

Crypto & Law (part 2)

Aloni Cohen

Selected Areas in Cryptography Summer School

August, 2024

Montreal



Congress of the United States

begun and held at the City of New York, on
Wednesday the fourth of March, one thousand seven hundred and eighty nine.

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.

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



Unlock your phone

I plead the 5th



IN THE

Supreme Court of the United States

ROBERT ANDREWS,

Petitioner,

—v.—

STATE OF NEW JERSEY,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI
TO THE SUPREME COURT OF NEW JERSEY

PETITION FOR A WRIT OF CERTIORARI

The Question Presented is:

Does the Self-Incrimination Clause of the Fifth Amendment protect an individual from being compelled to recall and truthfully disclose a memorized passcode, where communicating the passcode may lead to the discovery of incriminating evidence to be used against him in a criminal prosecution?

Outline

- Fifth Amendment's foregone conclusion doctrine
- ... for compelled decryption
- ... formalized



The Fifth Amendment

Cohen, Park. "Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries" (2019)

**"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

"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.

**"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

"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.

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

“Surely the Government is **in no way relying on the truth-telling** of the taxpayer to prove the existence of or his access to the documents. The existence and location of the papers are a foregone conclusion and the taxpayer **adds little or nothing to the sum total of the Government's information** by conceding that he in fact has the papers. ... The question is not of testimony but of surrender.”

(Authenticity handled separately.)

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

"Compliance with the subpoena
tacitly concedes"

