Encryption and the Law (Part 2)

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

Thursday – 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

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 (usually, maybe…)

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

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:

On 01/27/09 Officer Eng filed a report regarding two Boston College students who were having domestic issues. The reporting party was identified as [redacted] and the other student was identified as Riccardo F. Calixte. The roommate issues are being addressed by 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] is not only a named witness to these allegations but also a reliable witness in another investigation which he brought to our attention.

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] [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.

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

[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 that the computer was registered as a guest (rather than the usual studer 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, 2009 17:44:12
IP Lease End Time	Sunday, March 8, 2009 4:38:58

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.

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.

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 ac
Massachusetts General Law, Chapt
be located in the premises and in th

…facts and circumstances that would lead a person "of reasonable caution" to believe that the search will reveal evidence of criminal activity or contraband?

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…
  - …except for cell-site location information, *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))

No REP…

- Voluntarily surrendering information
- Information disclosed to third parties…
  - **…except for cell-site location information, *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))

Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley*, 573 U.S., at ——, 134 S.Ct., at 2484. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes

when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements. *Smith*, 442 U.S., at 745, 99 S.Ct. 2577.

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

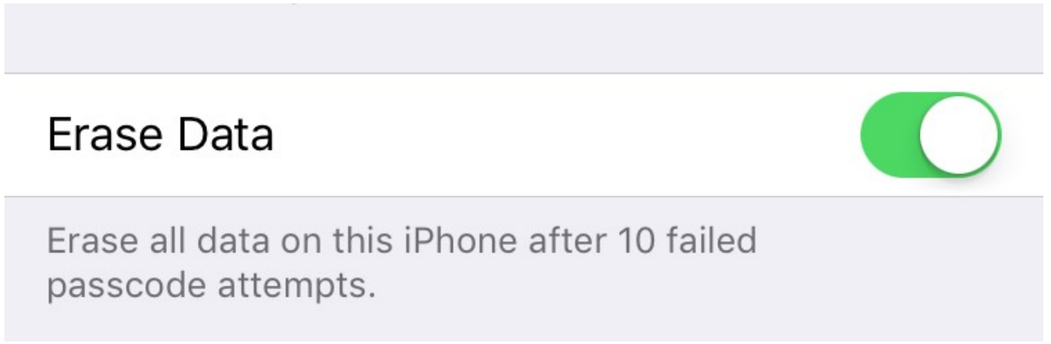
- All content and metadata in storage
- Differing levels of process for different types of information:
  - basic subscriber info – subpoena
  - most non-content records – "specific facts" showing "grounds to believe" that info. is "relevant and material"
  - content – search warrant (but maybe less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

… 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, and then brute force it?
- Compel the witness/target/suspect to unlock it?
- Compel the software manufacturer to design a break?

… but what if it doesn't work?

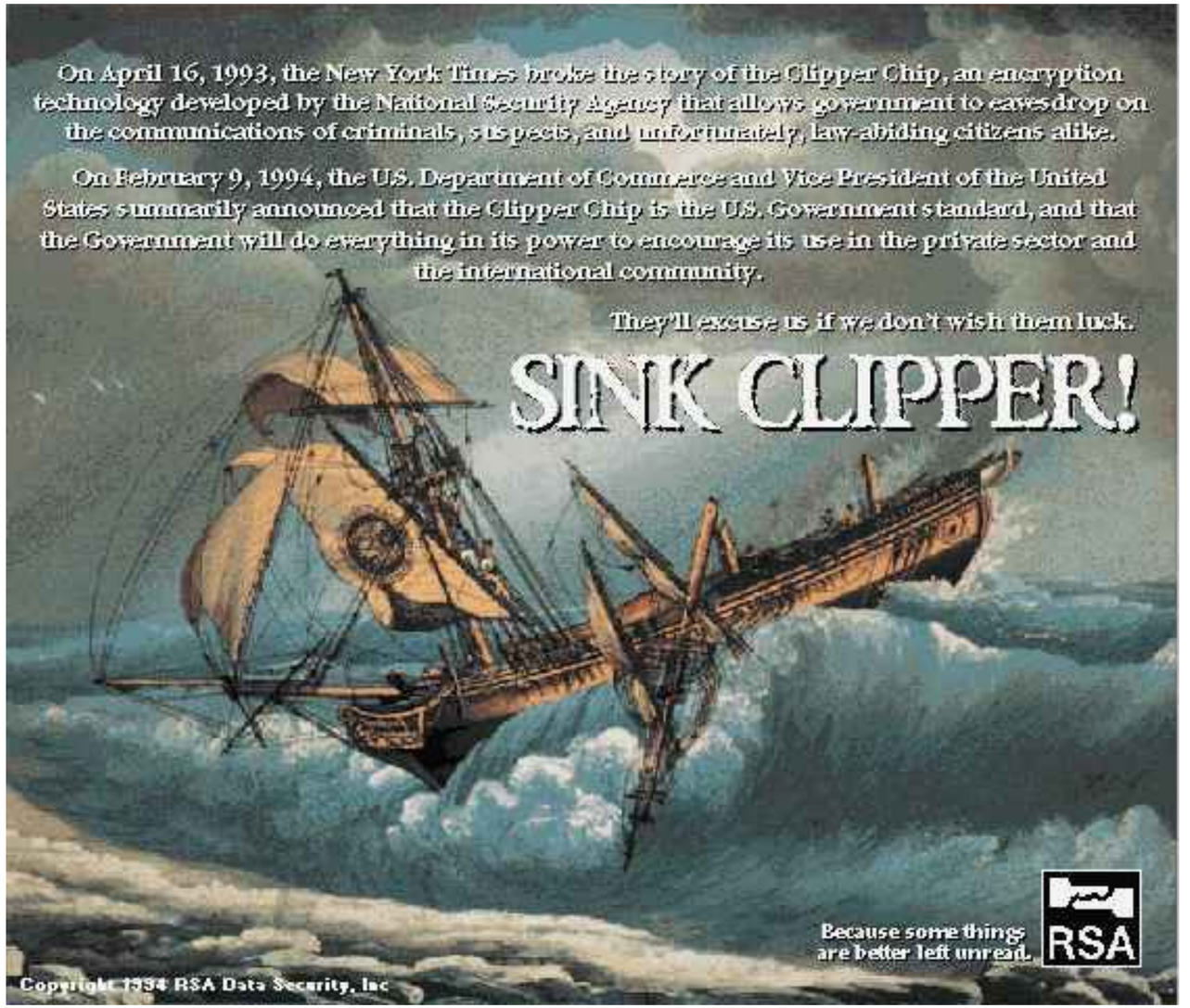
- **Force companies to use worse crypto?**
- Compel the witness/ target/suspect to unlock it?
- Compel the software manufacturer to design a break?

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?

