# Encryption and the Law

BU School of Law
Technology & Cyberlaw Clinic

Andy Sellars
BU/MIT Technology & Cyberlaw Clinic
Boston University School of Law

## Monday – Encryption research and the law

- Anticircumvention law
- The Computer Fraud and Abuse Act

## Today – Encryption law and policy

- Intro to lawful surveillance
- Reconciling encryption with lawful surveillance
- Regulation on sharing details of encryption – export control
- Code, speech, and the First Amendment

# Surveillance

# The Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

# The Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

A "search" requires a "warrant," which must be backed by "probable cause"

# The Fourth Amendment

A "**search**" requires a "warrant," which must be backed by "probable cause"

- A "search" requires government action
- A "search" has to intrude upon one's "reasonable expectation of privacy"
- A "search" does not include voluntarily disclosed information

# The Fourth Amendment

A "search" requires a "**warrant**," which must be backed by "probable cause"

- A "warrant" must go before a neutral party (usually a magistrate judge)
- A "warrant" must be accompanied by an affidavit demonstrating the factual basis for the search
- A "warrant" must be for a specific search or seizure, and not a "general warrant"

# The Fourth Amendment

A "search" requires a "warrant," which must be backed by "**probable cause**"

- The government must demonstrate the facts and circumstances that would lead a person "of reasonable caution" to believe that the search will reveal evidence of criminal activity or contraband

# The Fourth Amendment

COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, SS
NEWTON DIVISION

TRIAL COURT
DISTRICT COURT DEPT

---

APPLICATION AND AFFIDAVIT
IN SUPPORT OF APPLICATION FOR
SEARCH WARRANT

---

(M.G.L., Ch. 276, ss. 1 to 7; St. 1964, C. 557)

I, Kevin M. Christopher, being duly sworn, hereby depose and say that:

# The Fourth Amendment

Residential Life staff at this time. [redacted] also advised Officer Eng that Mr. Calixte is involved in some computer hacking incidents. [redacted] advised Officer Eng that Mr. Calixte has changed grades for other students by accessing the Boston College computer system. Mr. Calixte is also reported to be an employee of the Information Technology department here at Boston College. It should be noted that [redacted]

further. At this time he advised me of the following. Mr. Calixte is a computer science major who is considered a master of the trade amongst his peers. He is also employed by the Boston College I.T. department. [redacted] stated that he was aware of Mr. Calixte's reputation as a "hacker" prior to him being assigned into his room. [redacted] stated

and/or uses. [redacted] stated that it is not uncommon for Mr. Calixte to appear with unknown laptop computers which he says are given to him by Boston College for field testing or he is "fixing" for other students. Mr.

# The Fourth Amendment

report I investigated previously. [redacted] reported that Mr. Calixte uses two different operating systems to hide his illegal activities. One is the regular B.C. operating system and the other is a black screen with white font which he uses prompt commands on. This computer has three log on fields and it is reported that Mr. Calixte uses the nicknames "enigma" and "Bootleg enigma". [redacted] reported to me that he has observed Mr. Calixte hack into the B.C. grading system that is used by professors to change grades for students, he has "fixed" computers so that they cannot be scanned by any system for detection of illegal downloads and illegal internet use, "jail breaks" cell phones, possibly stolen ones, for people so that the phones can be used on networks other than they are meant for and downloaded program software against the licensing agreement for free. [redacted] also advised me that Mr. Calixte has a

# The Fourth Amendment

[redacted] has also recently been the victim of a mass e-mailing to the Boston College community in which he is reported to be gay and coming out of the closet. A gay web site profile was also created in [redacted]'s name and was attached to the e-mails. The use of a Boston College list server was used to accomplish this. The e-mails were sent via g-mail and yahoo. I have sent compliance/preservation letters to all of the

On two occasions web-based email accounts (gmail and yahoo mail) were used to send email to a mailing list at BC. The yahoo message included the IP address of the client used to send the message. This IP was 136.167.207.174 – indicating the sender was on the BC campus, and was using a wired connection in Gabelli residence hall.

(b) Records from the network registration system show tha computer was registered as a guest (rather than the usual student or faculty/staff). The registration system also contained the following additional information:

| | |
|---|---|
| Hardware Address: | 00:23:38:BE:38:24 |
| Computer Name | bootleg-laptop |
| Operating System | Unix Linux |
| Email Address | smaikopt@ctst.org |
| IP Lease Start Time | Saturday, March 7, 2 |
| IP Lease End Time | Sunday, March 8, 20 |

c) Searching the history of the registration system for additional uses of the computer name "bootleg-laptop" reveals that was used on August 24, 2008 by a computer registered to Riccardo F. Calixte.

# The Fourth Amendment

h. Your affiant believes and has probable cause to believe that the evidence that I seek permission to search for (consisting of the above-referenced computer system, computer data files, and other specified property, which all are directly associated with the above-stated facts and which all constitute evidence of the crime of "Obtaining computer services by Fraud or Misrepresentation" under Massachusetts General Law, Chapter 266, Section 120F and "Unauthorized access to a computer System" under Massachusetts General Law, Chapter 266, Section 120F.) are believed to be located in the premises and in the computer(s) at the premises.

# The Fourth Amendment

To conclude: taking into account the troublingly weak evidence of (1) Bennefield's reliability in connection with the allegation of unauthorized access to and hacking into the BC grading system, and (2) nexus, the search warrant affidavit fails to establish probable cause. Accordingly, because the search and seizure were not conducted pursuant to a lawful warrant, all ongoing forensic analysis of the items seized from Calixte must cease, see *Common wealth* v. *Kaupp*, 453 Mass. at 106-107, n.7 ([valid] search warrant required to search seized computer), and the items must be returned forthwith. See *Commonwealth* v. *Sacco*, 401 Mass. 204, 207 and n.3 (1987). Cf. *Matter of Lavigne*, 418 Mass. at 836. With respect to the two seized laptop computers and any other property that the Commonwealth claims do not belong to Calixte[9], the Commonwealth is to undertake to identify the owner(s) of this property, and, with prior notice to Calixte, return the items to those owners.

# The Fourth Amendment

A "**search**" requires a "warrant," which must be backed by "probable cause"

- A "search" requires government action
- A "search" has to intrude upon one's "reasonable expectation of privacy"
- A "search" does not include voluntarily disclosed information

# The Fourth Amendment

A "**search**" requires a "warrant," which must be backed by "probable cause"

- A "search" requires government action
- A "search" has to intrude upon one's "**reasonable expectation of privacy**"
- A "search" does not include voluntarily disclosed information

# No REP…

- Voluntarily surrendering information
- Information disclosed to third parties (stay tuned for *Carpenter v. United States* (SCOTUS 2018))
  - And with emails disclosed to a web host, *United States v. Warshak* (6th Cir. 2010)
- When crossing a border into the United States (stay tuned for *Alasaad v. Nielsen* (D. Mass. ???))
- When being searched incident to an arrest (Except with respect to devices! *Riley v. California* (2014))

# Statutory privacy protections

# ECPA

## Wiretap Act

- Real-time surveillance of content
- Requires "super warrant" – PC, plus serious felony, plus exhaustion

## Pen/Trap

- Real-time surveillance of DRAS information
- Requires that applicant "certify" that information is "relevant"

## Stored Communications Act

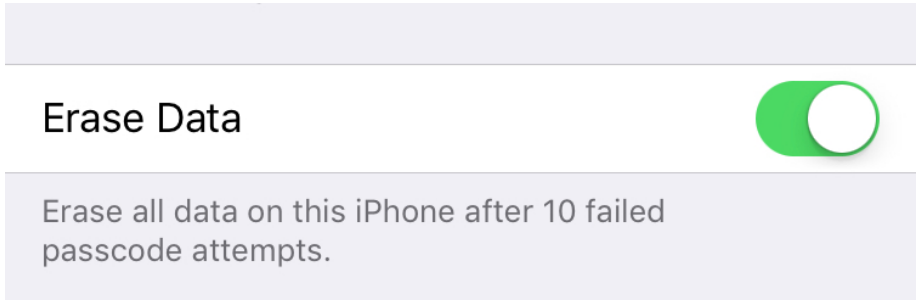
- All content and metadata in storage
- Differing levels of process for different types of information:
  - basic subscriber info – subpoena
  - most non-content records – "specific facts" showing "grounds to believe" that info. is "relevant and material"
  - content – search warrant (but maybe less for opened/old email)