- existence
- possession or control
- authenticity

Example

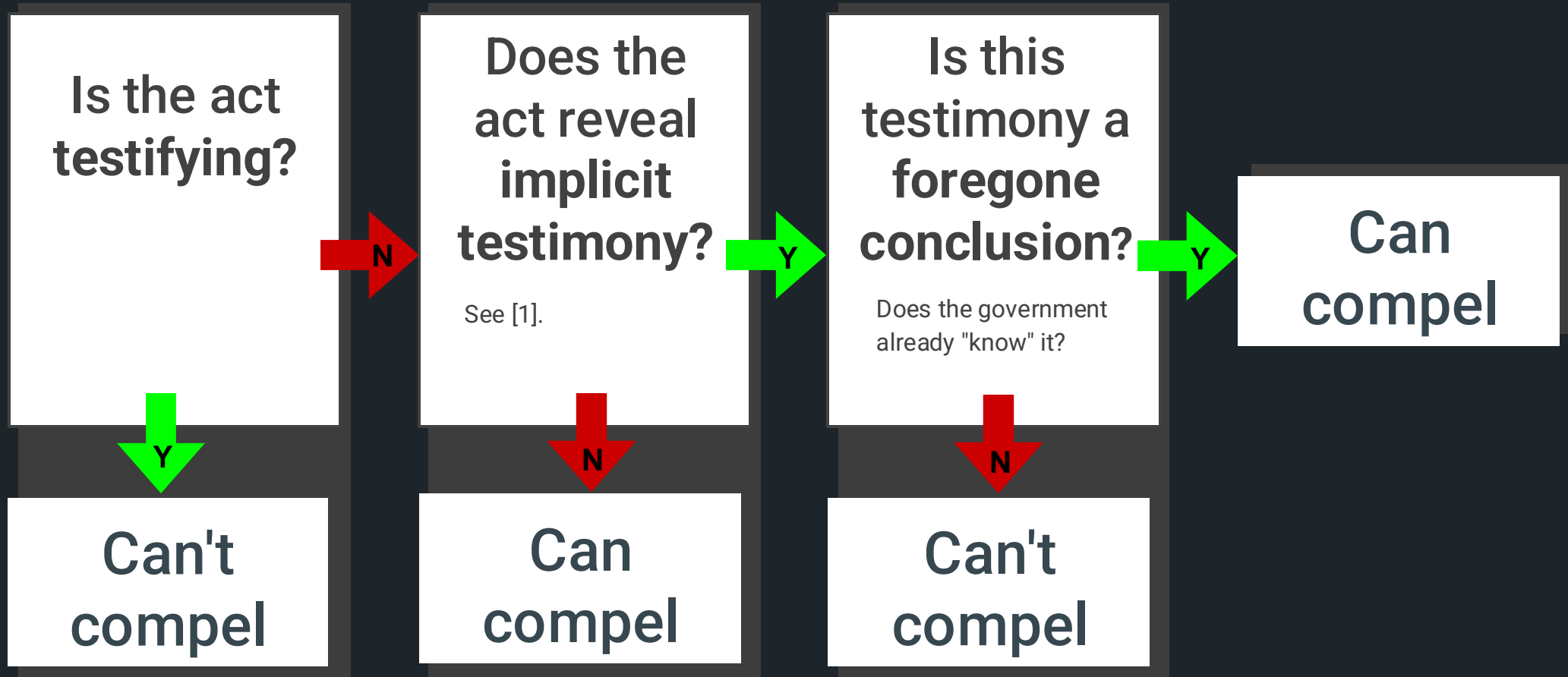
Handwriting exemplar admits to

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

But,

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

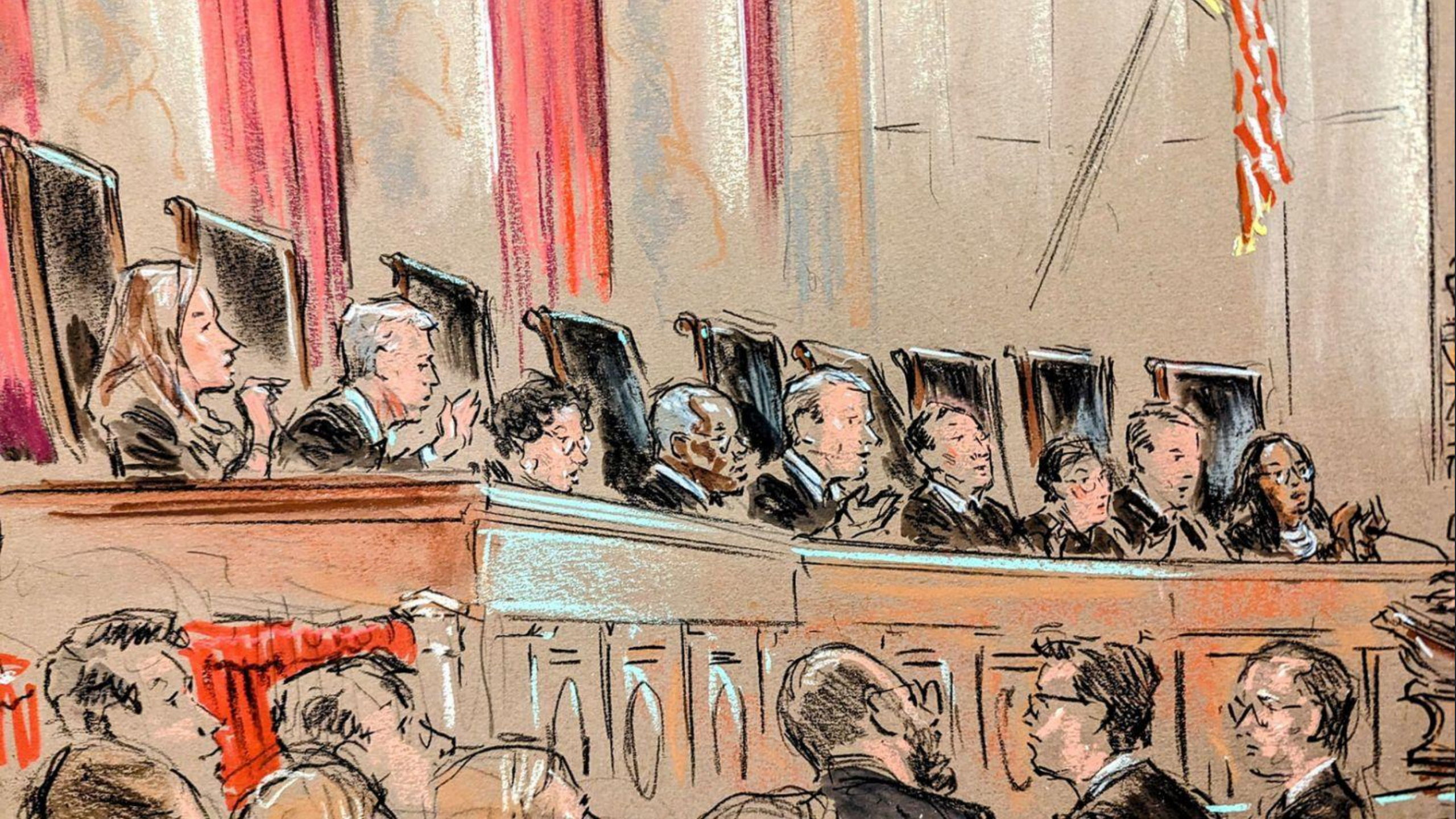
Can you compel an act?