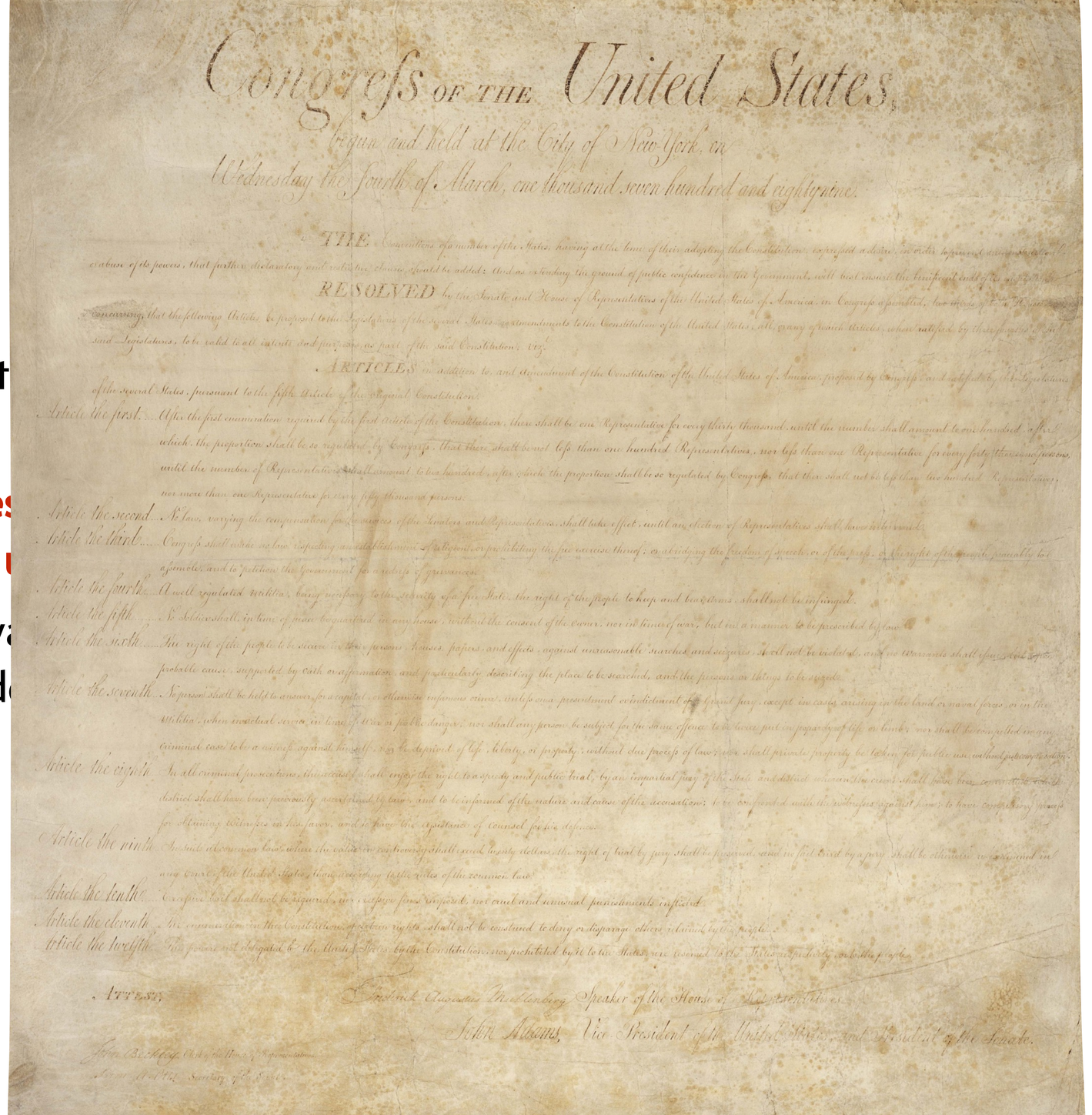
- **Force companies to use worse crypto?**
- Compel the witness/ target/suspect to unlock it?
- Compel the software manufacturer to design a break?



… 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?

- Force companies t
  worse crypto?
- **Compel the witnes
  target/suspect to u**
- Compel the softwa
  manufacturer to d
  break?



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?

Plead the Fifth?

- Has to be "testimonial" and "incriminating"
- "Foregone conclusion doctrine" prevents use of this to prevent disclosure of info the government already knows you have
- 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 unlo**
- Compel the software manufacturer to design break?

Harvard Journal of Law & Technology
Volume 32, Number 1 Fall 2018

COMPELLED DECRYPTION AND THE FIFTH AMENDMENT: EXPLORING THE TECHNICAL BOUNDARIES

*Aloni Cohen & Sunoo Park**

TABLE OF CONTENTS

ifth?

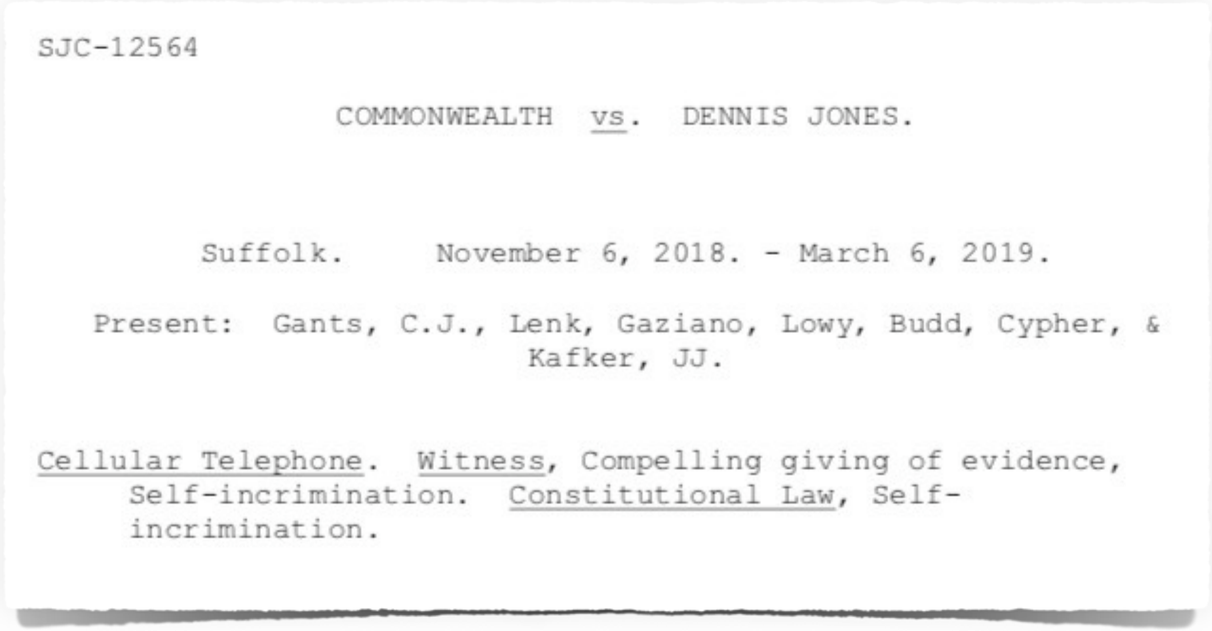
and "incriminating"

octrine" prevents use
ure of info the
ws you have

ocked phones are
d to be strongest
t already show that
word on the device in

… but what if it doesn't work?

Plead the Fifth?



SJC-12564

COMMONWEALTH vs. DENNIS JONES.

Suffolk. November 6, 2018. - March 6, 2019.

Present: Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.

Cellular Telephone. Witness, Compelling giving of evidence, Self-incrimination. Constitutional Law, Self-incrimination.

- Has to be "testimonial" and "incriminating"
- "**Foregone conclusion doctrine**" prevents use of this to prevent disclosure of info the government already knows you have
- 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

SJC-12564

COMMONWEALTH vs. DENNIS JONES.

Suffolk. November 6, 2018. - March 6, 2019.

Present: Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.

Cellular Telephone. Witness, Self-incrimination. Cor incrimination.

Accordingly, for the foregone conclusion exception to apply, the Commonwealth must establish that it already knows the testimony that is implicit in the act of the required production. Id. at 522-523. In the context of compelled decryption, the only fact conveyed by compelling a defendant to enter the password to an encrypted electronic device is that the defendant knows the password, and can therefore access the device.[9] See id. See also Kerr, Compelled Decryption and the

SJC-12564

COMMONWEALTH vs. DENNIS JONES.

Suffolk. November 6, 2018. - March 6, 2019.

Present: Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, &

Cellular Tele
Self-inc
incrimi

of the phone"). The analysis would be different had the Commonwealth sought to compel the defendant to produce specific files located in the contents of the LG phone. If that had been the case, the production of the files would implicitly convey far more information than just the fact that the defendant knows the password. See Subpoena Duces Tecum, 670 F.3d at 1347, 1349. The defendant's production of specific files would implicitly testify to the existence of the files, his control over them, and their authenticity. United States v. Hubbell, 530 U.S. 27, 36 n.19 (2000) ("by producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic"). Accordingly, the Commonwealth would be required to prove its prior knowledge of those facts.

SJC-12564

COMMONWEALTH vs. DENNIS JONES.

Suffolk. November 6, 2018. - March 6, 2019.

Present: Gants, C.J., Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.

Cellular Telephone.
Self-incriminat
incrimination.

