# Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries

•••

Aloni Cohen
Boston University,
4/9/2019

# Roadmap

1. The Fifth Amendment
2. Implicit Testimony and the Foregone Conclusion Doctrine
3. Compelled Decryption and Self-Incrimination: A Review of Cases
4. Technological Hypotheticals

Help us decrypt

I plead the 5th

# The Fifth Amendment

# "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."

Applies only to acts that are

- testimonial,
- compelled, and
- incriminating

Fisher v. United States, (1976)

# "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."

Applies only to acts that are

- testimonial,
- compelled, and
- incriminating

Not testimonial:

- Fingerprints,
- Blood sample,
- Voice exemplar,

**Evidence** may be compelled by **subpoena.**

Schmerber v. California, (1966)

# "No person . . . shall be compelled in any criminal case to be a witness against himself . . . .”

Applies only to acts that are

- testimonial,
- compelled, and
- incriminating

Not compelled:

- Voluntary confession
- Recorded conversation
- Diary

Fisher v. United States, (1976)

# "No person . . . shall be compelled in any criminal case to be a witness against himself . . . ."

Applies only to acts that are

- testimonial,
- compelled, and
- incriminating

Not incriminating:

- Grant of immunity

To simplify, let's mostly ignore this element.

Andrew T. Winkler, *Password Protection and Self-Incrimination,* (2013)

# Doe and the Bank (*Doe v US, 1988)*

"I . . . do hereby direct any bank or trust company at which I may have a bank account . . . to disclose all information . . . to Grand Jury."

Love,
John Doe

Supreme Court:
Signing this is **not testimonial,** and may therefore be **compelled.**

Contrast with made-up example:
"I do hereby direct Wells Fargo to disclose all information related to my account."

# Implicit Testimony
# and the Foregone Conclusion Doctrine

# What is Testimony?

"… disclose **the contents of his own mind.**"

*Curcio vs. US, 1957*

(There are other definitions)

Not testimony:

- Fingerprints,
- Blood sample,
- Voice exemplar

Testimony:

- Oral or written statements
- ???

# Act-of-Production Testimony (*Fisher v US, 1976*)

"Compliance with the **subpoena** tacitly concedes"

- existence
- possession or control
- authenticity

Does this make subpoenas powerless against the Fifth Amendment?

Not if the implicit testimony is a **foregone conclusion.**

# Act-of-Production Testimony (*Fisher v US, 1976)*

"Compliance with the **subpoena** tacitly concedes"

- existence
- possession or control
- authenticity

"The existence and location of the papers are **a foregone conclusion**"

"[T]he taxpayer **adds little or nothing** to the sum total of the Government's information **by conceding that he in fact has the papers.**"

(Authenticity handled separately.)

# Act-of-Production Testimony (*Fisher v US, 1976)*

"Compliance with the **subpoena** tacitly concedes"

