Cryptography Export Control Archives

This page indexes various cryptography-export related items. Contributions are welcome; send them to gnu@toad.com. Last updated 18 January 1996. [Many things have happened in export control since early 1996. I have only slightly updated this page since then. At the moment, consider it a historical snapshot of the export controls as they were then. --gnu 20 Sept 2000]

Export of Authentication Software

See the Domain Name System Security (DNSSEC) archives for details of our interactions with the export control bureacracies.

Political maneuvers -- Clipper-II

The Clinton Administration announced two meetings held in September by NIST about "software key escrow". They appear to be trying to use the export controls as a club to force domestic crypto providers to build key-escrow into their products. It doesn't look like industry will like this any better than they liked Clipper.

Court Cases

Courts are currently looking at several issues related to the export controls on cryptography:

Phil Karn's "paper versus online media" case

Phil Karn has filed a lawsuit against the State Department and one of its officials, in an attempt to get a judge to determine the Constitutional limits on media-based export control distinctions.

The State Department has apparently had a policy for some time of allowing printed publications to be exported, based on First Amendment concerns, but of refusing to allow similar software to be exported. Phil filed two CJ requests (see below, "Specific Commodity Jurisdiction Requests"), one for a popular textbook on cryptography, the other for a floppy containing the source code from the book. The State Department allowed export of the book, but denied export of the floppy.

Phil filed an administrative appeal on June 9, 1994, challenging both the details of the distinction between the paper and floppy copies, and the Constitutionality of restricting the export of the floppy version. Despite the regulations requiring 30-day response to appeals, Phil was told to expect a decision in mid-September 1994. On September 20, Martha C. Harris responded with a letter, stating that . . . ``your appeal raises particularly important and difficult issues. . . . I wanted to convey to you personally, as we have conveyed to [your lawyer], the care with which we are reviewing your appeal." She promised a response Real Soon Now.

Her final response to the appeal was sent on October 7, 1994. It reaffirms that they believe the floppy to be a munition, legally controllable, and worth controlling. With masterful vagueness, it also says, ``We have also reviewed your statement that the export of your disk is protected by the First Amendment to the Constitution, and have concluded that **continued control over the export of such material is consistent with the protections of the First Amendment.**" It goes on to reaffirm how much time and care they have taken in crafting the response, and thanks Phil and his lawyer for their patience.

As specified in the "final response", the decision can be appealed up the Executive Branch command-chain. If administrative appeals have not been taken far enough, the court might send

Phil back to the Executive Branch before actually looking at the issues. Phil's lawyers chose to send an appeal to Mr. Thomas E. McNamara, Assistant Secretary in the Department of State, on December 5, 1994. The appeal reiterates the Constitutional and factual arguments in more detail, and concludes, "We are taking this step only because ... we may be required to appeal to you before going to court. We hope that our pessimism proves unfounded, but the decisions in this case to date do not justify any expectation that a favorable decision is, as a practical matter, available within the Executive Branch." There is also an HTML version of this appeal, though I find it harder to read than the plain text.

On April 28, 1995, Phil's lawyers sent another letter to Mr. McNamara, saying that they have received no response since their early December letter. They believed that the delay appears to be a deliberate part of the Administration's attempt to chill the First Amendment-protected activities of Phil and others. They concluded with a promise to file suit by June 15 unless they receive a favorable decision by then. They received a reply from Mr. McNamara on June 13. As expected, it was useless. Phil's attorneys responded on July 19 with a letter pointing out the basic unaddressed inconsistency in the State Department's position (that a printed paper copy is exportable, but a floppy is not). The letter also promised that "we intend to seek judicial review in the near future".

On September 21, 1995, they filed the complaint (case #1:95CV01812) in the DC Federal District Court. It asks that "the provisions of the ITAR, as applied to Plaintiff KARN, be declared null and void, of no effect, as unconstitutional under the Fifth and First Amendments." and that "the determination to subject the Diskette to the export licensing controls of ITAR is unlawful in violation of the [Administrative Procedures Act]", which penalizes arbitrary or capricious acts and abuses of discretion by the Government."

The judge ordered on October 6 that the government file their motion for summary judgement by November 15, Phil's lawyers file their opposition to that motion by December 8, with the government replying by December 13. All these filings are available at Phil's web page below. As of January 18, the judge has not yet decided whether to grant summary judgement, i.e. whether to throw out the case.

Phil Karn's web page is the definitive source of information on the case.