With these considerations in mind, we conclude that when the Commonwealth seeks a Gelfgatt order compelling a defendant to decrypt an electronic device by entering a password, art. 12 requires that, for the foregone conclusion to apply, the Commonwealth must prove beyond a reasonable doubt that the defendant knows the password.[14] Whatever the standard under the

At the start of the investigation of the defendant, Sara made statements to police tending to show the defendant's regular use of the LG phone. Sara stated that she would speak directly with the defendant by calling the LG phone and that she also communicated with him by exchanging text messages with the LG phone. She also explained that the defendant would regularly respond to customer text messages by using the LG phone. Additionally, an examination of Sara's phone revealed that the LG phone's telephone number was listed in the contacts section of her phone as "[]Dennis," creating the reasonable inference that, at the very least, Sara understood that the defendant could be reached by contacting the LG phone.[16]

The record also reveals that the LG phone was in the defendant's possession at the time he was arrested by police. Indeed, it was recovered from his front pants pocket. Additionally, the motion judge acknowledged that the record revealed that the defendant had characterized the telephone number of the LG phone as his telephone number to police while he was being booked following an arrest in an unrelated criminal matter approximately one month before he was arrested in this case. Subscriber information for the LG phone also revealed that the LG phone subscriber had listed a "backup" telephone number. Police records pertaining to this backup telephone number showed that it belonged to a "Dennis Jones" with the same Social Security number and date of birth as the defendant. Finally, the LG phone's CSLI records revealed that at various times, the LG phone was in the same location at the same time as another cell phone that was confirmed to be the defendant's phone. The CSLI records also revealed that the phone calls were made from the LG phone when that phone was confirmed to be miles away from the female associate who assisted the defendant in conducting prostitution (and who had her own personal phone). These facts undoubtedly create the reasonable inference that the defendant regularly used the LG phone and that he therefore knew its password.

… 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?

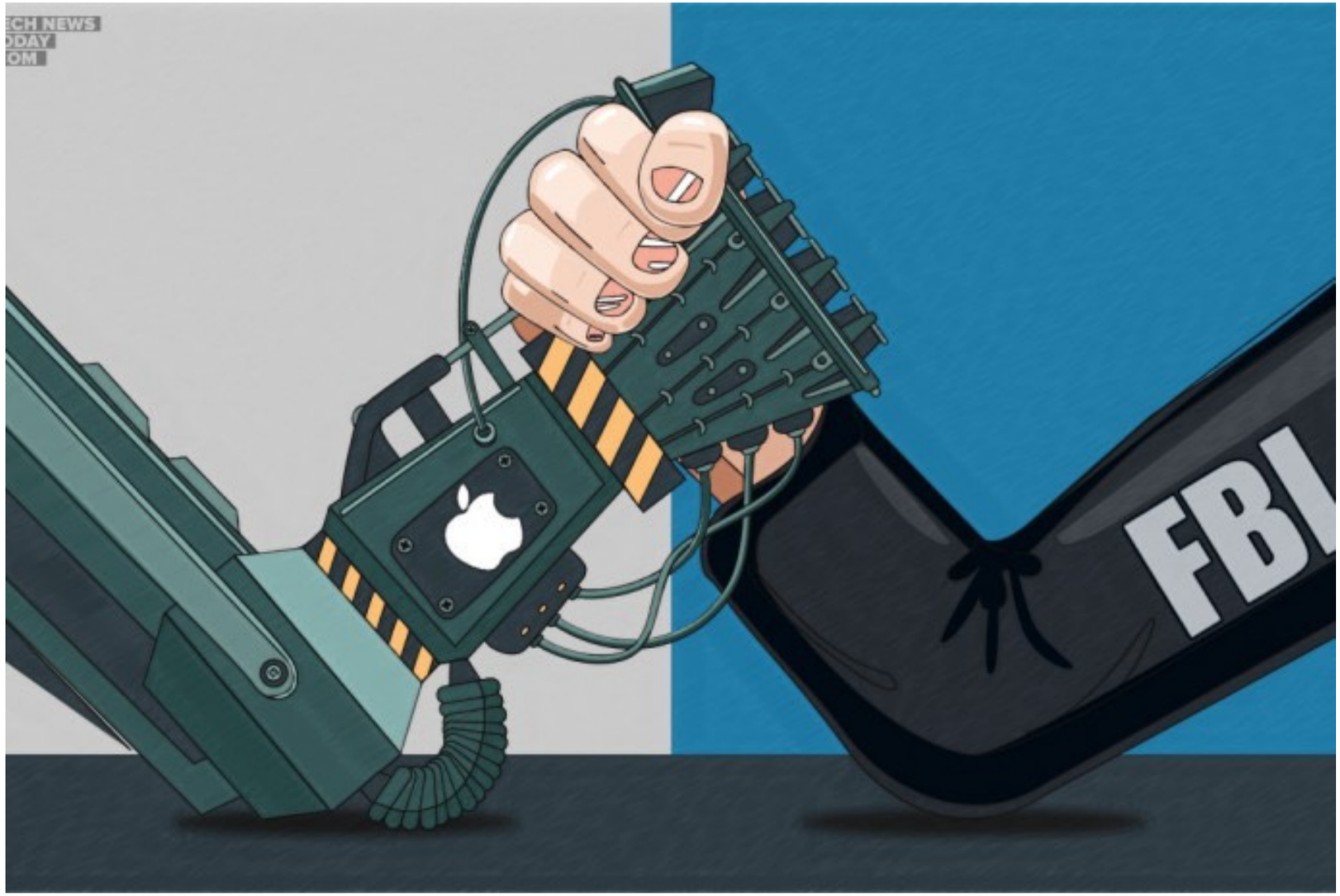
Plead the Fifth?

- Has to be "testimonial" and "incriminating"
- "Foregone conclusion doctrine" *prevents asserting the Fifth if LE can show beyond a reasonable doubt that you know the password (more or less inferred if they can show that it's your phone)*

Intro to Export Controls

… 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?**

Crypto Crumple Zones: Enabling Limited Access Without Mass Surveillance

Charles V. Wright
Portland State University, cvwright@cs.pdx.edu

Mayank Varia
Boston University, varia@bu.edu

***Abstract*—Governments around the world are demanding more access to encrypted data, but it has been difficult to build a system that allows the authorities *some* access without providing *unlimited* access in practice. In this paper, we present new techniques for maximizing user privacy in jurisdictions that require support for so-called "exceptional access" to encrypted data. In contrast to previous work on this topic (e.g., key escrow), our approach places most of the responsibility for achieving exceptional access on the government, rather than on the users or developers of cryptographic tools. As a result, our constructions are very simple and lightweight, and they can be easily retrofitted onto existing applications and protocols. Critically, we introduce no new third parties, and we add no new messages beyond a single new Diffie-Hellman key exchange in protocols that already use Diffie-Hellman.**

We present two constructions that make it possible—although arbitrarily expensive—for a government to recover the plaintext for targeted messages. First, our symmetric *crumpling* technique uses a hash-based proof of work to impose a linear cost on the adversary for each message she wishes to recover. Second, our public key *abrasion* method uses a novel application of Diffie-Hellman over modular arithmetic groups to create an extremely expensive puzzle that the adversary must solve before she can recover even a single message. Our initial analysis shows that we can impose an upfront cost in the range of $100M to several billion dollars and a linear cost between $1K-$1M per message. We show how our constructions can easily be adapted to common tools including PGP, Signal, SRTP, full-disk encryption, and file-based encryption.

1. Introduction

Since 2013, the security and privacy community has worked with renewed focus to protect Internet communications against warrantless government surveillance. In this paper, we focus on two resulting technologies that have been deployed to billions of smartphone and laptop users in a frictionless, user-friendly manner: end-to-end encrypted messaging and fine-grained encryption of data at rest. A new generation of user-friendly smartphone and web apps offer end-to-end encrypted messaging [101], including Apple iMessage [33], [48], Telegram, the Signal application along with other messaging systems like WhatsApp and Wire that implement the Signal protocol [27], [76], and a new browser-based standard for voice and video chat in WebRTC [81]. Additionally, encryption is now the norm for data at rest, in the form of full-disk encryption on all major PC operating systems and file-based encryption on the two major smartphone platforms.

