

Thomas Jefferson and Apple versus the FBI

Daniel J. Bernstein

University of Illinois at Chicago
& Technische Universiteit Eindhoven

Home Winemaking

FOR
DUMMIES®

Learn to:

- Master every step of the winemaking process
- Select the perfect grapes for your wines
- Craft a delicious range of red and white varietals
- Create sparkling, rosé, and dessert wines



1919 The Womens Christian Temperance Union requested the public library to remove books and pamphlets on the home production of alcohol for drinks. Librarian A.E. Bostwick said they would be preserved for historical value, but would not be made available to the general public.

1920 Lester Benson broadcast the Harding-Cox election returns over his experimental radio station at the Benwood Radio Company here. Benson was the first man to broadcast from a moving car. He would put the station that became WIL on the air in April 1922.

1925 The \$2 million Missouri Theatre at Grand and Morgan was dedicated. It was described as the most beautiful in America. The lobby was a replica of the chapel at Versailles.

1955 Someone in St. Louis County was taking no chances on the passage of an upcoming bond issue for road improvements. They blew up a bridge on Old Baumgartner at Mattese Creek. Engineers said the explosives had been placed perfectly to inflict maximum damage on the 80-year-old one lane bridge.

Freedom of speech

Why do censors try to ban instructions? Usual answer:
“It might be bad if people follow these instructions.”

More broadly: Why do censors try to ban information?
“It might be bad if people act upon this information.”

Freedom of speech

Why do censors try to ban instructions? Usual answer:
“It might be bad if people follow these instructions.”

More broadly: Why do censors try to ban information?
“It might be bad if people act upon this information.”

But we already have laws about people doing bad things.
Censorship adds very little benefit. Massive collateral damage.

These counterarguments generally win. Censorship is prohibited by, e.g., the First Amendment to the United States Constitution.

Narrow, carefully defined exceptions

Intentional solicitation of criminal activity:

“I’ll pay you \$1000 to steal that car for me.”

Advocacy of imminent lawless action

if it’s likely to produce such action:

“Come on, let’s go burn down that mosque!”

Many types of false information:

- Making false promises. (Breach of contract.)
- Deceiving people for profit. (Fraud.)
- Making false statements that damage reputation, with reckless disregard for the truth. (Defamation.)

OCEAN'S ELEVEN



“Nearly three hundred tons of aircraft and fuel struck the east face of the building at a speed of three hundred knots. The aircraft disintegrated on impact. No less fragile than a bird, its speed and mass had already fragmented the columns outside the walls. Next came the building itself. As soon as the wings broke up, the engines, the only really solid objects on the aircraft, shot forward, one of them actually smashing into and beyond the House Chamber . . .” —Tom Clancy, *Debt of Honor*, 1994

Emotional reaction: Clancy caused 9/11.

“Nearly three hundred tons of aircraft and fuel struck the east face of the building at a speed of three hundred knots. The aircraft disintegrated on impact. No less fragile than a bird, its speed and mass had already fragmented the columns outside the walls. Next came the building itself. As soon as the wings broke up, the engines, the only really solid objects on the aircraft, shot forward, one of them actually smashing into and beyond the House Chamber . . .” —Tom Clancy, *Debt of Honor*, 1994

Emotional reaction: Clancy caused 9/11.

Same emotional reaction to “The Kamikazes” history book etc.

Reality check: Burning books doesn't stop terrorism.

Aiding and abetting criminal activity

Recognized exception to freedom of speech:
instructions specifically intended to aid criminals.
e.g. no protection for a murder-manual publisher who “intended to provide assistance to murderers and would-be murderers”.

Aiding and abetting criminal activity

Recognized exception to freedom of speech:

instructions specifically intended to aid criminals.

e.g. no protection for a murder-manual publisher who “intended to provide assistance to murderers and would-be murderers”.

What if a “How to fish” book is used by terrorists?

What if a “Build your own secret bookcase door” book is used by criminals hiding from the police?

What if the 9/11 attackers were inspired by the Clancy novel?

These books are protected as free speech; no criminal intent.

Divide year by 100 giving result.
Add 1 to result giving century.

* Note: Always round down. Discard remainders.

Multiply century by 3 giving result.
Divide result by 4 giving leapdays.

Multiply century by 8 giving result.
Add 5 to result.
Divide result by 25 giving moondays.

Divide year by 19 giving result.
Multiply result by 19.
Subtract result from year giving J.

Multiply J by 11 giving result.
Add moondays to result.

Demystifying software

Previous slide: start of a few dozen instructions for [calculating the date of Easter](#).

You can understand these instructions.

These instructions are **software**:
a computer can understand them too.

Our computers are extensions of our brains.

They're often faster and more reliable than our brains are.
That's why we tell our computers to run software,
rather than following the same instructions by hand.

Removing the computer

Government argues that it wants new powers to censor software.

Main point of this talk: **Think about what happens when you remove the computer from the picture.**

- Could the government state the same rationale for censoring instructions followed by people?
- Are the instructions nevertheless protected as free speech?

Example: “Going dark”

Billions of people are using encryption software to protect their private files and communications.

But a few people protected by this are criminals. FBI claims that it’s “going dark”.

Should we be allowed to publish encryption software?

Let’s remove the computer from this picture.