- existence
- possession or control
- authenticity

Example

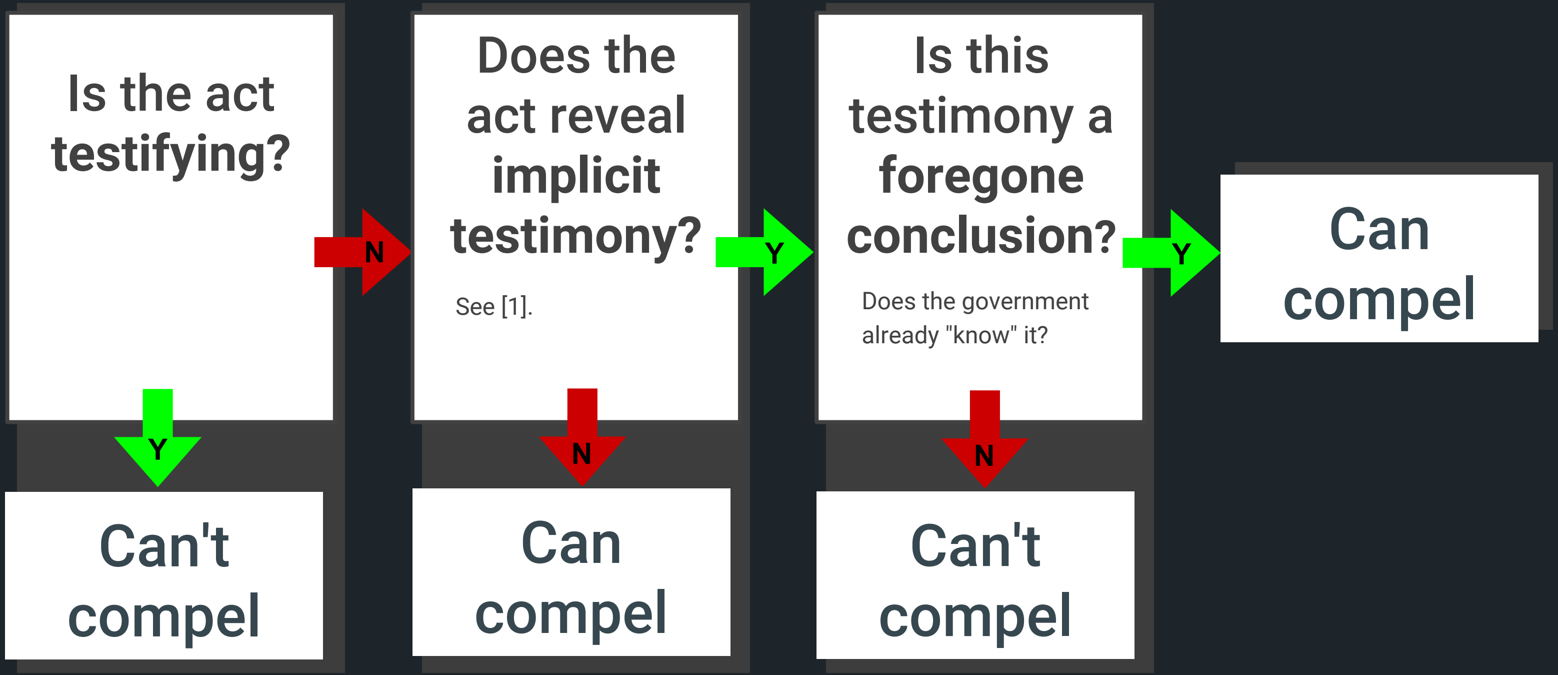
**Handwriting exemplar** admits to

- the **ability** to write
- **authenticity** of the exemplar

But,

- ability is a "**near truism**"
- authenticity is **self-evident**

# Can you compel an act?



Is the act testifying?

Can't compel

Does the act reveal implicit testimony?

See [1].

Can compel

Is this testimony a foregone conclusion?

Does the government already "know" it?

Can't compel

Can compel

[0] For simplicity, let's assume the act is **incriminating.**

[1] Usually, the **existence, possession,** and **authenticity** of the thing, corresponding to the **act of producing** that thing. Some assume that this is the **only** type of implicit testimony that matters.

# Compelled Decryption and Self-Incrimination: A Review of Cases

Disclaimer

There is much disagreement and inconsistency, among both courts and scholars, as to what the doctrine / precedent ***is*** and ***should be.***

What follows is simplified, and our own interpretation.

# General Case Outline

#@%
#@%
Help us decrypt
I plead the 5th

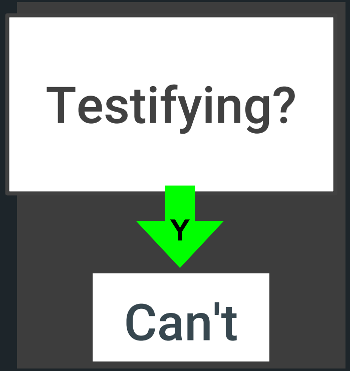
4 different ways to "help decrypt"

- Reveal the password
- Use a fingerprint
- Produce the decrypted contents
- Enter the password

The **government can choose** the type, and can **change** adaptively.