The widespread proliferation of strong, seamless encryption in transit and at rest has provided billions of people with increased personal privacy and civil liberty. However, the very popularity of the encrypted systems has generated a political conflict with powerful national governments that demand some level of access to citizens' communications and files (which we refer to collectively as "messages" from now onward) [95]. These demands are usually made in the name of public safety, national security, and counter-terrorism.

Tension. In this work, we examine the tension between two essential components of modern societies: the human right to privacy and the rule of law to provide safety. With regard to encryption, we posit the following:

1) There exist a few messages whose disclosure would aid public safety and law enforcement.
2) The vast majority of messages are either irrelevant to public safety or offer insufficient value to outweigh the individual and public good from privacy.

In the physical world, justice systems around the world have spent centuries specifying and interpreting laws like the 4th Amendment to the US Constitution in an effort to find an appropriate balance between these competing objectives. In the digital world, the law enforcement and technology communities largely agree on the aforementioned two premises, but their different prioritization between the two has led to absolutist positions whereby law enforcement authorities' decryption abilities should be either technologically cheap (i.e., restricted only by judicial oversight) or effectively impossible. We seek a middle ground between these two extremes.

Governments around the world have bifurcated along these absolutist positions. According to a recent report [63], more than half of the world's population lives in countries where strong end-to-end encryption is already illegal without some sort of backdoor or assistance for the authorities. For example, Blackberry was almost pushed out of India in 2010 until they agreed to provide governmental access [9] to customers' communications, and WhatsApp has been repeatedly banned in Brazil after failing to deliver decrypted messages under a court order. Even in Western democracies with strong traditions of civil liberties, support for strong encryption is falling among citizens and their

“Export Control”

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.

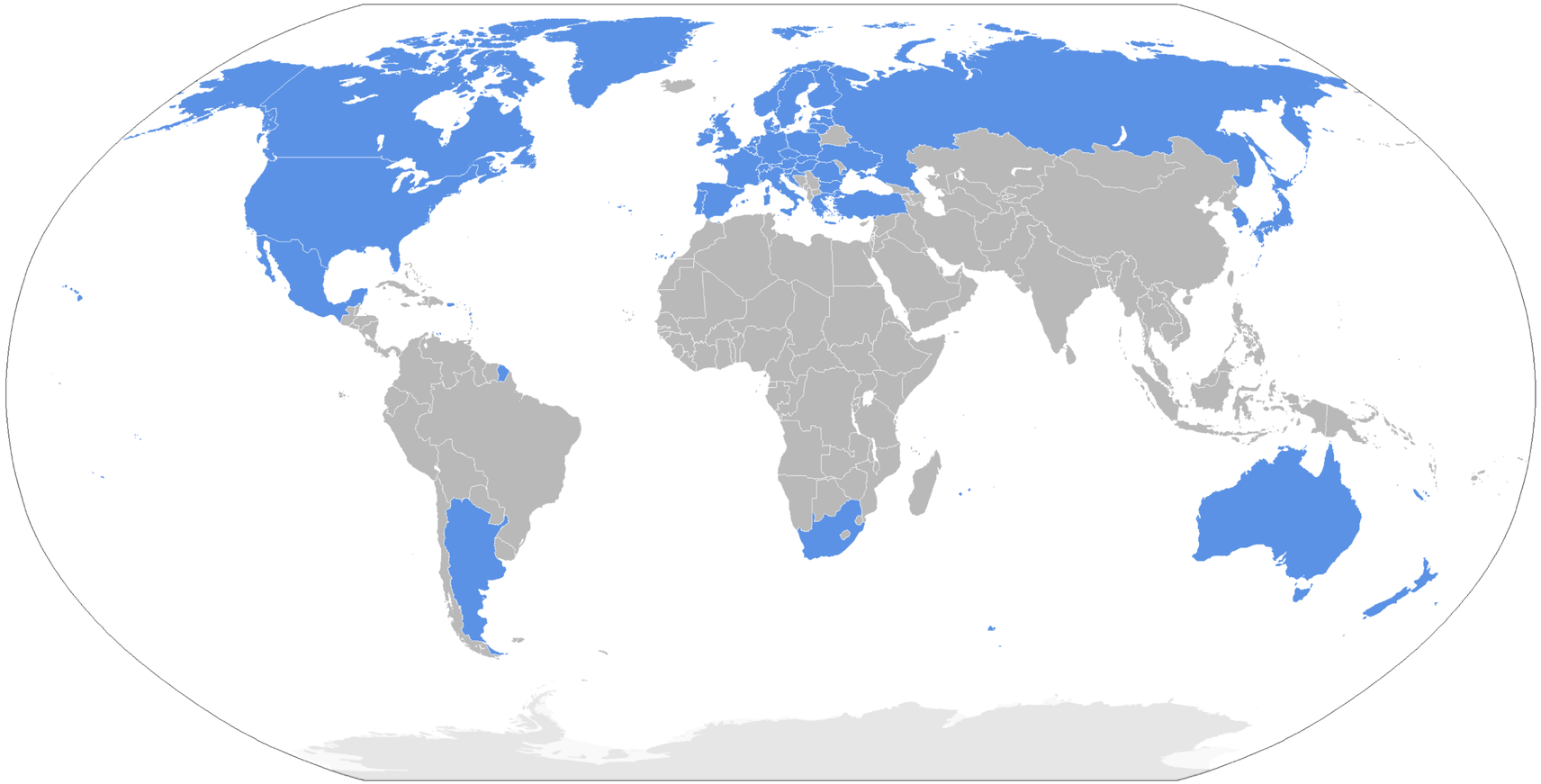
Legal restrictions on technology information

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)

Adhering to Export Administration Regulations

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

Chirinos, Carlos Fernando	68 FR 52436	2003-09-03
Chitron Electronics, Inc.	76 FR 70805	2011-11-15
Chornoletskyy, Ernest (a.k.a. Erik September, 1984	78 FR 66984	2013-11-07

					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

DERIPASKA, Oleg Vladimirovich, Moscow, Russia; 64 Severnaya Street, Oktyabrsky, Khutor, Ust-Labinsky District, Krasnodar Territory 352332, Russia; 5, Belgrave Square, Belgravia, London SW1X 8PH, United Kingdom; DOB 02 Jan 1968; POB Dzerzhinsk, Nizhny Novgorod Region, Russia; citizen Russia; alt. citizen Cyprus; Gender Male (individual) [UKRAINE-EO13661] [UKRAINE-EO13662].

Appropriate *Federal Register* Citations: 77 F.R. 34339 6/11/12			
CHITRON (HK) ELECTRONICS COMPANY LIMITED ROOM 05 13/F NANYANG PLAZA, NO. 57 HUNG TO ROAD, KWUM TONG, KOWLOON , HK	06/04/2012	01/28/2021	Standard
Appropriate *Federal Register* Citations: 77 F.R. 34339 6/11/12			
CHITRON ELECTRONICS COMPANY LIMITED 2127 SUNGANG ROAD, HUATONG BUILDING 19/F, LUOHU DISTRICT, SHENZHEN, CN, 518001	06/04/2012	01/28/2021	Standard
Appropriate *Federal Register* Citations: 77 F.R. 34339 6/11/12			
CHITRON ELECTRONICS, INC. 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			
CHUN HAI CHENG			

Adhering to Export Administration Regulations

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

- Quite broadly to those in Cuba, Iran, North Korea, Sudan, Syria
- Certain persons in governments and former governments in Belarus, Burundi, Central African Republic, Democratic Republic of the Congo, Iraq, Libya, Myanmar, Nicaragua, Russia, Somalia, South Sudan, Yemen, Zimbabwe

Adhering to Export Administration Regulations

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

15 C.F.R. § 734.3 – all US-origin items, all items in the United States, and all items that transit through the United States, but *not*:

- Items where another agency takes exclusive authority (e.g., Dep't of State with ITAR)
- **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**

Adhering to Export Administration Regulations

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

Transfer of "technology" to a foreign person in the United States ***is*** an export (a "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.