# … but what if it doesn't work?

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2

hQIMAxpLIFYWEsv/AQ//XupXnj+cJiLlKof0GVqReQQFwvoRtB/ZZCz7IT5FYZxX
Vw6fJ0+TzG8aRw2sKjotPCmvZV260u8NydYhBxvW+/KUWA/LGnd9edw9lteZBA8G
7ncDfihhySRjQL4ELyNEMeGuiydS7R4baXx48bxl0ThBsHDNbwHpQjngvwU+E9fl
j5Hbsj+f93h5kidhBIldZNIIB5Nz6BW1eW09ij3CZE8FplMMtTTby/vB8DdOlVHh
Gm8zNzmAAho1vXzvg9FT40A3Zjzj7IHyG6mhov+E3ILQP0QdstEuQGmEpwda+IDZ
T3LpJsZavlflas8PR0UbEeQqEpTZCFzjwq8fb5vhmphRAdvWhUi8uxqpaRfNJbI3
Q+GB2+eg6PFvNYF3zsBEeBgJVJUKTegipknYgmvr+uA5pgCniDeccBvqNAu2PkSu
krYFL5XKVDgSQ8gTMheDzCDrgeMpzniklDh6t/NlWs2vRseoIIwsEfsbdTuuG/No

# … but what if it doesn't work?




# … but what if it doesn't work?

- Force companies to use worse crypto?
- Compel the witness/target/suspect to unlock it?
- Compel the software manufacturer to design a break?

# … but what if it doesn't work?

- **Force companies to use worse crypto?**
- Compel the witness/target/ suspect to unlock it?
- Compel the software manufacturer to design a break?

CALEA (47 U.S.C. § 1001 et seq.)

- Requires telecommunications carriers to be able to isolate and provide LE to communications when they have lawful authorization to access them.
- Does not regulate "information services" – ISPs, cable TV, etc.
- Does not prohibit users from employing their own end-to-end encryption

# … but what if it doesn't work?

- **Force companies to use worse crypto?**
- Compel the witness/target/ suspect to unlock it?
- Compel the software manufacturer to design a break?

# … but what if it doesn't work?

- Force companies to use worse crypto?
- **Compel the witness/target/ suspect to unlock it?**
- Compel the software manufacturer to design a break?

# … but what if it doesn't work?

- Force companies to use worse crypto?
- **Compel the witness/target/ suspect to unlock it?**
- Compel the software manufacturer to design a break?

Possibly, but yet another Constitutional Amendment!

# The Fifth Amendment

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

# The Fifth Amendment

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; **nor shall be compelled in any criminal case to be a witness against himself,** nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

# … but what if it doesn't work?

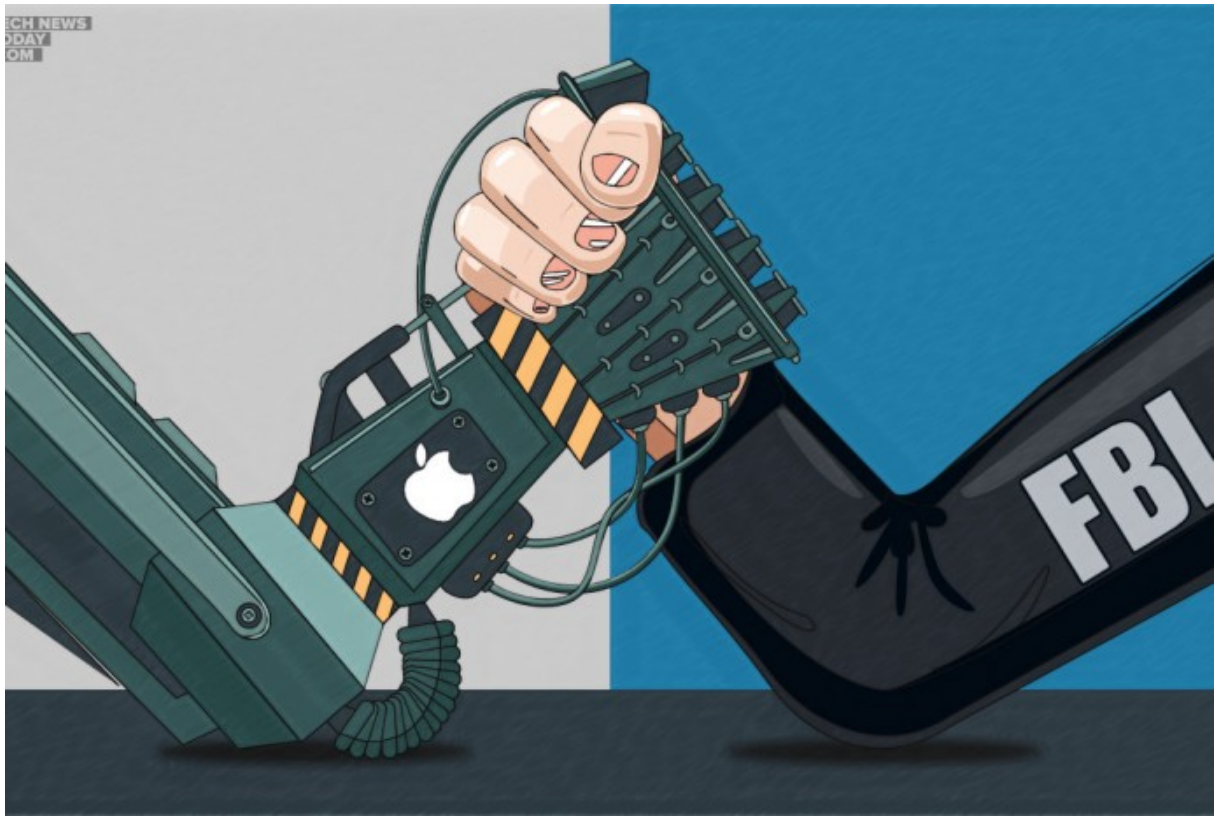
- Force companies to use worse crypto?
- **Compel the witness/target/ suspect to unlock it?**
- Compel the software manufacturer to design a break?

## Take the Fifth?

- Has to be "testimonial" and "incriminating"
- "Foregone conclusion doctrine" says that producing evidence alone is likely not enough to qualify
- Courts applying this to locked phones are fracturing – defenses tend to be strongest when government cannot already show that the suspect put the password on the device in question

# … but what if it doesn't work?

- Force companies to use worse crypto?
- Compel the witness/target/ suspect to unlock it?
- **Compel the software manufacturer to design a break?**



# Intro to Export Controls

Facebook Share Tweet

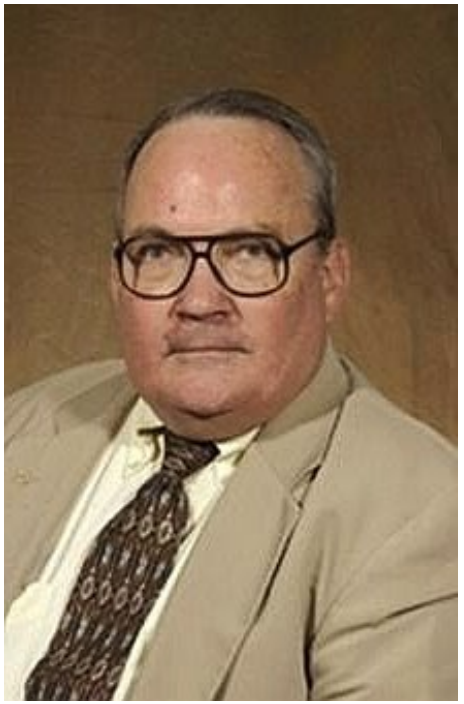
# Former University of Tennessee Professor John Reece Roth Begins Serving Four-Year Prison Sentence on Convictions of Illegally Exporting Military Research Data

**U.S. Attorney's Office**
February 01, 2012

**Eastern District of Tennessee**
(865) 545-4167

KNOXVILLE, TN—On January 18, 2012, John Reece Roth, a former professor of electrical engineering at the University of Tennessee (UT) in Knoxville, began serving a four-year prison sentence for his September 2008 convictions. Roth had been on bond pending his appeals, all of which were unsuccessful. He self-surrendered to the federal correctional facility in Ashland, Kentucky.