[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.

**Foregone conclusion
and
compelled decryption**



General Case Outline



Help us decrypt

I plead the 5th



FN10. The Commonwealth's "protocol" is as follows:

- "1. The defendant, in the presence of his counsel, shall appear at the Computer Forensics Laboratory of Massachusetts Attorney General Martha Coakley within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
 - "2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
 - "3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
 - "4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
 - "5. 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;
 - "6. The Commonwealth shall not view or record the password or key in any way; [and]
 - "7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter."
- At the hearing on the motion to compel decryption, the Commonwealth stated that it "would be seeking to introduce the fact of encryption in order to suggest consciousness of guilt."

General Case Outline



Help us decrypt



I plead the 5th



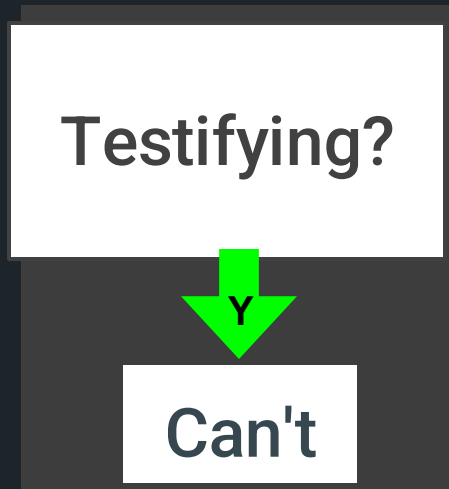
4 different ways to "help decrypt"

- 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*)

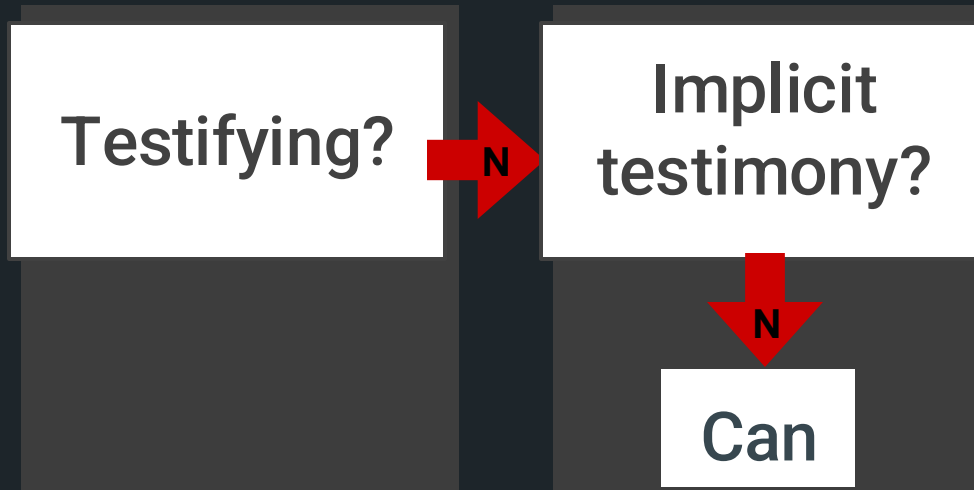
Can you compel it?