Exceptions for "Fundamental Research"

Fundamental research (EAR):

[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.
(15 C.F.R. § 734.8(c))

Fundamental research (ITAR):

Through fundamental research [...] accredited institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community. Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community [...]. University research will not be considered fundamental research if:

(i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or

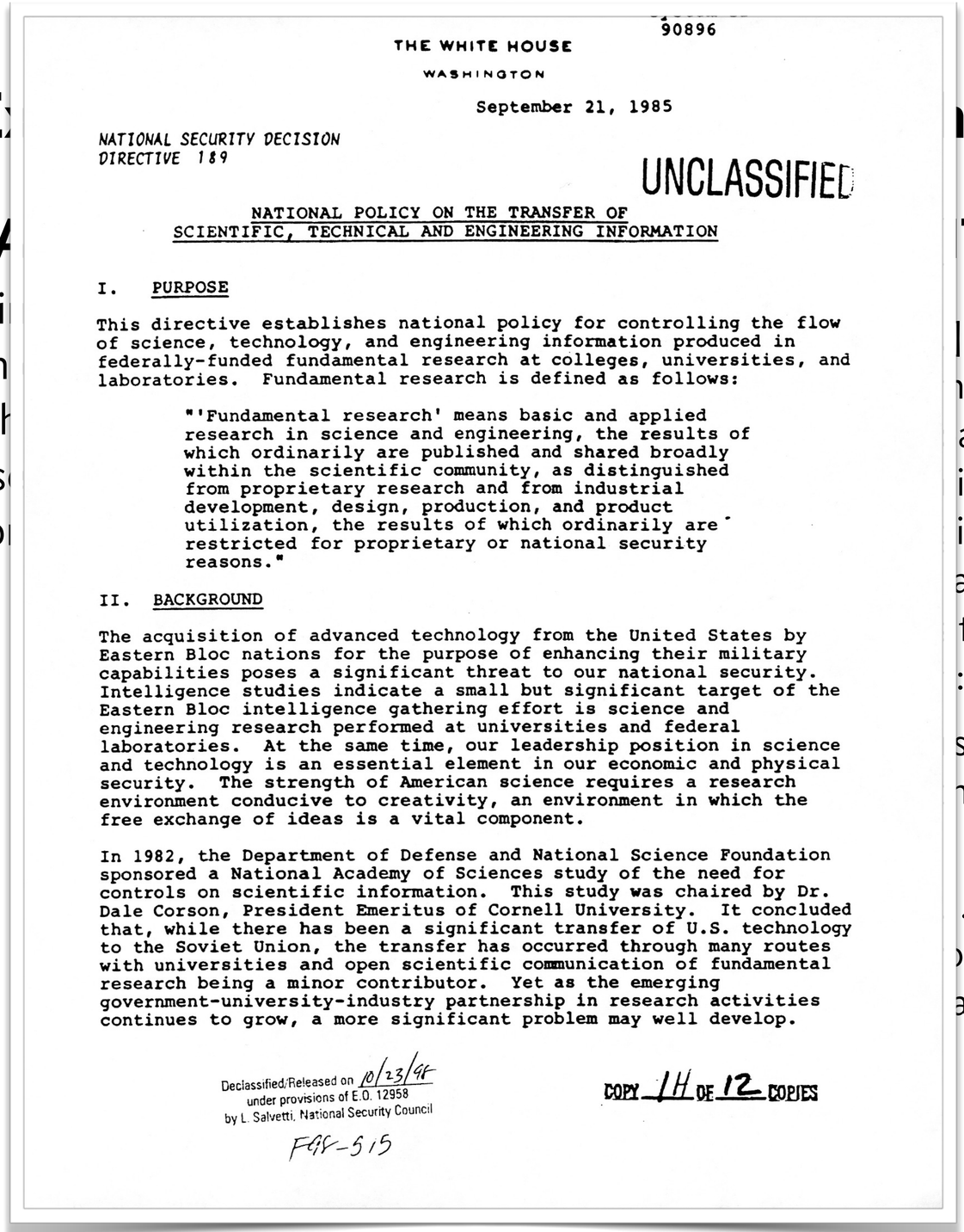
(ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

(22 C.F.R. § 120.11(8))

E

Fundamental research (EA

[M]eans research in science, engi
mathematics, the results of which
published and shared broadly with
community, and for which the res
not accepted restrictions for propr
national security reasons.
(15 C.F.R. § 734.8(c))



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.

Declassified/Released on 10/23/96
under provisions of E.O. 12958
by L. Salvetti, National Security Council
FOIA-515

COPY 1H OF 12 COPIES

n"

TAR):

| accredited institutions of
ne resulting information is
adly in the scientific
is defined to mean basic and
ineering where the resulting
and shared broadly within the
ty research will not be
.

s accept other restrictions on
nnical information resulting

.S. Government and specific
ols protecting information
applicable.