Phil Zimmermann's harassment over PGP

Philip R. Zimmermann, author of the popular free cryptographic program PGP, has been subjected to harassment by Federal officials since his release of the program. He was informed in 1993 that a Grand Jury in San Jose, California, was investigating charges that Mr. Zimmermann had somehow been involved in exporting the PGP program. On November 9, 1994, upon his return to the United States from Europe, he was detained in Customs before he could re-enter the country, his luggage was searched, and he was interrogated for half an hour about his itinerary, public speaking activities, prior trips overseas, and possible PGP exports -- all without the benefit of counsel. He was eventually re-admitted to the United States (where he has a Constitutional right to enter), though the Customs Service promised to subject him to the same hassle upon every re-entry into the United States. On November 23, his lawyers complained to the Customs Service about the incident.

The whole investigation was dropped after three years with a short, useless press release in January 1996. The case is now closed and Phil need not fear further prosecution.

Dan Bernstein's attempt to publish Snuffle

A good summary of this case is in the EFF press release from when the suit was filed.

Daniel J. Bernstein invented a cryptosystem called Snuffle while a graduate student in math at UC Berkeley. He asked the State Department whether he could publish a short paper describing the new algorithm, and two pages of C-language source code that implement encryption and decryption using it. They denied his request. For fear that his paper had been lumped in with the software, he then sent in five separate requests asking separately whether he could publish the paper, the encryption source code, the decryption source code, an English description of how to encrypt, and an English description of how to decrypt. The State Department consolidated and denied all five requests. He also administratively appealed his initial request. The State Department never responded.

Mr. Bernstein sent various informal letters to the government, trying to get a reasonable response. It didn't work. Mr. Bernstein then spoke with the Electronic Frontier Foundation, who found him a pro-bono legal team and agreed to cover the out-of-pocket costs of suing to overturn the export controls. Cindy Cohn of McGlashan & Sarrail is the lead attorney.

February 21, 1995
: The lawsuit, case #C95-0582-MHP was filed against the State Department (and other agencies such as NSA who collaborate in enforcing export controls). It alleges that the export control law is an unconstitutional prior restraint on publishers protected by the First Amendment. It also claims that the current State Department regulations exceed the authority granted by the law, and that the actual practices of the agencies exceed the authority granted by their own regulations and the law.

May
: The government answered the lawsuit, denying everything that they can plausibly deny (and also denying that they ever received Mr. Bernstein's administrative appeal).

July
: Both sides met with the judge for the first time. Judge Patel set several dates for papers to be filed in preparation for a hearing on whether the court has jurisdiction over the case, held off other motions from all parties, and stayed discovery (the process of asking for documents from the other side) until the justiciability issue is settled.

August 15
: Government filed a "motion to dismiss" on justiciability. They hope to demonstrate that the case cannot even be brought before the court, and to show that software is not protected by the First Amendment.

September 22
: Opposition papers were filed, arguing that the suit is a proper subject for the court to address.

  - Motion opposing the motion to dismiss
  - Objection to the introduction of evidence while examining the question of jurisdiction
  - Request that the judge notice some Justice Department memos on the constitutionality of the export controls
  - Cindy Cohn's declaration
  - Lee Tien's declaration re the Justice Department memos

October 6
: Government filed reply papers in response.

October 20, 10:30am

Oral hearing on the government's motion, at the Federal Building at 450 Golden Gate Avenue in San Francisco, Judge Patel's courtroom. The judge asked various good questions, but did not yet rule on the motion.

EFF maintains the full archive of all the documents in the case. See in particular the Legal subdirectory.

Constitutionality of export controls on crypto

Office of Legal Counsel, Department of Justice

The Office of Legal Counsel contends that the export regulations regarding technical data and cryptography are not constitutional. John Gilmore obtained various papers and letters from them under the Freedom of Information Act, as well as from printed Congressional testimony. These were scanned in by the Electronic Frontier Foundation.

Law Review articles

A short bibliography of articles in law review journals, relating to the export of crypto.

State Department export guidance

The State Department controls most cryptography exports.

Arms Export Control Act (22 USC Sec. 2778)

The law under which cryptography exports are controlled. Cryptography is not even mentioned, but it empowers the President to designate which items are "defense articles" or "defense services".

International Traffic in Arms Regulations (ITAR)

The full set of export regulations created by State Department under the law. Cryptography is heavily controlled under these regulations, as if it was a weapon like a tank. Search in it for words like ``crypto", ``technical data", ``software", and ``public domain". This document is about 380K.

Writing your own Commodity Jurisdiction Requests

This handy kit will help you to write your own CJ requests and shepherd them through the bureacracy. It was collected and brought online by Lee Tien, tien@eff.org, lawyer for John Gilmore.

Munition Control Newsletter #80

This 1980 newsletter article was issued in response to the decision in the court case United States v. Edler Industries, 579 F2d 516 (9th Cir. 1978), in an attempt to clarify the State Department's position on how the crypto export regulations apply to scientific and technical speech protected under the First Amendment.