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

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

Can you compel it?



" . . . 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)

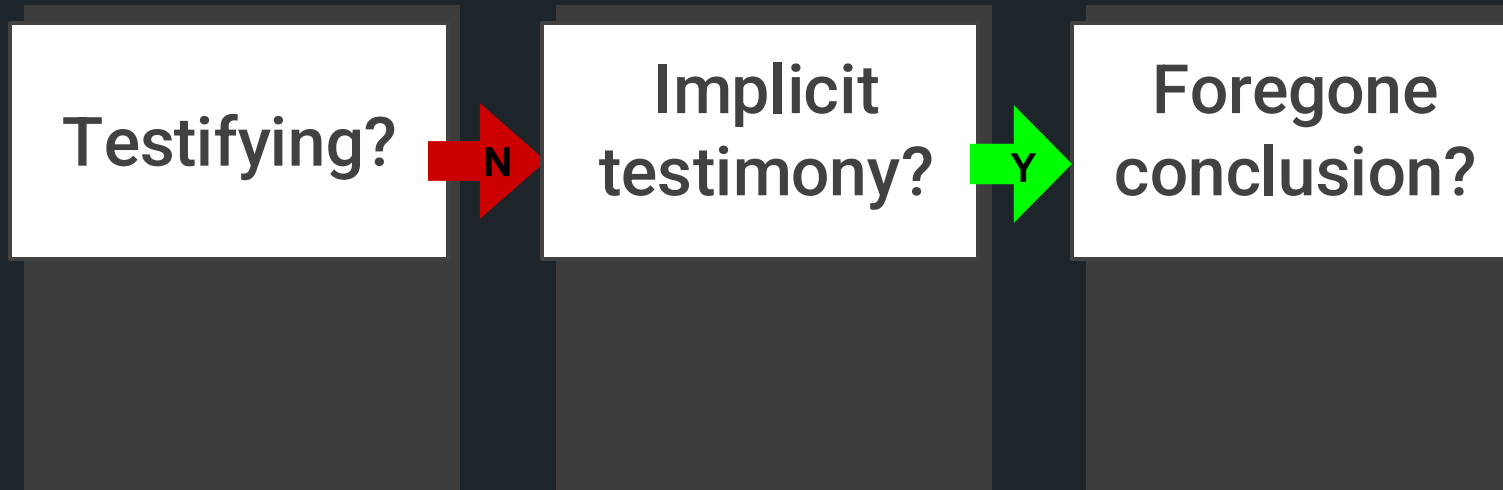
US v. Fricosu, 2012

"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*)