Roth was convicted after a jury trial in U.S. District Court in Knoxville, of conspiracy, wire fraud, and 15 counts of exporting "defense articles and services" without a license. As a UT professor, Roth obtained an U.S. Air Force (USAF) contract to develop plasma actuators to control the flight of small, subsonic, unmanned, military drone aircraft. During the course of that contract, he allowed two foreign national students to access export controlled data and equipment, and export some of the data from the contract on a trip to China. The Arms Export Control Act prohibits the export of defense-related materials, including the technical data, to a foreign national or a foreign nation. This case was a first-of-its-kind prosecution of a university professor for the transfer of controlled defense technology to foreign national graduate students.



# What are export controls?
# Why have export controls?

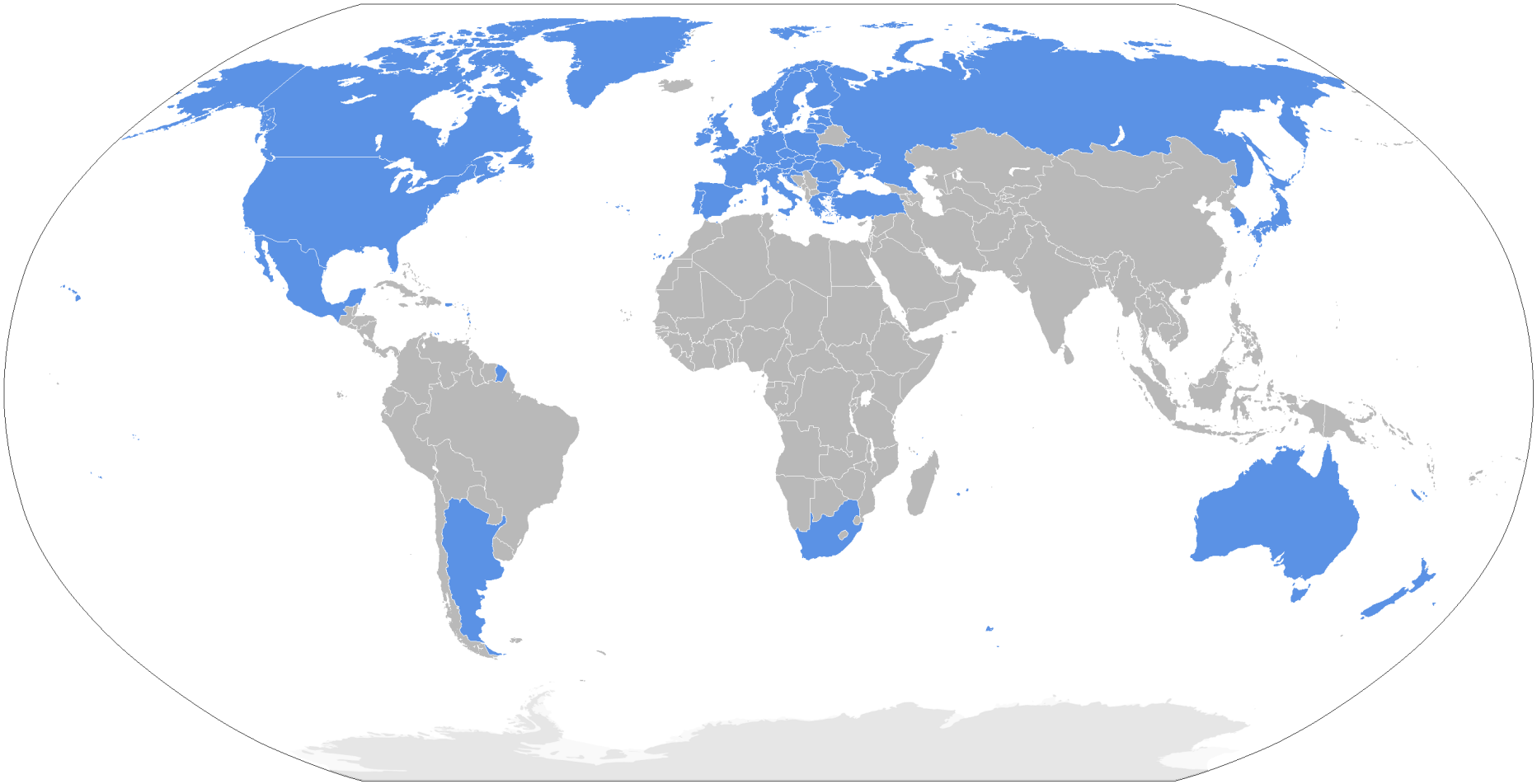
# Legal restrictions on technology information

1. Arms Export Control Act (AECA)
    1.1. International Traffic in Arms Regulations (ITAR)
2. Export Administration Act / Int'l Emergency Economic Powers Act
    2.1. Export Administration Regulations (EAR)
3. Trading With the Enemy Act of 1917 and related EOs
4. Invention Secrecy Act
5. Atomic Energy Act
6. Executive Order 13,526 (Classification of Information)

# Legal restrictions on technology information

1. Arms Export Control Act (AECA)
    1.1. International Traffic in Arms Regulations (ITAR)
2. Export Administration Act / Int'l Emergency Economic Powers Act
    2.1. Export Administration Regulations (EAR)
3. Trading With the Enemy Act of 1917 and related EOs
4. Invention Secrecy Act
5. Atomic Energy Act
6. Executive Order 13,526 (Classification of Information)

# Legal restrictions on technology information



Wassenaar Arrangement

# Legal restrictions on technology information

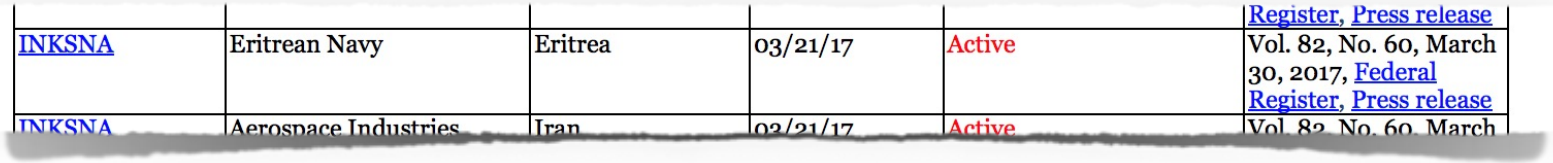
1. Arms Export Control Act (AECA)
    1.1 International Traffic in Arms Regulations (ITAR)
2. Export Administration Act / Int'l Emergency Economic Powers Act
    2.1. Export Administration Regulations (EAR)
3. Trading With the Enemy Act of 1917 and related EOs
4. Invention Secrecy Act
5. Atomic Energy Act
6. Executive Order 13,526 (Classification of Information)

# Export Administration Regulations

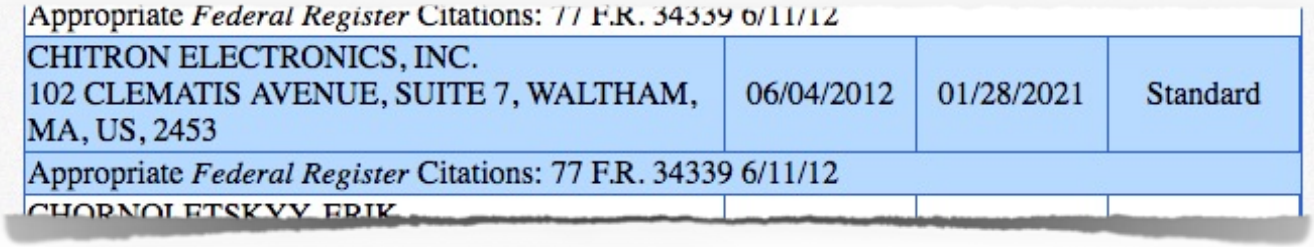
- Controlled Items
- Controlled Nations
- Controlled People

# Export Administration Regulations

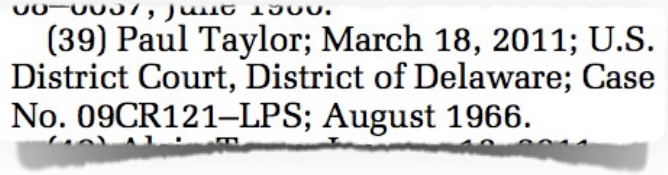
- Controlled Items
- Controlled Nations
- **Controlled People**