(Col. Gwynne tells me he has sent you the first
volume of the fasciculi, and adds the 2^d. by this conveyance,
I believe I never have yet mentioned to you that publication
was undertaken last fall by Jay Hamilton and myself
1297. 1254. 470. 640. 293. 649. 1461. 227. 1247. 770. 987. 1004. 672. 451. 440.
The proposal came from the two former occasion was shown
The 492. 450. 1921. 252. 812. 1091. 1067. 1645. The 577. 918. 1293. 252. 1256.
by the sketches of Jay mostly on the two others
1461. 812. 471. 542. 546. 1352. 227. 1247. 1619. 1599. 1179. 812. 1091. 1927.
changed in consent the letters are not mutually
Though 1926. 1719. 145. 1527. 1143. 965. 812. 1076. 1155. 1470. 549. 773. 824.
unavoidable all the
479. 812. ideas of each other
925. 157. 1449. 1645. 973. for ~~the~~ 464. 764. 1952. 320. 1747. There being
seldom time for even a pencil
719. 1490. 1020. 248. 744. 101. 576. 1162. 450. of the 1095. 1156. 649. 1261.
any but the writer before they were wanted at the press
p. 6. 967. 812. 1476. 1155. 572. 1174. 1260. 1261. 920. 1759. 301. 812. 498.
sometimes, hardly by the writer himself
and 473. 1020. 1288. 1957. 1421. 812. 1470. 1155. 925. 440.

“Going dark” without the computer

Thomas Jefferson was a cryptographer.

He distributed instructions that James Madison used, by hand, to encrypt private files.

Should a modern-day Jefferson be allowed to publish a “How to encrypt” book?
What if FBI says that Jefferson is helping criminals?

This is a classic aiding-and-abetting question.

Does the publisher intend to help criminals? No.

Crypto publishers **stop criminals** and **protect human rights**.

How government lawyers try to scare courts

Typical arguments from government lawyers claiming that free speech needs a software exception:

- Imagine software to destroy navigational systems on airplanes.
- Imagine a “Super stock picker” app that’s actually malware: when you run it, it ends up giving your money to a thief.

Clearly the government needs to be able to make laws regulating software!

Scaring courts without the computer

Imagine a book called
“How to destroy navigational systems on airplanes”.

Imagine a book called “Super stock picker” that, when you follow its instructions, ends up giving your money to a thief.

Free speech doesn't include fraud, and doesn't include intentionally aiding and abetting criminal activity.

The computer is irrelevant.

The out-of-control surveillance state

- 1963: FBI Domestic Intelligence head calls Martin Luther King, Jr., the “most dangerous Negro of the future in this Nation from the standpoint of communism, the Negro and national security.”
- 1963: FBI starts surveillance of King.
- 1964: King wins the Nobel Peace Prize.
- 1964: FBI sends King an anonymous letter encouraging suicide.
- 1967: NSA starts surveillance of King.
- 1977: NSA employee Joseph Meyer threatens organizers of a crypto conference with prosecution under export laws.

The crypto wars go to court

- 1993: I send crypto paper and crypto software to NSA, asking them for permission to publish it.
- 1993: NSA refuses, classifying paper+software as “munitions” subject to export control.
- 1995: NSA tells court that its goal is to “control the widespread foreign availability of cryptographic devices and software which might hinder its foreign intelligence collection efforts”.
- 1995: NSA says that publishing paper is ok.

Imagining the crypto wars without the computer

Imagine government censors prosecuting modern-day Jefferson for publishing his “How to encrypt” book.

Easy to imagine the justification: government wants to “control the widespread foreign availability of **encryption instructions** which might hinder its foreign intelligence collection efforts.”

NSA certainly wants this control.

See, e.g., 1977 Meyer letter; 1993 paper censorship.

Imagining the crypto wars without the computer

Imagine government censors prosecuting modern-day Jefferson for publishing his “How to encrypt” book.

Easy to imagine the justification: government wants to “control the widespread foreign availability of **encryption instructions** which might hinder its foreign intelligence collection efforts.”

NSA certainly wants this control.

See, e.g., 1977 Meyer letter; 1993 paper censorship.

NSA's modified strategy after being dragged into court:
retreat to software, try to confuse judge regarding software.

The judge was not confused: part 1

Judge Marilyn Hall Patel, United States District Court for the Northern District of California, 1996: “Contrary to defendants’ suggestion, the functionality of a language does not make it any less like speech. . . . Instructions, do-it-yourself manuals, recipes, even technical information about hydrogen bomb construction, see *United States v. The Progressive. Inc.*, 467 F. Supp. 990 (W.D. Wisc. 1979), are often purely functional; they are also speech. . . .

The judge was not confused: part 2

“The music inscribed in code on the roll of a player piano is no less protected for being wholly functional. Like source code converted to object code, it ‘communicates’ to and directs the instrument itself, rather than the musician, to produce the music. That does not mean it is not speech. Like music and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who can read it.

The judge was not confused: part 3

“Defendants argue in their reply that a description of software in English informs the intellect but source code actually allows someone to encrypt data. Defendants appear to insist that the higher the utility value of speech the less like speech it is. An extension of that argument assumes that once language allows one to actually do something, like play music or make lasagne, the language is no longer speech. The logic of this proposition is dubious at best. Its support in First Amendment law is nonexistent.”

An appellate judge also figured it out

Judge Betty Fletcher, majority opinion for Ninth Circuit Court of Appeals, 1999: “The distinction urged on us by the government would prove too much in this era of rapidly evolving computer capabilities. The fact that computers will soon be able to respond directly to spoken commands, for example, should not confer on the government the unfettered power to impose prior restraints on speech in an effort to control its ‘functional’ aspects.”

Imagining Apple–FBI case without the computer

Jefferson’s “How to Encrypt” instructions are used by Madison and many other innocent people, but they’re also used by evil Farook.

As part of a sting operation against Farook, FBI demands that Jefferson write new anti-encryption instructions and falsely sign those instructions as being legitimate.

Jefferson says these instructions are “too dangerous to create”.

U.S. Supreme Court: freedom of speech includes “both what to say and what not to say”.