

ITAR Sticks Users with Unfair Encryption Restrictions

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

“I’m from the government, and I’m here to help you.” Isn’t it sad how funny that seems? But on Sept. 17, 1993, bureaucrats *claiming to act in your best interest* once again interfered with your ability to protect your network transmissions using the best, most cost-effective encryption algorithms available. It’s time for network managers to take action to stop government meddling in the business of privacy.

U.S. software and hardware manufacturers are not permitted to export their most powerful encryption tools without a license. The difficulty of obtaining such export licenses forces U.S. manufacturers either to forego sales outside the U.S. and Canada or to produce a weaker version of their software for international distribution.

The costs of maintaining the different versions are paid for in higher prices for U.S. users. Similarly, giving away foreign markets also decreases the profits of U.S. firms and keeps prices higher than they could be if vigorous competition were the rule.

In addition, U.S. taxpayers have been paying bureaucrats’ salaries to apply the International Traffic in Arms Regulations (ITAR) to encryption software. According to ITAR, the Office of Defense Trade Controls of the U.S. Department of State can define anything it wants as equivalent to munitions. There is nothing to stop the bureaucrats from adding the decoder rings found in popcorn boxes to the U.S. Munitions List and designating them as a restricted export.

Just because some paper-pusher claims that encryption is a munition shouldn’t make it so. In the words of Lennart Benschop of Eindhoven University of Technology, the Netherlands, “Making cryptographic software equivalent to munitions is just as foolish as making addictive crossword puzzles equivalent to drugs.”

The notion that the U.S. government *should* let alone *can* prevent foreign nationals from having access to encryption technology was never reasonable in the first place, but it’s ludicrous today.

Trying to restrict the export of encryption programs in this age of the global Internet is about as useful as trying to keep cigarette smoke from drifting into the no-smoking zone in your favorite restaurant. Trying to control the flow of information via diskette or paper when data can travel unimpeded through the Internet is just plain dumb. How can a government official stop international users from using anonymous file transfer protocol (FTP) to get a copy of any encryption algorithm found on a file server anywhere in the world?

ITAR’s application to software is unenforceable and has been for years. One can already find encryption technology of the highest quality everywhere on the planet, ITAR notwithstanding.

On Sept. 17, [1993] the latest incident in which the federal government has attempted to enforce these ill-conceived regulations occurred. Grady Ward, president of Austin Code Works (ACW), a software firm in Austin, Texas, was ordered by a U.S. Customs special agent to turn over all paper and electronic documents pertaining to the distribution of ACW’s encryption products.

Ward has compiled a nine-megabyte anthology of already-published encryption source code, which he called “Moby Crypto.” This collection includes no executable code – only the algorithmic descriptions in C language that can be found (and exported) from scores of books and journals from the U.S. and elsewhere already freely distributed throughout the world.

Ward argued that the only difference between his cryptographic “whale” and other descriptions of encryption algorithms is that “Moby Crypto” is purely electronic, whereas textbooks and journal articles – which are freely circulated internationally without interference from ITAR – are printed on “paper pulp.” Even the Supreme Court, he continued, will provide its judgments in electronic form, and electronic White House records must be treated with the same respect as official paper documents.

Another software company, Phoenix, Ariz.-based ViaCrypt, was served with a similar subpoena because ViaCrypt recently contracted to sell a commercial version of Pretty Good Privacy (PGP), an encryption utility that has been circulated worldwide via the Internet. Indeed, although the first version of PGP was written in the U.S. by Phil Zimmermann, Version 2.0 of PGP came from the Netherlands, not the U.S.

The Electronic Freedom Foundation (EFF), which is dedicated to supporting the cause of liberty in cyberspace, has publicly announced its intention to support ACW and ViaCrypt, stating: “Neither of these companies are[sic] engaged in the international distribution of any illegal materials.... [I]f Moby Crypto contains no executable code, it should be exportable under ITAR, just as textbooks containing such materials are exportable.” A legal defense fund has been started to help defray the enormous costs that these two victims of bureaucratic meddling are likely to incur.

ITAR is not a dead letter, either. The latest modifications to ITAR are reported in the July 22 [1993] issue of the *Federal Register*.

Network managers need encryption technology to secure transmissions against eavesdropping and stored data against unauthorized access. You should brook no interference with the natural evolution of this technology.

The House Foreign Affairs Committee, Subcommittee on Economic Policy, Trade and the Environment held a hearing on mass market cryptography and export controls on the 12th of October at which speakers from industry expressed outrage over inclusion of cryptography in ITAR. Chair Sam Gejdenson (D-Conn.) opened the hearing with a statement which summed up the situation pretty clearly: “Just as in the case of telecommunications, the National Security Agency is attempting to put the genie back in the bottle. It won’t happen; and a vibrant and productive sector of American industry may be sacrificed in the process.”

In (nearly) the words of the great Canadian Prime Minister Pierre Elliott Trudeau, “The government has no place in the file servers of the nation.”<
http://archives.cbc.ca/politics/rights_freedoms/topics/538/> Tell your congressional representatives to take cryptography out of ITAR.

Note added in 2010: The encryption restrictions were eventually moved out of the control of the State Department’s ITAR in 1996 and changed to the much more lenient Export Administration Regulations (EAR) administered by the Department of Commerce.

* * *

M. E. Kabay,< <mailto:mekabay@gmail.com> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc.< <http://acsi-cybersa.com/> > and Associate Professor of Information Assurance< <http://norwich.edu/academics/business/infoAssurance/index.html> > in the School of Business and Management< <http://norwich.edu/academics/business/faculty.html> > at Norwich University.< <http://www.norwich.edu> > Visit his Website for white papers and course materials.< <http://www.mekabay.com/> >

The original version of this article was originally published as Security Perspectives column in the paper edition of Network World 10(45):42 (8 Nov 1993). At that time, Kabay was Director of Education for the National Computer Security Association (NCSA) which later became the ICSA and later TruSecure and then Cybertrust. Online versions of the original article are available through commercial databases such as ProQuest through your local, school or university library. This version has minor tweaks such as the insertion of the year and an additional reference link.