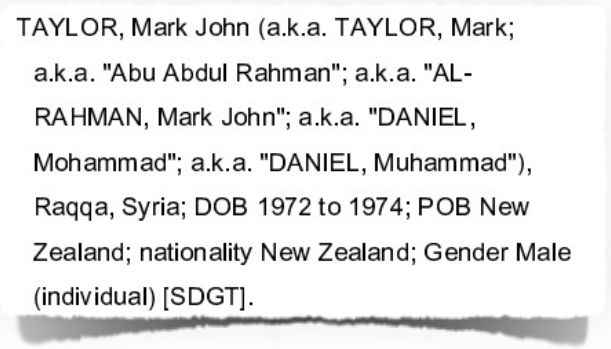
| | | | | | |
|---|---|---|---|---|---|
| | | | | | Register, Press release |
| INKSNA | Eritrean Navy | Eritrea | 03/21/17 | Active | Vol. 82, No. 60, March 30, 2017, Federal Register, Press release |
| INKSNA | Aerospace Industries | Iran | 03/21/17 | Active | Vol. 82, No. 60, March |



| | | | |
|---|---|---|---|
| Appropriate *Federal Register* Citations: 77 F.R. 34339 6/11/12 | | | |
| CHITRON ELECTRONICS, INC.<br>102 CLEMATIS AVENUE, SUITE 7, WALTHAM, MA, US, 2453 | 06/04/2012 | 01/28/2021 | Standard |
| Appropriate *Federal Register* Citations: 77 F.R. 34339 6/11/12 | | | |
| CHORNOLETSKYY, ERIK | | | |



(39) Paul Taylor; March 18, 2011; U.S. District Court, District of Delaware; Case No. 09CR121–LPS; August 1966.



TAYLOR, Mark John (a.k.a. TAYLOR, Mark; a.k.a. "Abu Abdul Rahman"; a.k.a. "AL-RAHMAN, Mark John"; a.k.a. "DANIEL, Mohammad"; a.k.a. "DANIEL, Muhammad"), Raqqa, Syria; DOB 1972 to 1974; POB New Zealand; nationality New Zealand; Gender Male (individual) [SDGT].

# Export Administration Regulations

- Controlled Items
- **Controlled Nations**
- Controlled People

Cuba, Iran, Iraq, North Korea, Russian-controlled Crimea, Syria, and "Russia Industry Sector"

# Export Administration Regulations

- **Controlled Items**
- Controlled Nations
- Controlled People

15 C.F.R. § 734.2(c): "Items subject to EAR" consist of the items listed on the Commerce Control List (CCL) … and all other items which meet the definition of that term.

15 C.F.R. § 734.2(a)(1): "Subject to the EAR" is a term used in the EAR to describe those items and activities over which BIS exercises regulatory jurisdiction under the EAR.

# Export Administration Regulations

- **Controlled Items**
- Controlled Nations
- Controlled People

***Excluded:***

- Items where another agency takes exclusive authority (e.g., Dep't of State with ITAR)
- De minimis US contact
- Generally available for free
- **Published material** – books, pamphlets, newspapers, and sheet music (?)
  - Incl. "posting on the Internet on sites available to the public" (§ 734.7(a)(4))
    - *note*: ITAR has not taken a similar position
- Disclosed in a patent or published patent application
- **Fundamental research**

# Export Administration Regulations

- **Controlled Items**
- Controlled Nations
- Controlled People

**Fundamental research:**

*[M]eans research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.* (§ 734.8(c))

- **Controlled It**
- Controlled N
- Controlled P

**rch:**

*ngineering, or*
*ich ordinarily*
*dly within the*
*hich the*
*restrictions for*
*y reasons.*

90896

THE WHITE HOUSE

WASHINGTON

September 21, 1985

NATIONAL SECURITY DECISION
DIRECTIVE 189

UNCLASSIFIED

NATIONAL POLICY ON THE TRANSFER OF
SCIENTIFIC, TECHNICAL AND ENGINEERING INFORMATION

I. PURPOSE

This directive establishes national policy for controlling the flow of science, technology, and engineering information produced in federally-funded fundamental research at colleges, universities, and laboratories. Fundamental research is defined as follows:

> "'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

II. BACKGROUND

The acquisition of advanced technology from the United States by Eastern Bloc nations for the purpose of enhancing their military capabilities poses a significant threat to our national security. Intelligence studies indicate a small but significant target of the Eastern Bloc intelligence gathering effort is science and engineering research performed at universities and federal laboratories. At the same time, our leadership position in science and technology is an essential element in our economic and physical security. The strength of American science requires a research environment conducive to creativity, an environment in which the free exchange of ideas is a vital component.

In 1982, the Department of Defense and National Science Foundation sponsored a National Academy of Sciences study of the need for controls on scientific information. This study was chaired by Dr. Dale Corson, President Emeritus of Cornell University. It concluded that, while there has been a significant transfer of U.S. technology to the Soviet Union, the transfer has occurred through many routes with universities and open scientific communication of fundamental research being a minor contributor. Yet as the emerging government-university-industry partnership in research activities continues to grow, a more significant problem may well develop.



COPY 1H OF 12 COPIES

# Export Administration Regulations

*The Commerce Control List:*

- **Controlled Items**
- Controlled Nations
- Controlled People

**3A227 High-voltage direct current power supplies, having both of the following characteristics (see List of Items Controlled) , excluding items that are subject to the export licensing authority of the Nuclear Regulatory Commission (see 10 CFR part 110).**

# Software and Export Control

# Software and Export Control

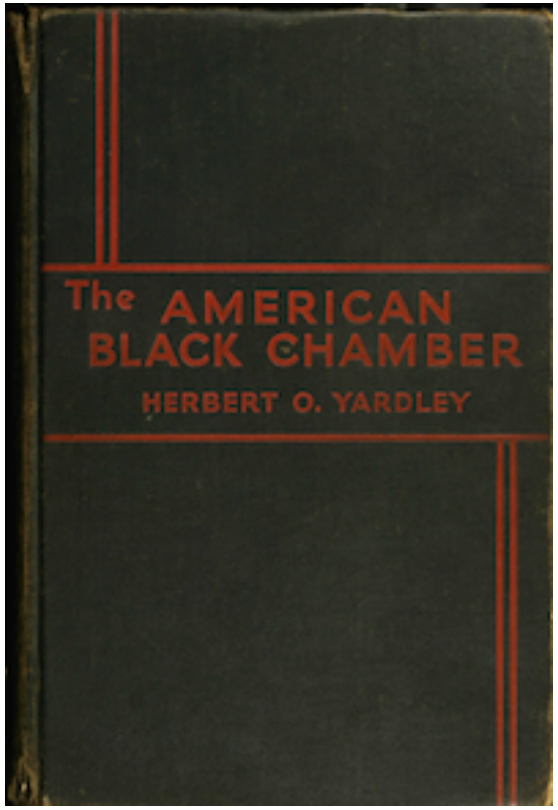
*generally speaking…*

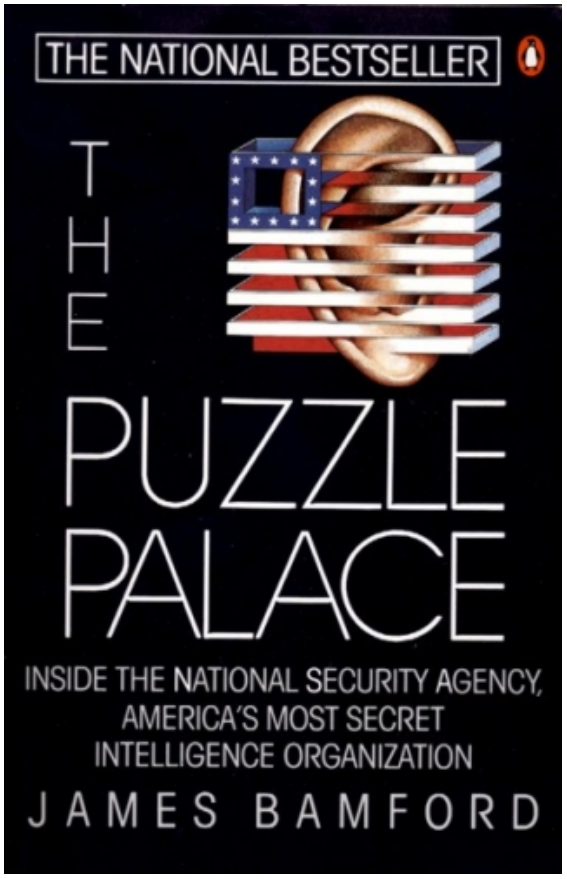
- software related to military uses or ITAR "defense articles" regulated by ITAR instead of EAR*
- software that is publicly available without charge is not restricted*
- export to Canada is not restricted, with only a few specific exceptions (software related to nuclear technology, firearms, and some wiretapping tech)
- "Mass market software" EAR § 740.13(d) – sold from stock, designed for installation without further support from supplier (beyond help lines, etc.)*
- Software patches for pre-cleared software ok
- The underlying media that embody software are not restricted (CDs, USB sticks, etc.)