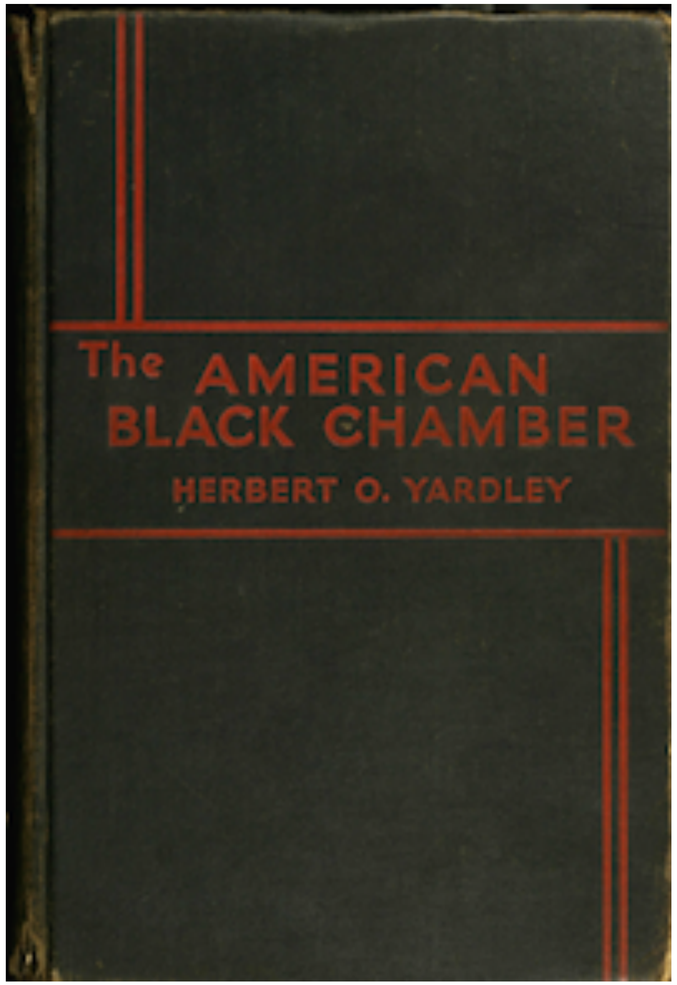
Software and Export Control

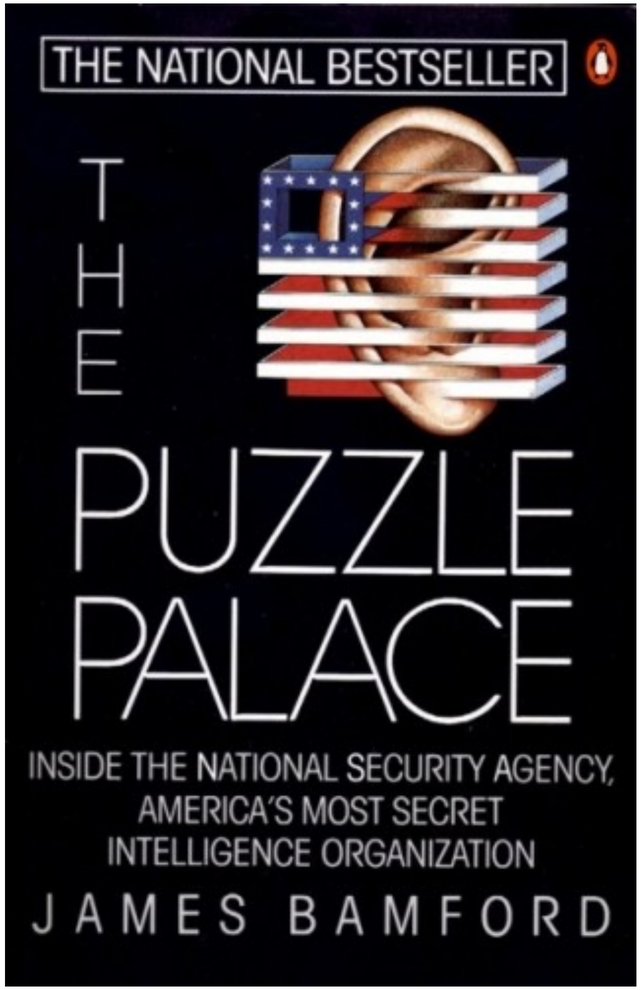
generally speaking…

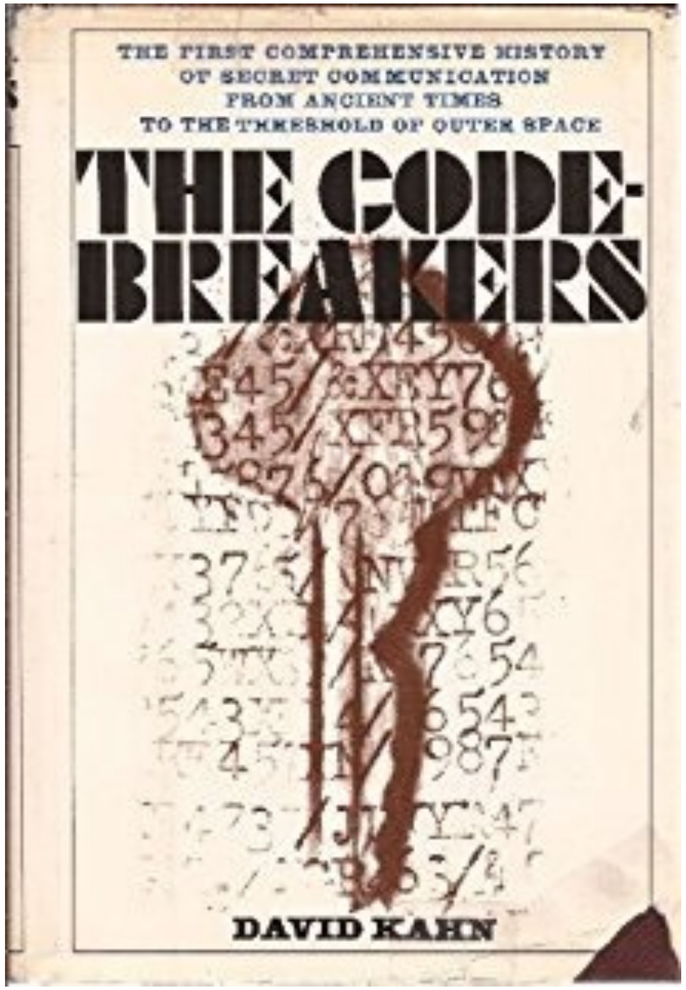
- software related to military uses or ITAR "defense articles" regulated by ITAR instead of EAR*
- software that is publicly available without charge is not restricted*
- export to Canada is not restricted, with only a few specific exceptions (software related to nuclear technology, firearms, and some 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

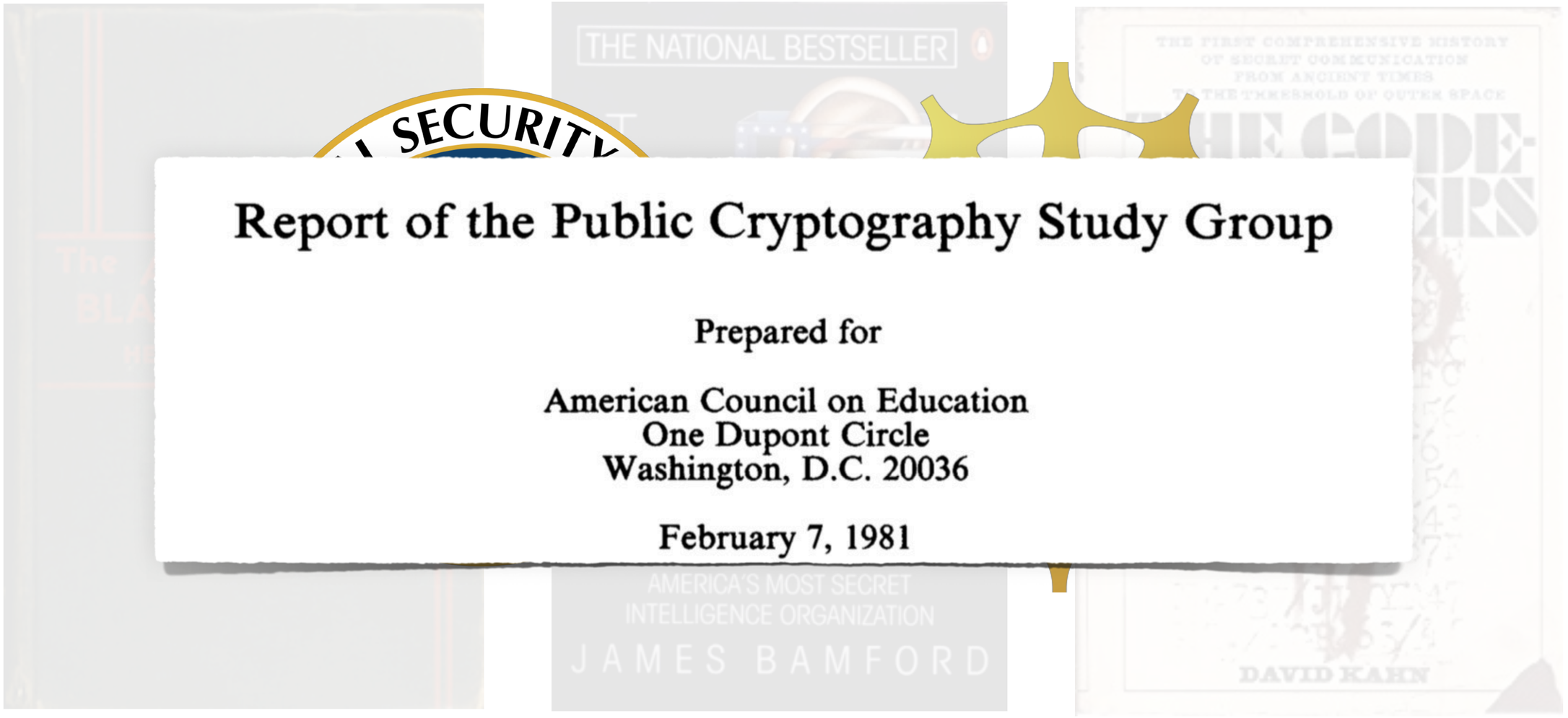

The AMERICAN BLACK CHAMBER
HERBERT O. YARDLEY


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
THE NATIONAL BESTSELLER
AMERICA'S MOST SECRET
INTELLIGENCE ORGANIZATION
JAMES BAMFORD
THE FIRST COMPREHENSIVE HISTORY
OF SECRET COMMUNICATION
FROM ANCIENT TIMES
TO THE THRESHOLD OF OUTER SPACE
DAVID KAHN