# Reveal the Password *(US v. Kirschner, 2010)*

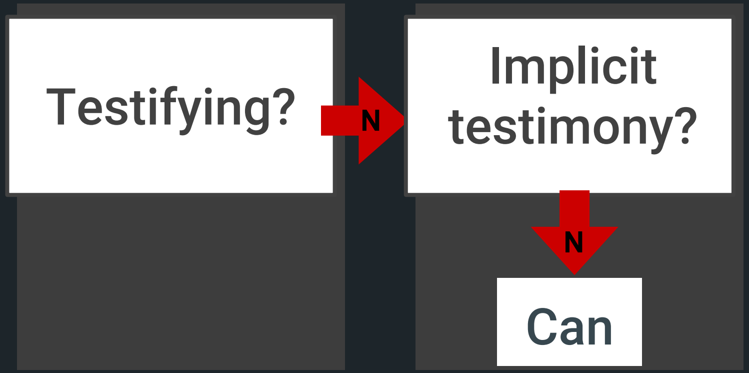
Can you compel it?



"... the government is not seeking documents or objects — it is seeking testimony ..."

# Use a Fingerprint *(Virginia v. Baust, 2014)*

Can you compel it?



Testifying?

N

Implicit testimony?

N

Can

" . . . like ***physical characteristics*** that are non-testimonial, the fingerprint of Defendant if used to access his phone is likewise nontestimonial and does not require Defendant to ***'communicate any knowledge'*** at all."

# Produce the Decrypted Contents

## US v. Doe, 2012

"The subpoena required Doe to produce the 'unencrypted contents' of the digital media, and 'any and all containers or folders thereon.' "

(Almost all cases in this category are worded like this)

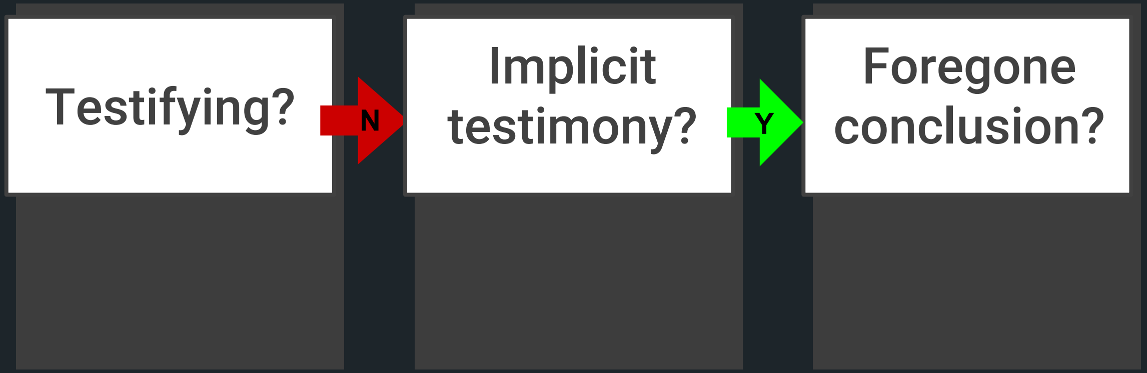
## US v. Fricosu, 2012

"The government shall provide . . .
a copy of the [encrypted] hard drive
. . .

"Fricosu shall provide. . .
an unencrypted copy of the hard drive . . ."

# Produce the Decrypted Contents *(US v. Doe, 2012)*

Can you compel it?



Testifying?

N

Implicit testimony?