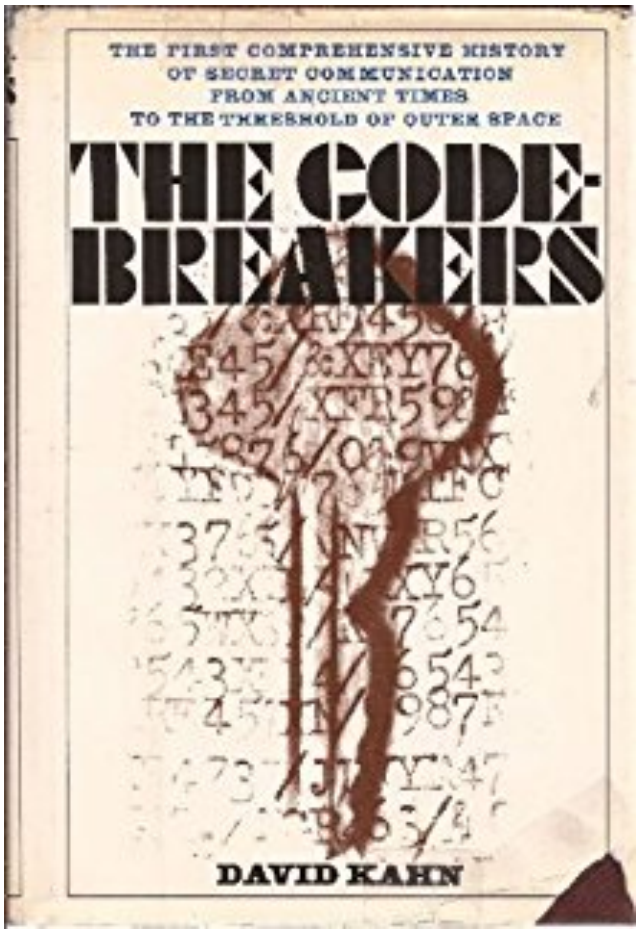


**(* = encryption caveat, stay tuned)**

# Encryption and Export Control


The AMERICAN BLACK CHAMBER
HERBERT O. YARDLEY


THE NATIONAL BESTSELLER
THE PUZZLE PALACE
INSIDE THE NATIONAL SECURITY AGENCY, AMERICA'S MOST SECRET INTELLIGENCE ORGANIZATION
JAMES BAMFORD


THE FIRST COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE THRESHOLD OF OUTER SPACE
THE CODE-BREAKERS
DAVID KAHN


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


NSF

# Report of the Public Cryptography Study Group

Prepared for

American Council on Education
One Dupont Circle
Washington, D.C. 20036

February 7, 1981

# Report of the Public Cryptography Study Group

Prepared for

American Council on Education
One Dupont Circle
Washington, D.C. 20036

February 7, 1981

In an era of instantaneous communication and pervasive computer data bases, it is becoming increasingly important to protect the privacy of both individuals and corporations, often using the tools previously used only by national governments.

There is growing evidence that enhanced security for unclassified but sensitive information will be needed in a wide variety of applications, ranging from personal records (insurance, criminal, health, law enforcement) to commercial proprietary and financial data in storage or in transit electronically. As the major world economies continue the trend toward information dependence, e.g., electronic mail, electronic funds transfer, point of sale terminals, etc., protection of business and even home computer systems from unauthorized monitoring or tampering will become increasingly important.

In many of these areas, cryptography is one of the most effective ways for providing the requisite security. Restriction of public research and development in cryptography might have an adverse effect on the ability of American industry to compete in world telecommunications and data-processing markets.

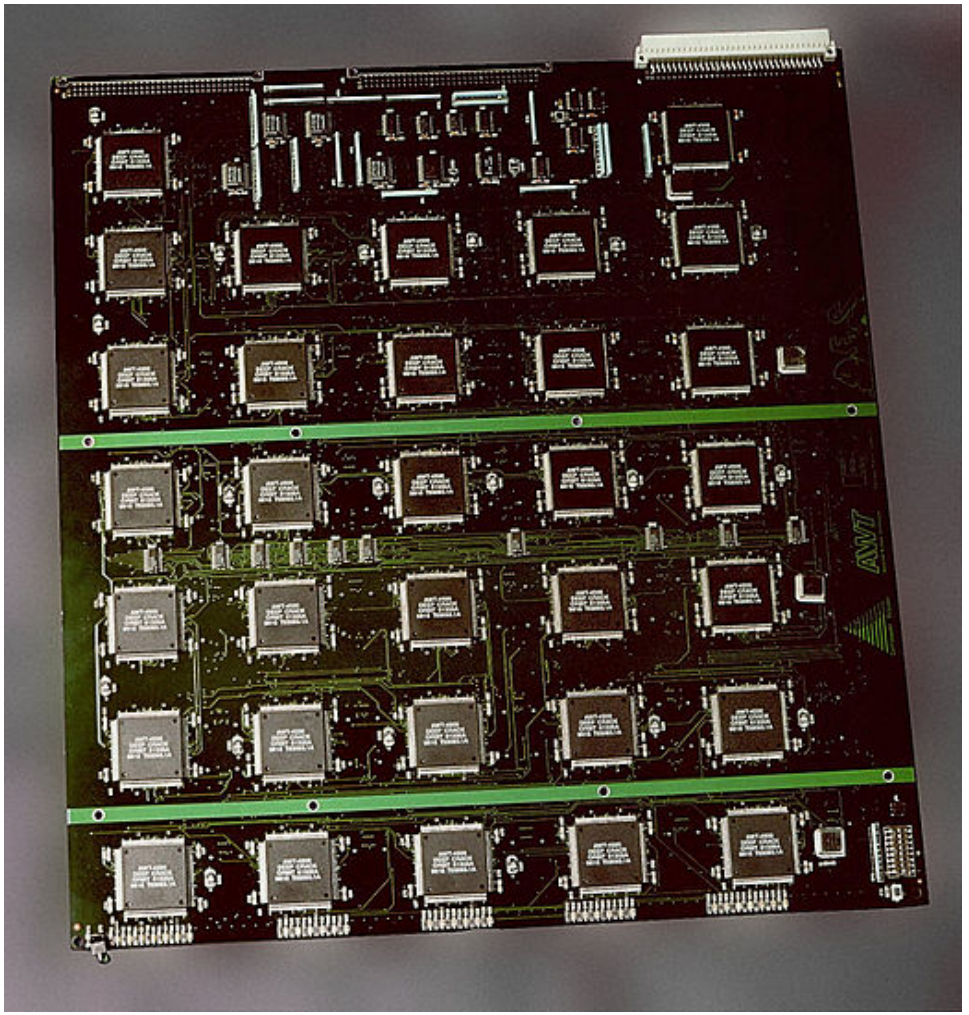
# Report of the Public Cryptography Study Group

