 1932) (ack!!); I’m a Life Member of the NAACP and I carry an ACLU membership card in my wallet (so I can claim to be a CCMACLU). I must be a threat to the
security of the United States. Gosh, perhaps I should be wiping my University laptop’s hard disk of all client, student and confidential University data and disabling the PGP encryption software on the system before I take the computer out of the country from now on. And I should warn my colleagues in the Information Technology group to be prepared to provide me with a nice replacement computer on demand after any trip abroad just in case someone decides to keep it indefinitely without explanation.

I’ll let you know how my next cross-border plane trip turns out – if I make it back home.

* * *

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.