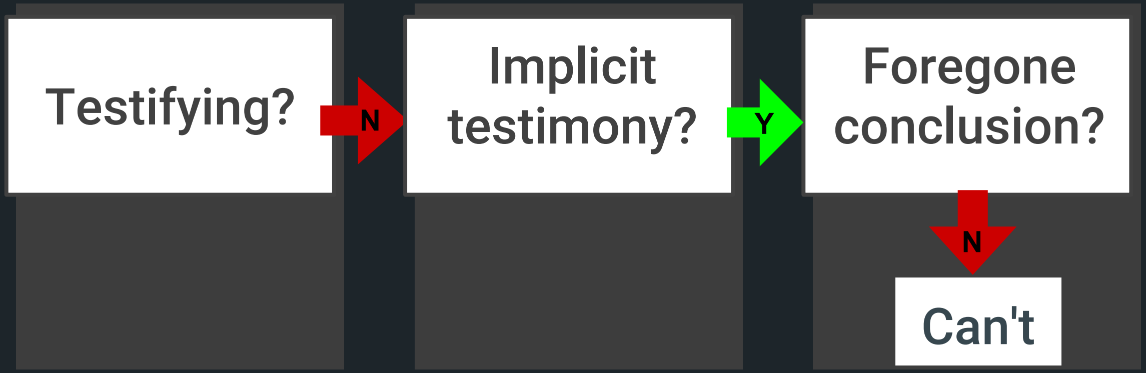
Y

Foregone conclusion?

1. Knowledge of the existence and location of potentially incriminating files;
2. Possession, control, and access to the encrypted portions of the drives;
3. Capability to decrypt the files.

# Produce the Decrypted Contents *(US v. Doe, 2012)*

Can you compel it?



Testifying?

N

Implicit testimony?

Y

Foregone conclusion?

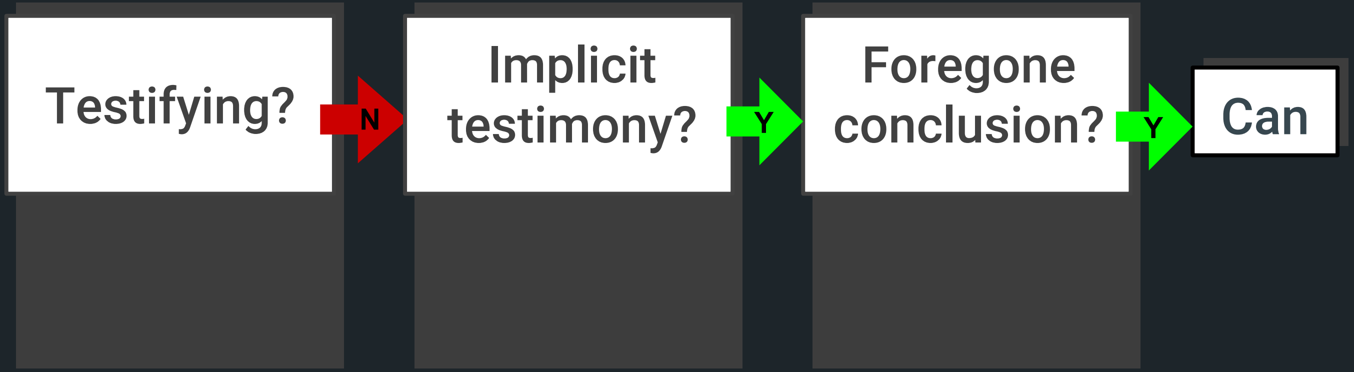
N

Can't

"Nothing in the record before us reveals that the Government knows whether any files exist and are located on the hard drives . . . [or] that Doe is even capable of accessing the encrypted portions of the drives."

# Produce the Decrypted Contents *(US v. Fricosu, 2012)*

Can you compel it?



" . . . the government has met its burden to show by a preponderance of the evidence that the . . . computer belongs to Ms. Fricosu, or, in the alternative, that she was its sole or primary user, who, in any event, **can access the encrypted contents** of that laptop computer.