Prepared for

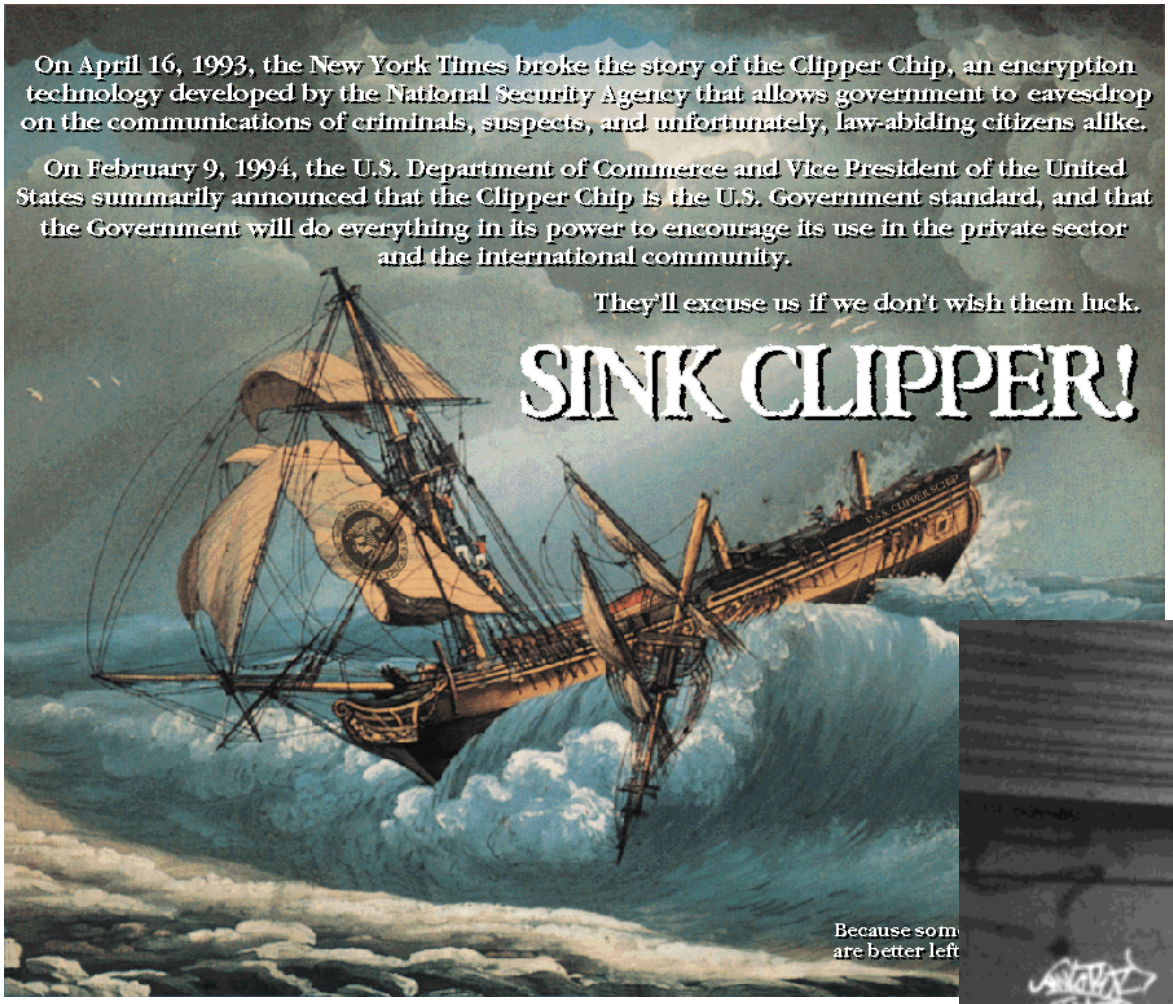
American Council on Education
One Dupont Circle
Washington, D.C. 20036

February 7, 1981

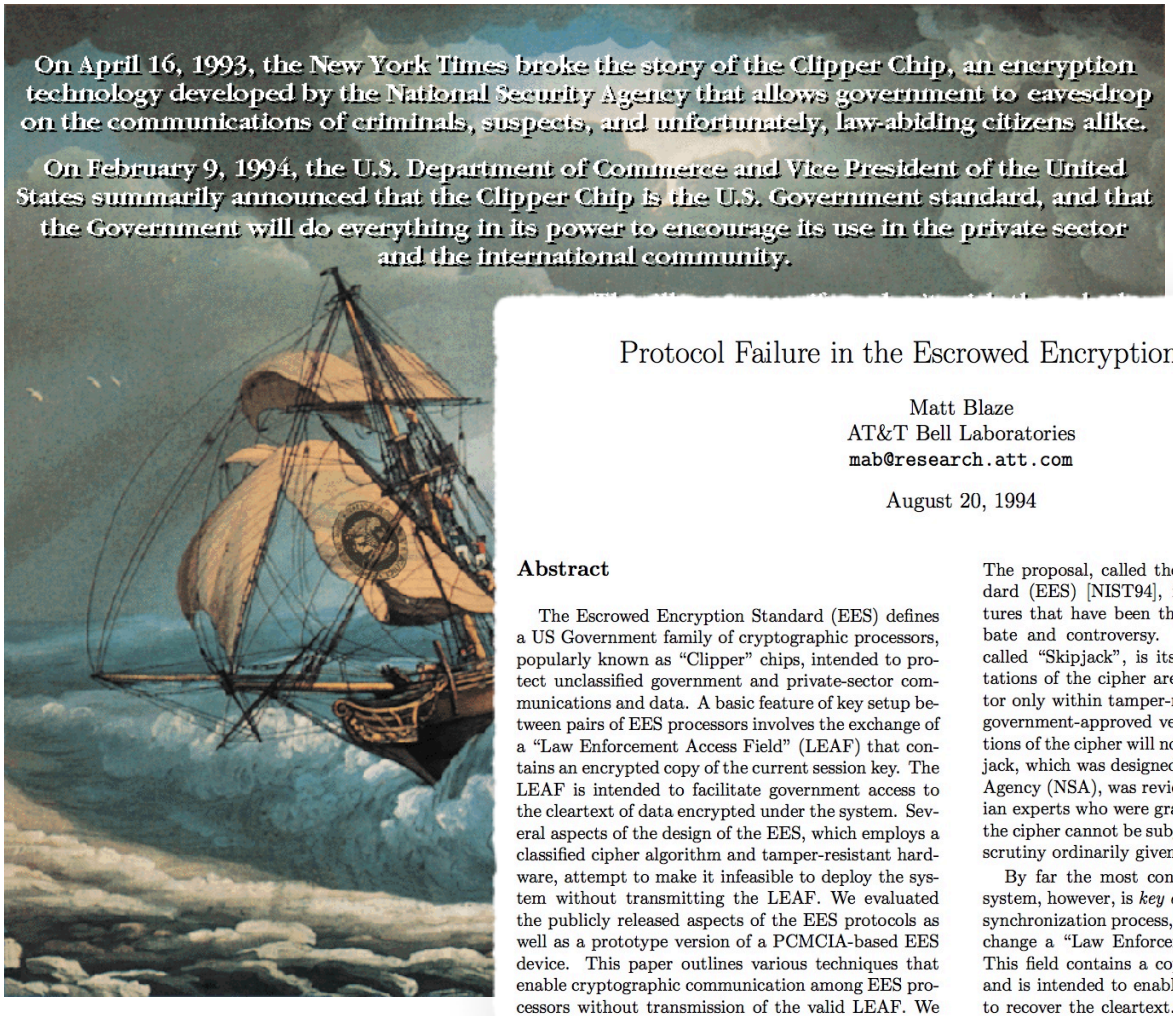
The Study Group has recommended that a voluntary system of prior review of cryptology manuscripts be instituted on an experimental basis. While the group would prefer no such system of review, its members, with one dissent, accepted as a working premise NSA's concern that some information contained in cryptology manuscripts could be inimical to the national security of the United States and see the proposed system as a potential way to test that working premise. The group rejected a compulsory statutory solution to the perceived problem.



2^56 combinations
(72,057,594,037,927,936)


On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.
On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.
They'll excuse us if we don't wish them luck.
SINK CLIPPER!