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

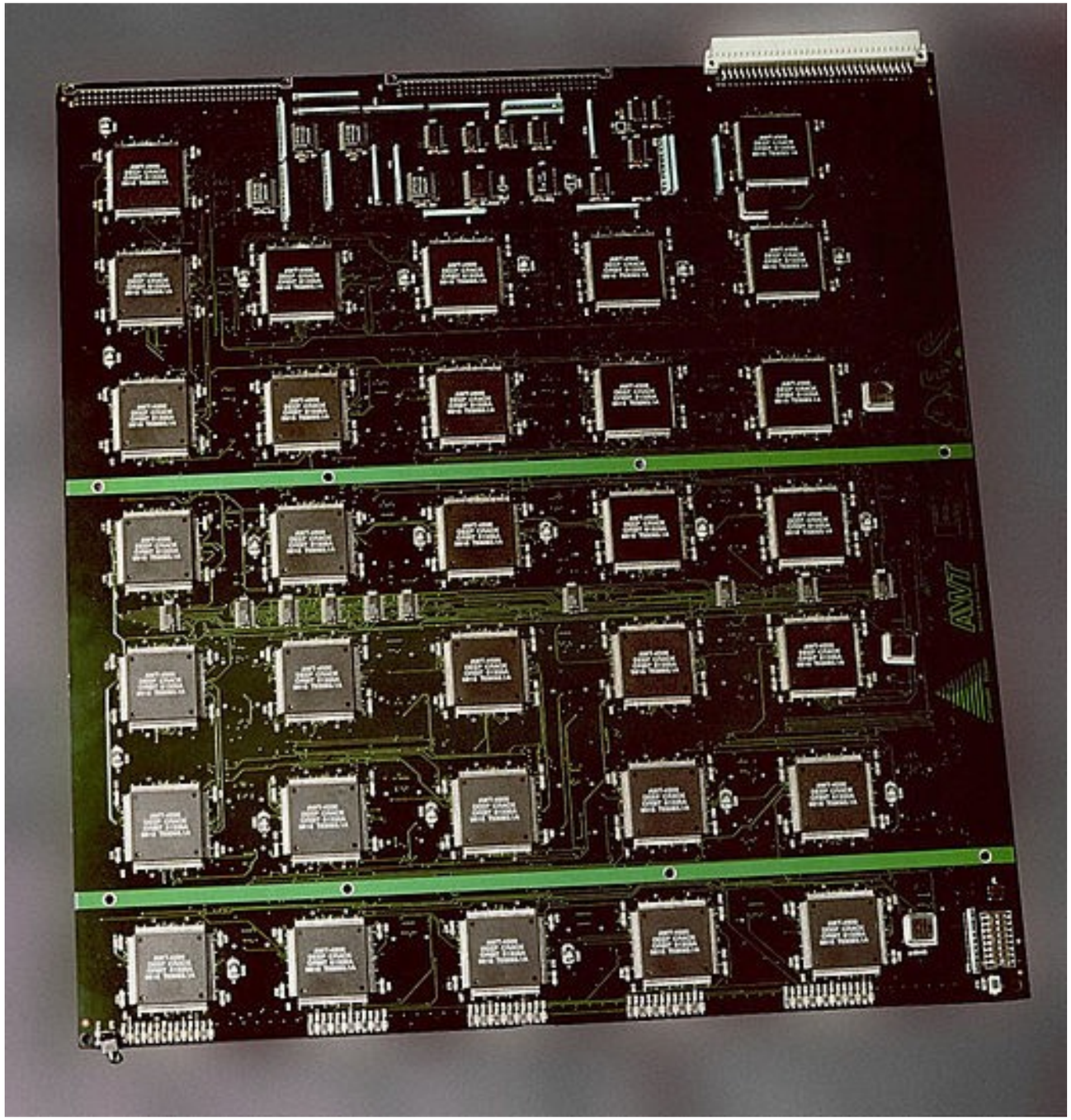
February 7, 1981

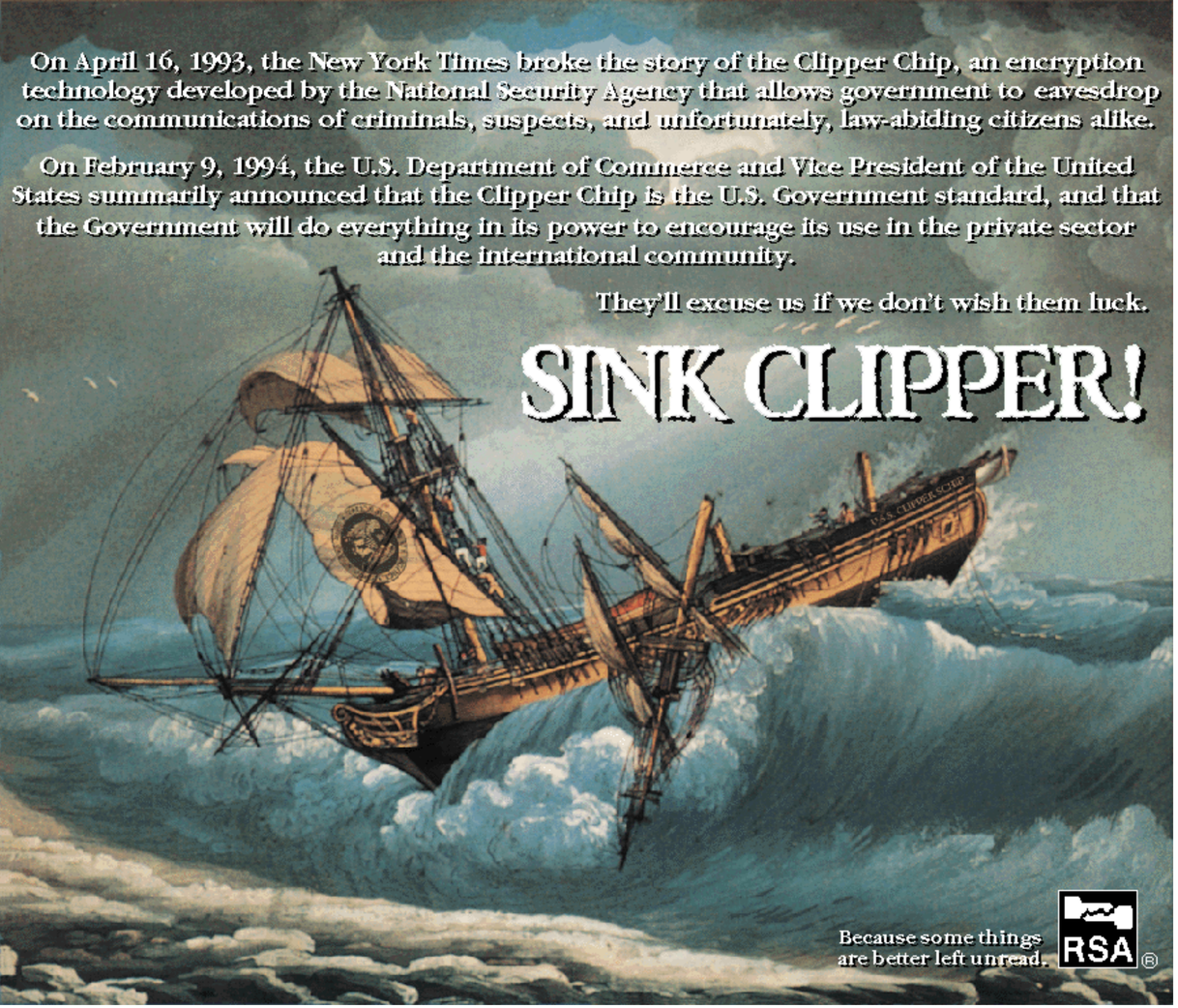
The Study Group has recommended that a voluntary system of prior review of cryptology manuscripts be instituted on an experimental basis. While the group would prefer no such system of review, its members, with one dissent, accepted as a working premise NSA's concern that some information contained in 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.

tion of business and even home computer systems from unauthorized monitoring or tampering will become increasingly important.