# Produce the Decrypted Contents

US v. Doe, 2012

**CAN'T** compel, because implicit testimony **NOT** a foregone conclusion

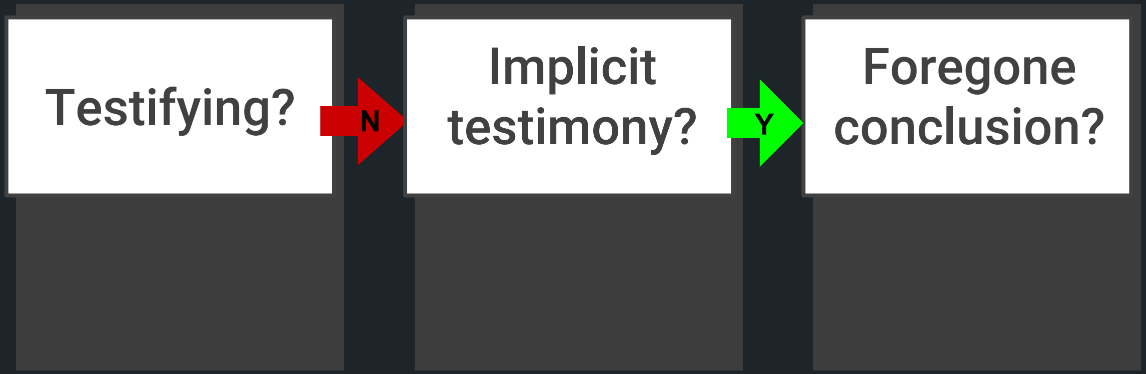
US v. Fricosu, 2012

**CAN** compel, because implicit testimony **IS** a foregone conclusion

1. Whether the production of decrypted contents can be compelled depends on facts of the case.
2. Contents are not privileged, as they were voluntarily created.

# Enter the Password *(Comm. v. Gelfgatt, 2014)*

Can you compel it?



Testifying?

N

Implicit testimony?

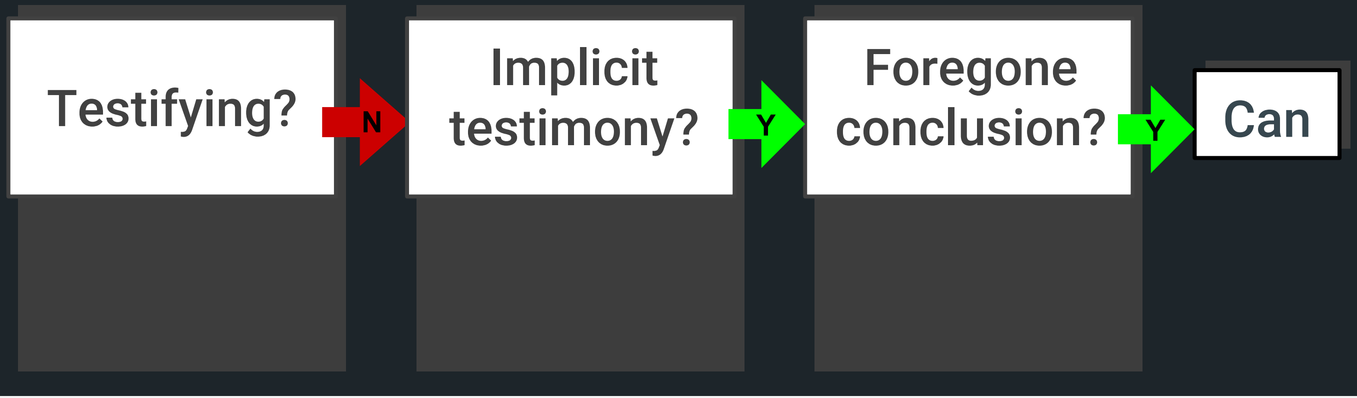
Y

Foregone conclusion?

1. Ownership and control of the computers and their contents,
2. Knowledge of the fact of encryption
3. Knowledge of the encryption key

# Enter the Password *(Comm. v. Gelfgatt, 2014)*

Can you compel it?



Testifying?

N

Implicit testimony?

Y

Foregone conclusion?

Y

Can

1. Whether the production of decrypted contents can be compelled depends on facts of the case.
2. Contents are not privileged, as they were voluntarily created.

# Act of **Production** v. Act of **Decryption**

US v. Doe

1. Knowledge of the existence and location of potentially incriminating files;
2. Possession, control, and access to the encrypted portions of the drives;
3. Capability to decrypt the files.

Comm v Gelfgatt

1. Ownership and control of the computers and their contents,
2. Knowledge of the fact of encryption
3. Knowledge of the encryption key

# Authenticity

- The government must "independently verify that the compelled documents **are in fact what they purport to be**."
- Most compelled decryption cases don't seriously examine authenticity.
- Are passwords / cryptography "self-authenticating?"