STOP CLIPPER
Fuck the NSA.
DOPER
Graffiti found at 16th/Harrison, San Francisco, Mar/Apr 94
tomj@wps.com




# Protocol Failure in the Escrowed Encryption Standard

Matt Blaze
AT&T Bell Laboratories
mab@research.att.com

August 20, 1994

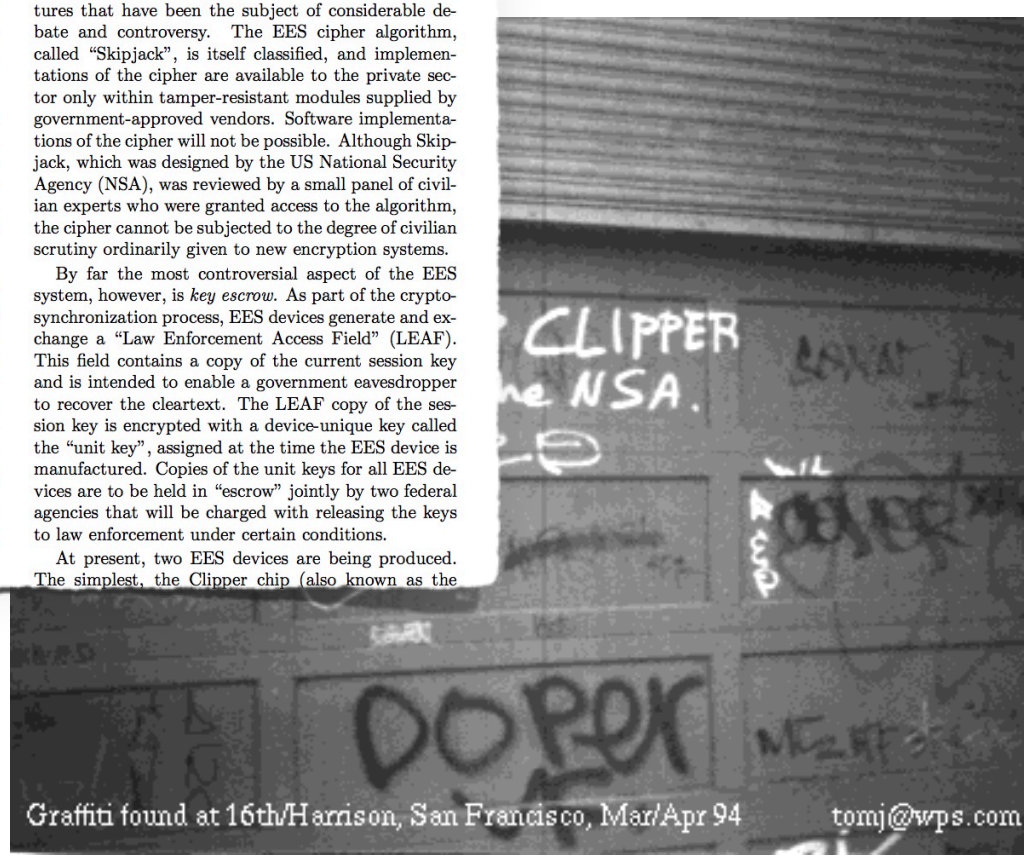
**Abstract**

The Escrowed Encryption Standard (EES) defines a US Government family of cryptographic processors, popularly known as "Clipper" chips, intended to protect unclassified government and private-sector communications and data. A basic feature of key setup between pairs of EES processors involves the exchange of a "Law Enforcement Access Field" (LEAF) that contains an encrypted copy of the current session key. The LEAF is intended to facilitate government access to the cleartext of data encrypted under the system. Several aspects of the design of the EES, which employs a classified cipher algorithm and tamper-resistant hardware, attempt to make it infeasible to deploy the system without transmitting the LEAF. We evaluated the publicly released aspects of the EES protocols as well as a prototype version of a PCMCIA-based EES device. This paper outlines various techniques that enable cryptographic communication among EES processors without transmission of the valid LEAF. We identify two classes of techniques. The simplest allow communication only between pairs of "rogue" parties. The second, more complex methods permit rogue applications to take unilateral action to interoperate with legal EES users. We conclude with techniques that could make the fielded EES architecture more robust against these failures.

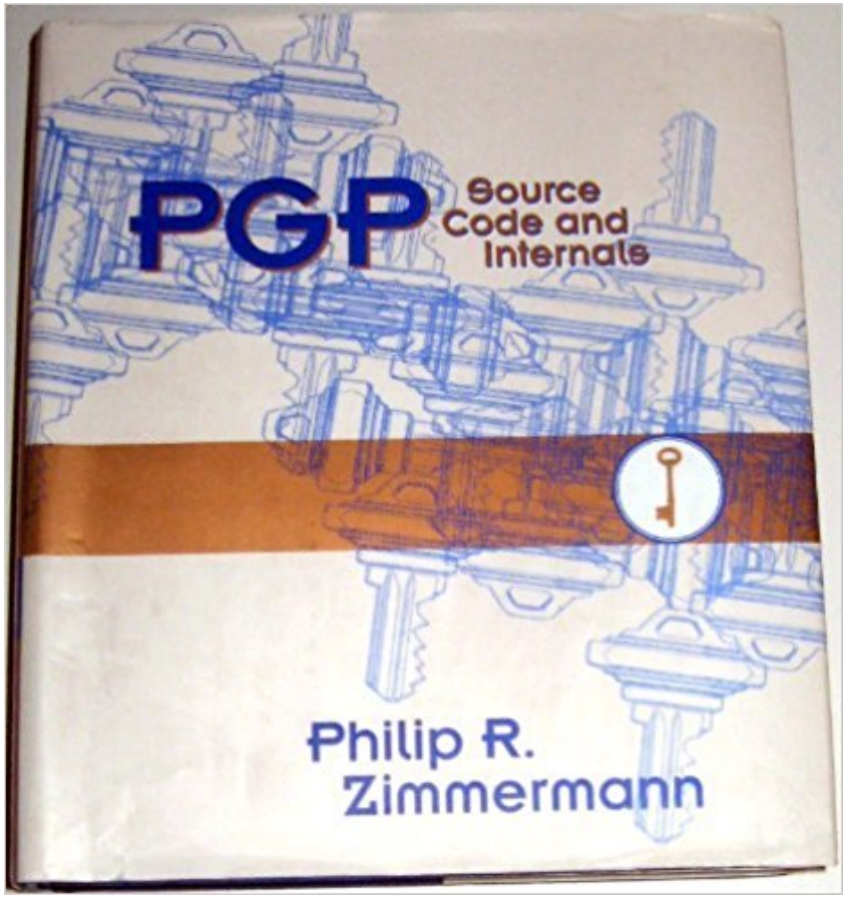
The proposal, called the Escrowed Encryption Standard (EES) [NIST94], includes several unusual features that have been the subject of considerable debate and controversy. The EES cipher algorithm, called "Skipjack", is itself classified, and implementations of the cipher are available to the private sector only within tamper-resistant modules supplied by government-approved vendors. Software implementations of the cipher will not be possible. Although Skipjack, which was designed by the US National Security Agency (NSA), was reviewed by a small panel of civilian experts who were granted access to the algorithm, the cipher cannot be subjected to the degree of civilian scrutiny ordinarily given to new encryption systems.

By far the most controversial aspect of the EES system, however, is *key escrow*. As part of the crypto-synchronization process, EES devices generate and exchange a "Law Enforcement Access Field" (LEAF). This field contains a copy of the current session key and is intended to enable a government eavesdropper to recover the cleartext. The LEAF copy of the session key is encrypted with a device-unique key called the "unit key", assigned at the time the EES device is manufactured. Copies of the unit keys for all EES devices are to be held in "escrow" jointly by two federal agencies that will be charged with releasing the keys to law enforcement under certain conditions.

At present, two EES devices are being produced. The simplest, the Clipper chip (also known as the



2^128 combinations
(340,282,366,920,938,463,463,
374,607,431,768,211,456)





BU **School of Law**
Technology & Cyberlaw Clinic

# Encryption and Export Control

*generally speaking…*

- certain applications (e.g., use in medical applications) is regulated instead by those provisions – often EAR99
- If "primary function" is not computing; networking; sending, receiving, or storing communications; or information security, the use is excluded.
  - e.g., DRM and anti-piracy, HVAC systems, certain CAD and visualization software
- "Weaker" encryption (below 56-bit symmetric, 512-bit asymmetric, or 112-bit elliptic curve) is excluded. But check.
- For other "Mass Market" items that don't qualify above, OK to self-classify and file an annual report instead of a license, though must subject to BIS and NSA inspection.

# Encryption and Export Control

*generally speaking…*

- Some things need BIS notification and 30-days delay, even if "mass market"
  - certain electronic assemblies and field-programmable logic devices
  - cryptographic development kits
  - automated vulnerability analysis
  - advanced digital forensics tools
- BIS now (reluctantly) exempts publicly available source code and object code for encryption, provided you notify BIS where on the Internet you found it

# “Deemed Export”

# "Deemed Export"

15 C.F.R. § 734.13(a)(2) – ["Export" includes] Releasing or otherwise transferring "technology" or source code (but not object code) to a foreign person in the United States.