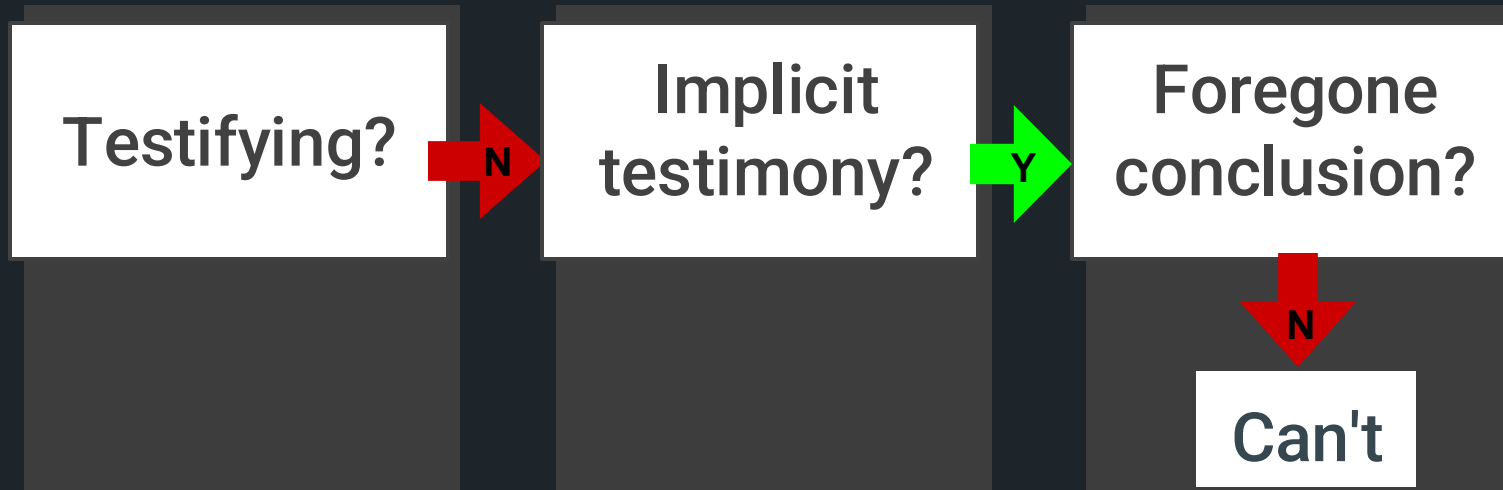
Can you compel it?



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?



"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

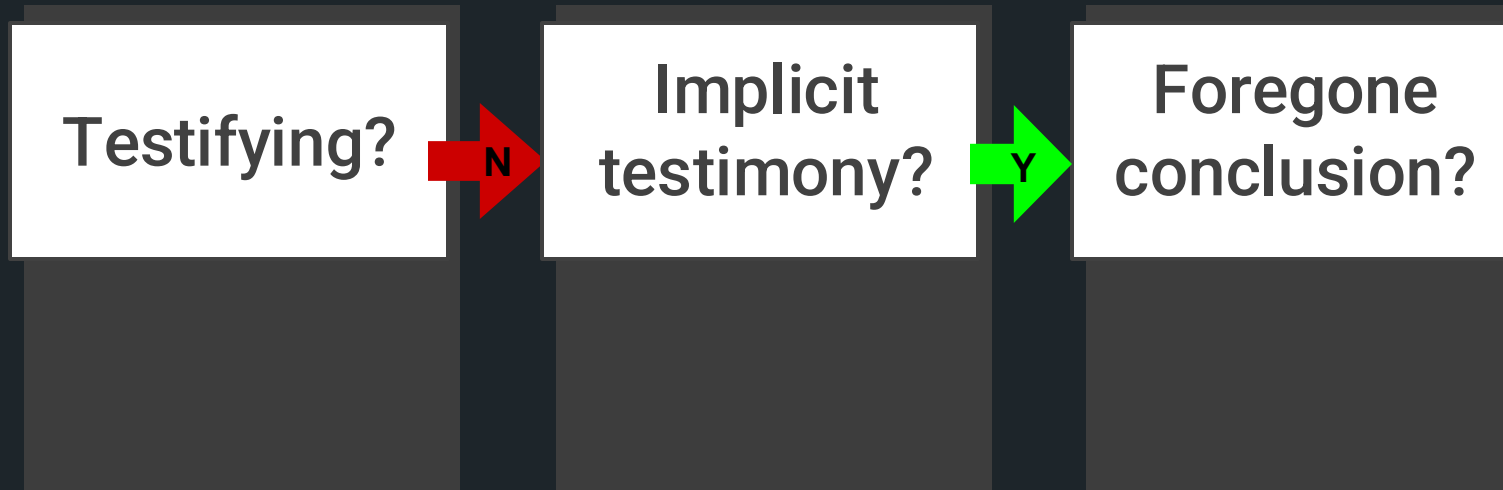
US v. Fricosu, 2012

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. Gelfatt, 2014*)