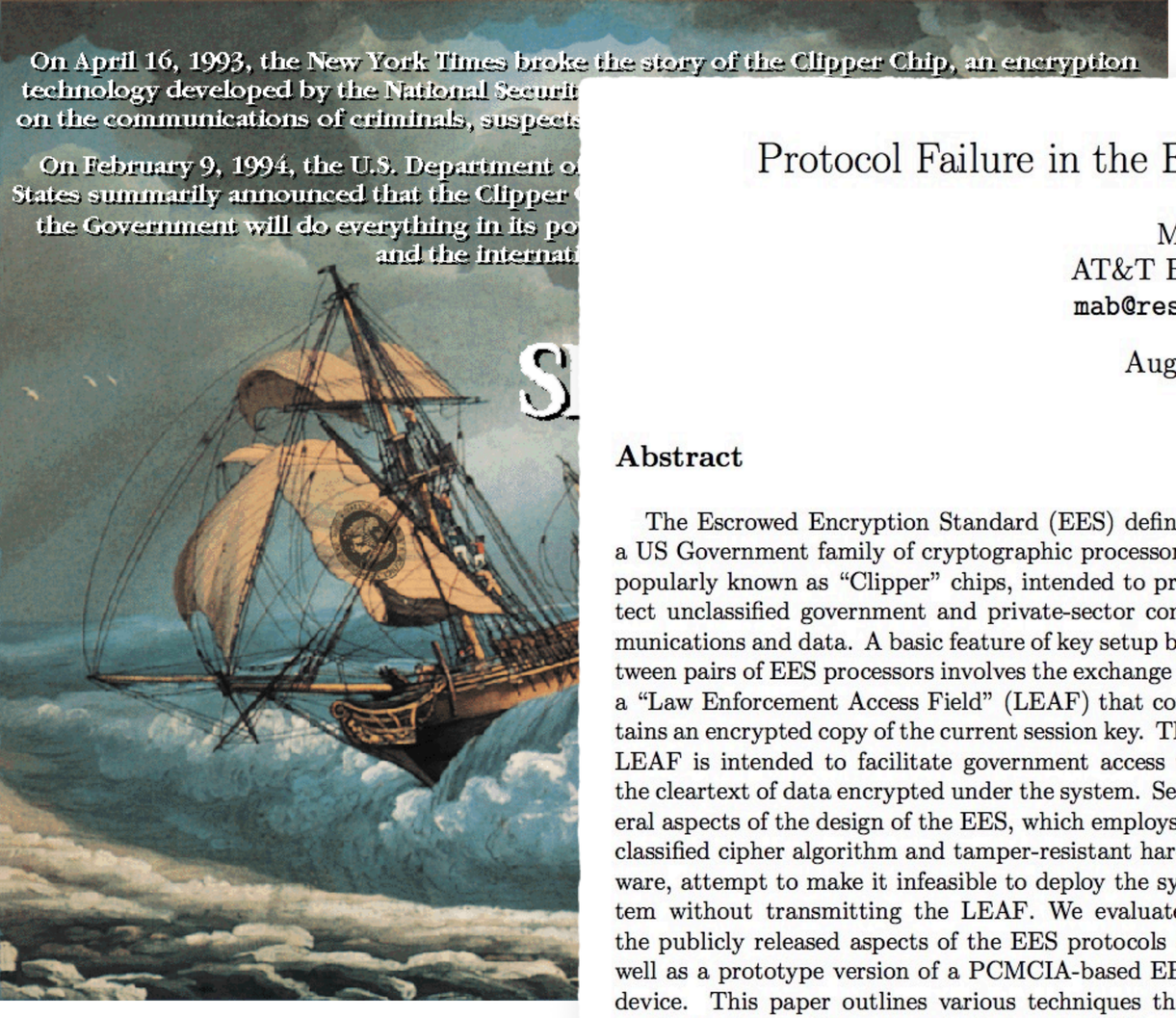
In many of these areas, cryptography is one of the most effective ways for providing the requisite security. Restriction of public research and development in cryptography might have an adverse effect on the ability of American industry to compete in world telecommunications and data-processing markets.

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!
Because some things are better left unread.
RSA


STOP CLIPPER
Fuck the NSA.
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.

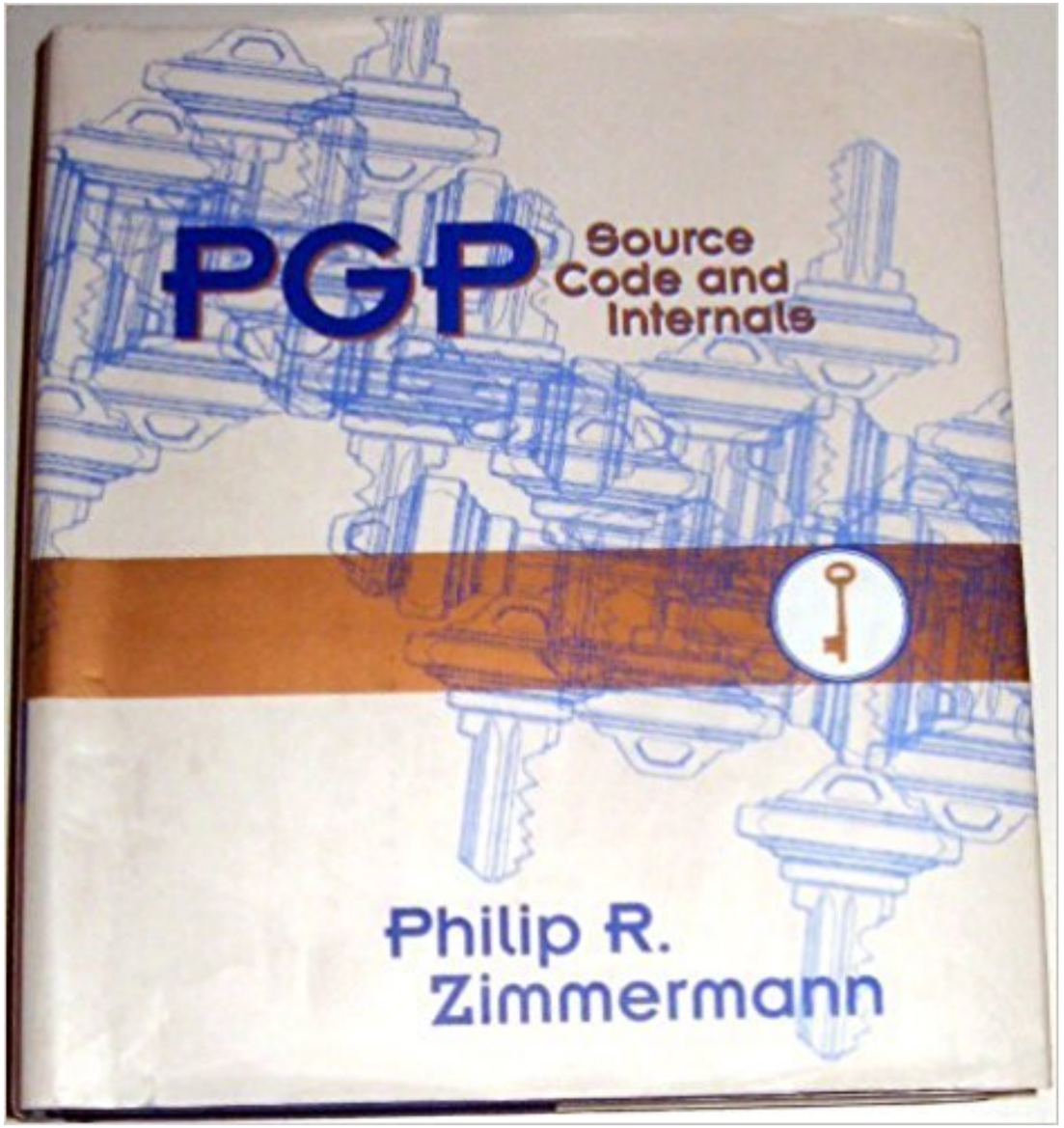
The proposal, called the Escrowed Encryption Standard (EES) [NIST94], includes several unusual features that have been the subject of considerable debate and controversy. The EES cipher algorithm, called "Skipjack", is itself classified, and implementations of the cipher are available to the private 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.

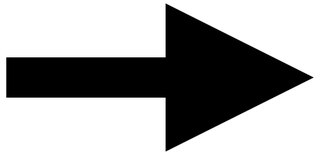
At present, two EES devices are being produced. The simplest, the Clipper chip (also known as the

Graffiti found at 16th/Harrison, San Francisco, Mar/Apr 94 tomj@wps.com

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




DEPARTMENT OF STATE
E PLURIBUS
UNUM
UNITED STATES OF AMERICA




U.S. DEPARTMENT OF COMMERCE
BUREAU OF INDUSTRY AND SECURITY

Encryption and Export Control

generally speaking…

- certain applications (e.g., use in medical applications) is regulated instead by those provisions – often easily exportable
- 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 some quirks.)
- 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