Defense Trade News

This "quarterly" newsletter from the Department of State offers occasional news about changes in the export control regulations on cryptography. This and much more State Department information is available online in the Department of State Foreign Affairs Network and in the Office of Defense Trade Controls.

Commerce Department export guidance

These documents related to general Commerce Department rules about exports. They are not specific to cryptography, which is also controlled by the State Department. When the State Department has released jurisdiction of a particular cryptography-related export to the Commerce Department, then these rules take effect.

General License GTDA regulations, including FAQ

This document contains the licensing regulations for General Technical Data exportable to All destinations (GTDA). It is followed by a question-and-answer guide written by the Commerce Department to help explain their often confusing regulations. The management of the BITNET obtained these documents in electronic form and made them available to the net.

Export aspects of international networks

This letter from Bill Clements, Director of the Office of Technology and Policy Analysis, Commerce Department, to the BITNET management explains their obligations and their members' obligations under the export laws, regarding exports of technical data and/or software over an international network.

Legal opinion

This letter from BITNET's lawyers explains a few more issues that were not clearly addressed in the above letter.

Crypto export survey

This survey is to document the economic arguments about how much business depends on cryptography and how it is affected by export controls. PLEASE FILL IT IN if you produce or maintain crypto software (either free or proprietary). Even if it's after the due date, they can still use the information.

Specific Commodity Jurisdiction Requests

These are formal requests sent to the U.S. State Department to ask what rules need to be followed before a product can be exported from the United States.

Applied Cryptography -- the book

An excellent textbook by Bruce Schneier (schneier@chinet.com). It contains descriptions of scores of cryptographic algorithms, including `C' source code for about a dozen. Phil Karn (karn@unix.ka9q.ampr.org) filed this CJR. You would think that under the First Amendment, there would be no law prohibiting the freedom to publish this book...and, indeed, the State Department affirms in its response that it does not control export of this book.

Applied Cryptography -- the floppy

This floppy disk, available from Bruce Schneier, contains the exact same `C' source code that was printed in the book. You would think that under the First Amendment, there would be no law prohibiting the freedom to publish this floppy...but the State Department disagrees. Phil Karn filed this CJR on March 8, 1994, as soon as he got the response to the first one, but the State Department tarried long beyond their 15-working-day limit for telling Phil whether he can export this floppy or not. Phil sent in a further request that they answer him on April 19, 1994. He also kept calling them, and Alan Suchinsky of the Office of Defense Trade Controls returned his call on May 10th, saying that the response had been rewritten twice but was going to be finalized that week. The formal response arrived on May 11, determining that ``The text files on the subject disk are not an exact representation of what is found in "Applied Cryptography." Each source code listing has been partitioned into its own file and has the capability of being easily compiled into an executable subroutine." As a result, ``This article is designated as a defense article under category XIII(b)(1) of the United States Munitions List."

See "Court Cases" above for further details about this CJ Request.

PGP: Source Code and Internals book

MIT Press has published the complete source code of PGP release 2.6.2 in book form. This 900-page book is printed in a fixed-width, highly readable font, convenient for optical character recognition. (The page numbers are in comments.) Since the State Department seems to think that books are exportable, while software is not, MIT thought this would be an interesting experiment.

Personally I think it'll be a collector's item. I got mine! Your grandchildren will be amazed that a supposedly free country's government ever tried to control cryptography. But you'll have the hard-copy evidence of the lengths we had to go to to debunk this ridiculous and oppressive policy. Here is the book's web page and an MIT Press order form. It's ISBN 0-262-24039-4, by Philip R. Zimmermann, US$60.

MIT Press has reportedly submitted a CJ request for the book, but has not yet received a response from the State Department.

Kerberos software without the cryptography

The file "bones.tar.Z" at this URL is a stripped-down version of the MIT Kerberos network security software, with all the cryptographic code removed, and all the calls to cryptographic code removed. It's called the "bones" of Kerberos. MIT did this to produce a version that was likely to be exportable. Indeed, when Cygnus asked, the State Department confirmed that it is not controlled by State. We then sent a formal request to the Commerce Department to see whether it was exportable according to their rules. They replied, but did not rule on whether we could use the GTDA export license, which permits exports to all countries without any paperwork. We sent in a second request and eventually the Commerce Department replied that indeed, because ``the software is available to the public without charge over the Internet, it is eligible for export under General License GTDA". They still haven't told us whether and how we need to file a ``Shipper's Export Declaration" when someone FTP's this software from us.

EFF ITAR Crypto Export Archive

The Electronic Frontier Foundation maintains an archive of Crypto Export related documents.

---

gnu@toad.com, gnu@eff.org