22 C.F.R. § 120.17(a)(2) – ["Export" includes] Releasing or otherwise transferring technical data to a foreign person in the United States.

# Software and Free Speech

SCHOOL OF LAW
CASE WESTERN RESERVE
UNIVERSITY

# Computing and the Law

This site will always be under construction.

---

Go to Table of Contents.

---

## Introduction

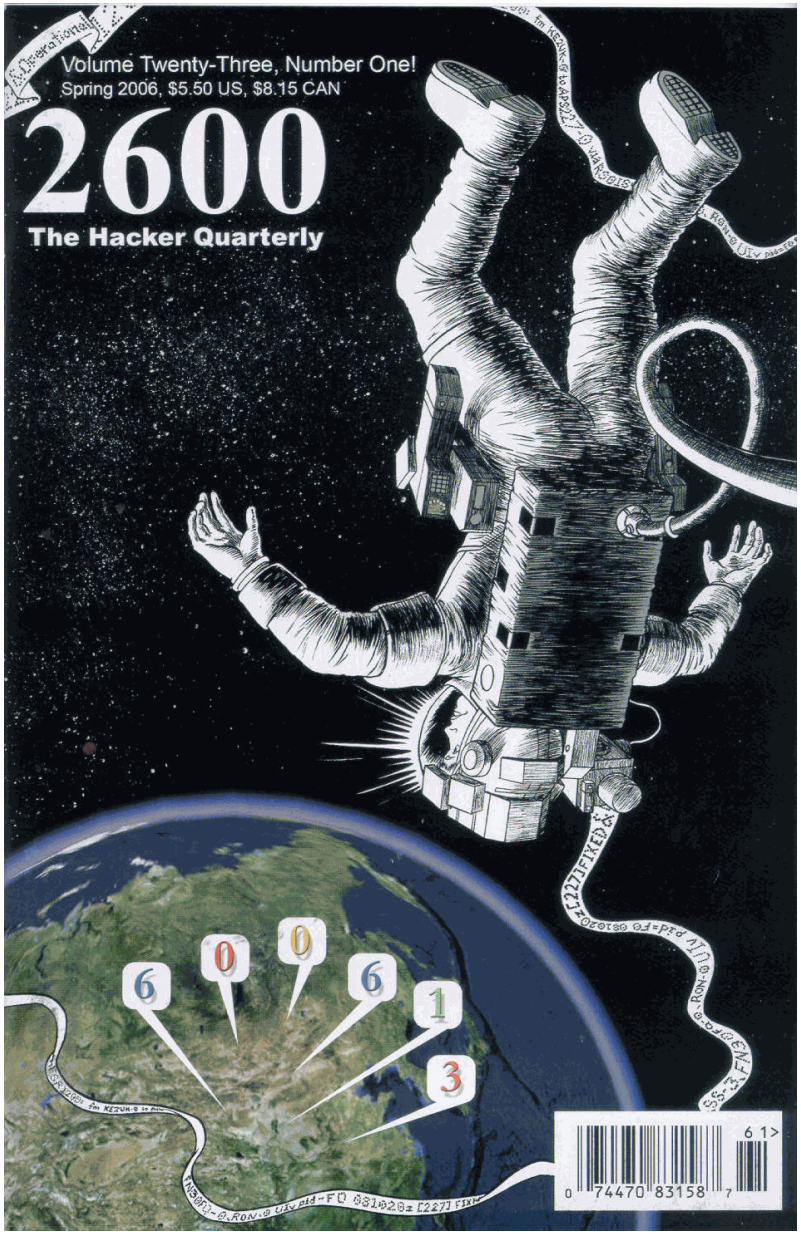
This is the WWW site for Professor Junger's course in Computing and the Law, offered at Case Western Reserve University Law School in the Fall Term of 1998. The course is scheduled to meet on Wednesday, Thursday, and Friday at 9:30 a.m. in room A65.

A new feature of the course this year will be the Computing and the Law Electronic Discussion List that will be used both for assignments and announcements and for the discussion of the issues that arise during the year. All members of the class will be expected to subscribe to this discussion list and to check it at least once a week for assignments and announcements. Instructions on how to subscribe will be handed out at the first class meeting.

Matters are changing so rapidly in the area of Computing and the Law that it is difficult to predict exactly what will be covered during the semester, but it is safe to say that most---but not all---of the issues will relate to the fact that computers are first and foremost tools that are used in the manipulation of symbols and that most activities involving computing involve the creation, processing, and communication of information and data. Thus one can safely assume that a considerable portion of the course will be directed towards issues of so-called ``Intellectual Property", *i.e.*, issues relating to the patenting and copyrighting of computer software and also to the application of copyright law to texts and data in digital form.

And we can also expect considerable attention to be spent on the constitutional issue of whether, and to what extent, the First Amendment freedoms of speech and of the press extend to the writing of computer programs, especially as the instructor in the course is the plaintiff in the case of *Junger v. Daley* where he seeks an injunction on First Amendment grounds against the enforcement of federal export regulations that forbid the publication or other communication of cryptographic software on the Internet or the World Wide Web or through other electronic means.

DVD VIDEO™




BU School of Law
Technology & Cyberlaw Clinic

DEFENSE DISTRIBUTED
ANTI-MONOPOLIST DIGITAL PUBLISHING.

HOME ABOUT DOWNLOADS PRESS SHOP

DD History
Current Projects
Contact DD

## ABOUT DEFENSE DISTRIBUTED

Defense Distributed is a corporation organized in the state of Texas.

The specific purposes for which this corporation is organized are: To defend the human and civil right to keep and bear arms as guaranteed by the United States Constitution and affirmed by the United States Supreme Court; to collaboratively produce, publish, and distribute to the public information and knowledge related to the digital manufacture of arms.

### Additional Information:

› Learn about DD's achievements
› Learn more about DD's founding

## NEWSLETTER

Email address Sign Up

## GHOST GUNNER

United States Department of State

*Bureau of Political-Military Affairs*
*Office of Defense Trade Controls Compliance*
*Washington, D.C. 2052*

In reply refer to
[redacted]

Mr. Cody Wilson
Defense Distributed
[redacted]

Dear Mr. Wilson:

The Department of State, Bureau of Political Military Af
Trade Controls Compliance, Enforcement Division (DTCC/EN
compliance with and civil enforcement of the Arms Export Control Act (22 U.S.C.
2778) (AECA) and the AECA's implementing regulations, the
Arms Regulations (22 C.F.R. Parts 120-130) (ITAR). The AEC
certain requirements and restrictions on the transfer of, and acce
articles and related technical data designated by the United Stat
(USML) (22 C.F.R. Part 121).

DTCC/END is conducting a review of technical data mac
Defense Distributed through its 3D printing website, DEFCAD.
which appear to be related to items in Category I of the USML.
may have released ITAR-controlled technical data without the r
authorization from the Directorate of Defense Trade Controls (I
the ITAR.

Technical data regulated under the ITAR refers to inform
design, development, production, manufacture, assembly, opera
maintenance or modification of defense articles, including infor
blueprints, drawings, photographs, plans, instructions or docum
definition of technical data, see § 120.10 of the ITAR. Pursuan

DTCC/END requests that Defense Distributed submit its CJ requests within three weeks of receipt of this letter and notify this office of the final CJ determinations. All CJ requests must be submitted electronically through an online application using the DS-4076 Commodity Jurisdiction Request Form. The form, guidance for submitting CJ requests, and other relevant information such as a copy of the ITAR can be found on DDTC's website at http://www.pmddtc.state.gov.

Until the Department provides Defense Distributed with final CJ determinations, Defense Distributed should treat the above technical data as ITAR-controlled. This means that all such data should be removed from public access immediately. Defense Distributed should also review the remainder of the data made public on its website to

Additionally, DTCC/END requests information about the procedures Defense Distributed follows to determine the classification of its technical data, to include the aforementioned technical data files. We ask that you provide your procedures for determining proper jurisdiction of technical data within 30 days of the date of this letter to Ms. Bridget Van Buren, Compliance Specialist, Enforcement Division, at the address below:

Office of Defense Trade Controls Compliance
[redacted]

We appreciate your full cooperation in this matter. Please note our reference number in any future correspondence.