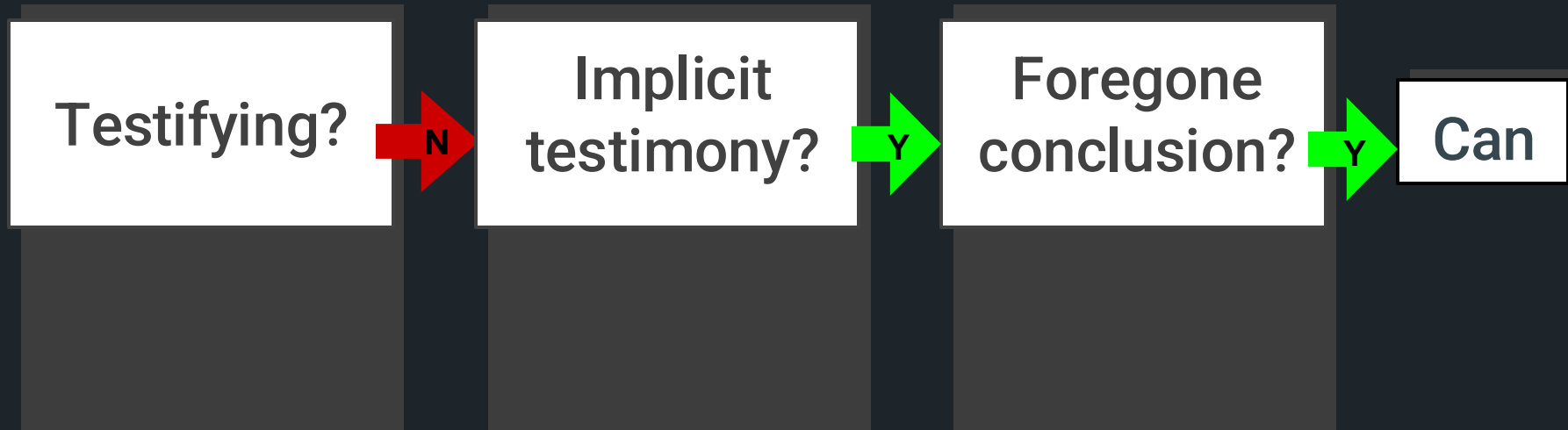
Can you compel it?



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?



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.

Compelling acts, in brief

1. Enumerate the implicit testimony
2. Determine whether it is all foregone

Enter a password:

"I know the password"

Other scenarios?

Produce a hash preimage

Perform 2-factor authentication

Enter your ATM PIN into this locked phone

Enter a non-duress password

Authenticity

- The government must "independently verify that the compelled documents **are in fact what they purport to be.**"
- Most accounts of compelled decryption cases don't take authenticity seriously