In re Grand Jury Subpoena, Dated Apr. 18, 2003, 383 F.3d at 910;
Rules of Evidence 902; State of Florida v. Stahl

*Gelfgatt*:

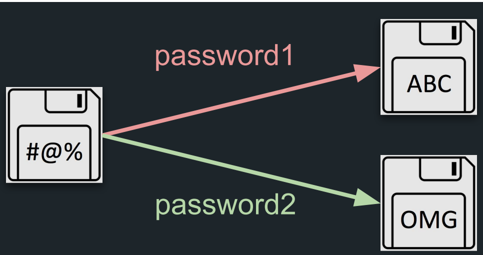
"[T]he defendant's decryption of his computers **does not present an authentication issue** analogous to that arising from a subpoena for specific documents because he is . . . **merely entering a password** into encryption software."

*Stahl*:

**If the phone** or computer **is accessible** once the passcode or key has been entered, the **passcode** or key **is authentic.**

# Technological Hypotheticals

# “Plausibly deniable” encryption

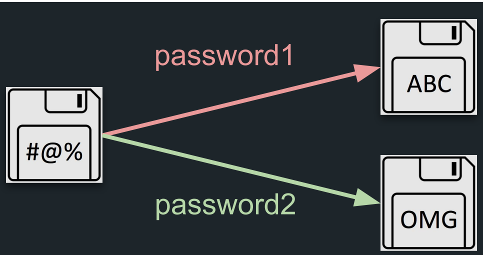


ASSUMPTION:

*“If the decryption procedure appears to be successful, its output must be correct!”*

Is authenticity of decryption really a foregone conclusion?

# “Plausibly deniable” encryption



ASSUMPTION:

*“If the decryption procedure appears to be successful, its output must be correct!”*
Is authenticity of decryption really a foregone conclusion?

**CHALLENGE:**

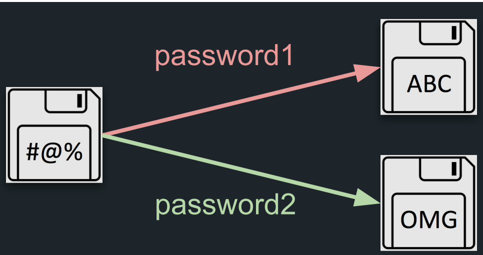
There could be 2 (or many) indistinguishable ways to decrypt a single encryption, some yielding incriminating results, and others yielding innocuous results.

- Commercially available software (Veracrypt) offers such functionality today!

POSSIBLE RESPONSES:

> *The defendant is expressly ordered not to enter a false or ‘fake’ password or key, thereby causing the encryption program to generate ‘fake, prepared information’ as advertised by the manufacturer of the encryption program.*
>
> — **Gelfgatt**

# “Plausibly deniable” encryption



**ASSUMPTION:**

*“If the decryption procedure appears to be successful, its output must be correct!”*
Is authenticity of decryption really a foregone conclusion?

**CHALLENGE:**

There could be 2 (or many) indistinguishable ways to decrypt a single encryption, some yielding incriminating results, and others yielding innocuous results.

- Commercially available software (Veracrypt) offers such functionality today!

**POSSIBLE RESPONSES:**

- ➔ Forbid use of “duress password” (*Gelgatt*), ignoring the authenticity issue?
- ➔ Demonstrate that the defendant is not using deniable encryption?
- ➔ Demonstrate specific use of deniable encryption, and demand both decryptions?

Against sophisticated defendants, may need specific **knowledge of contents?**

# Kill switches

ASSUMPTION:

*“We saw the data on your laptop before you shut it off, so it must still be there!”*

Is persistence of data on a computer really a foregone conclusion?

> “*The agent located and examined several videos or images that appeared to meet the definition of child pornography. The agent arrested Boucher, seized the laptop and shut it down.*
>
> *[Therefore, to produce the decrypted contents would] add little or nothing … to the Government’s information about the existence and location of files that may contain incriminating information.*”

**— In re Grand Jury Subpoena to Sebastien Boucher, 2009 WL 424718**

# Kill switches

**ASSUMPTION:**

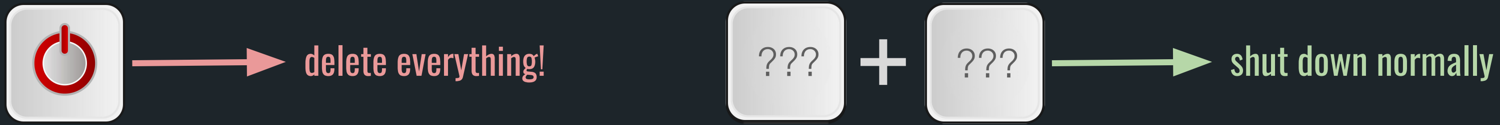
*“We saw the data on your laptop before you shut it off, so it must still be there!”*
Is persistence of data on a computer really a foregone conclusion?

**CHALLENGE:**

There could be multiple ways to shut down a laptop computer,
some simply putting the computer to sleep,
and others deleting or overwriting all the (encrypted) data on the computer.

**POSSIBLE RESPONSES:**

- ➔ Demonstrate absence of kill switch?
- ➔ Compel “enter the password” instead of “produce the decrypted contents?”
- ➔ Obstruction of justice?



delete everything!

shut down normally

# Possession without the ability to decrypt

ASSUMPTION:

*"The encrypted data is on your computer, so you must know how to access it!"*
Does possession of encrypted data imply the ability to decrypt it?

CHALLENGES:

1. **Custodianship of other people's encrypted data** may become common.
   - Startup companies offering "peer-to-peer Dropbox" already exist.

2. **"Multi-stakeholder encryption"** (via *secret sharing*):

   No single party has the ability to decrypt without the cooperation of others (a little like co-signatories to a bank account).

   - Could be useful for important information concerning multiple people, e.g., married couples, families, or organizational secrets.

> “*[T]he court [initially] held that it was not ‘reasonably clear, in the absence of compelled decryption, that Feldman actually ha[d] access to and control over the encrypted… devices… .*
>
> *[Then] the government presented a… request for reconsideration… based on the discovery of new information… attesting to the following facts:*
>
> - *… Recently, the FBI was able to decrypt and access a small part of Feldman’s storage system…*
> - *In addition to numerous files of child pornography, the decrypted part… contains detailed personal financial records and documents belonging to Feldman.*
> - *The decrypted part… contains dozens of personal photographs of Feldman.*
> - *[A colleague of Feldman said] that Feldman is a competent software developer who could have learned how to use encryption.*
>
> **— In re The Decryption of a Seized Data Storage System (Feldman), E.D. Wis. 2013** ”

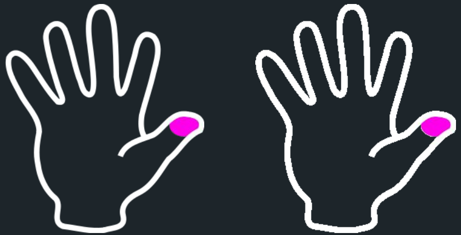
# Enhanced biometric-based encryption

**ASSUMPTION:**

*"Biometric-based encryption methods do not have a testimonial aspect."*
Is it really impossible to have encryption that is biometric-based and testimonial?

**CHALLENGE:**

Additional testimonial components could easily be added on to supplement existing biometric-based encryption methods.



today

tomorrow?

## 1. Sequence of fingerprints

location

second hand position

## 2. Situation-based decryption

> *Car, drive to where I went last Monday afternoon.*

> *Dear home security system, what time did I leave home today?*

## 3. Voice commands

# Main take-aways

- The doctrine is very sensitive to changes in available technology, and changes in common usage of technology.
    - E.g., changes in default settings or implementation details, etc.
    - Even changes in the "protocol"

- Applying the doctrine "correctly" (as we understand it) requires case-by-case technical expertise.
    - Applying precedent is difficult with rapidly changing technology & context.
    - May get harder over time.