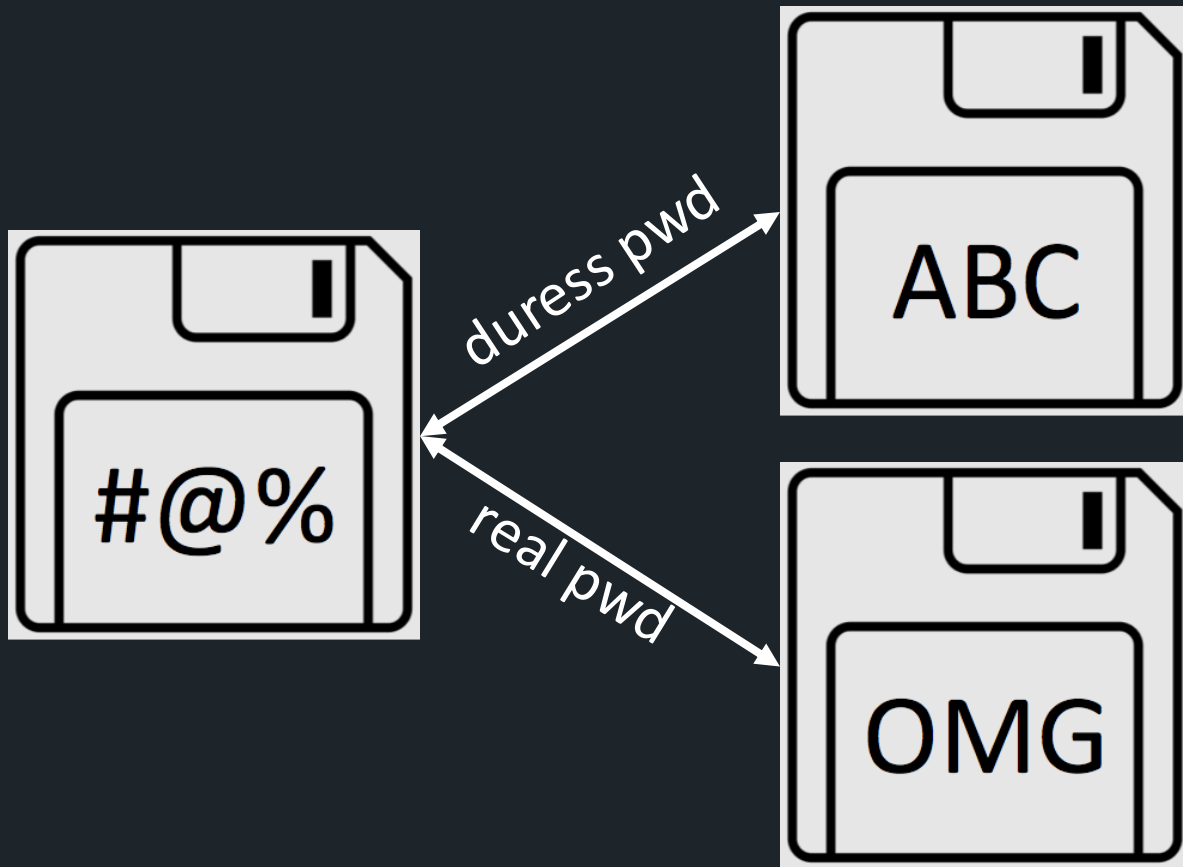
Gelfgatt:

"[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.**

Deniable encryption



FN10. The Commonwealth's "protocol" is as follows:

"1. The defendant, in the presence of his counsel, shall appear at the Computer Forensics Laboratory of Massachusetts Attorney General Martha Coakley within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;

"2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;

"3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';

"4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;

"5. 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;

"6. The Commonwealth shall not view or record the password or key in any way;

[and] "7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the

manner in which the digital media in this case was decrypted in its case in chief.

Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter."

At the hearing on the motion to compel decryption, the Commonwealth stated that it "would be seeking to introduce the fact of encryption in order to suggest consciousness of guilt."

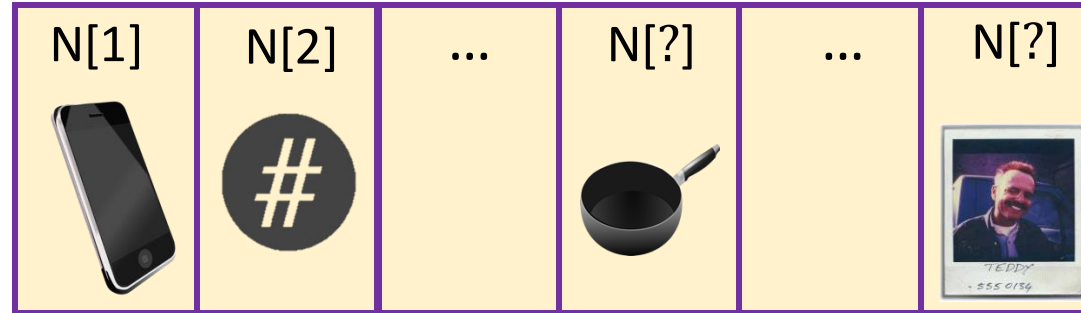
Sounds like simulation!

Let's try to formalize it

*“the taxpayer **adds little or nothing to the sum total of the Government's information** by conceding that he in fact has the papers.” (Fisher v US, 1976)*



Government G



Nature N
(everything except the mind of R)



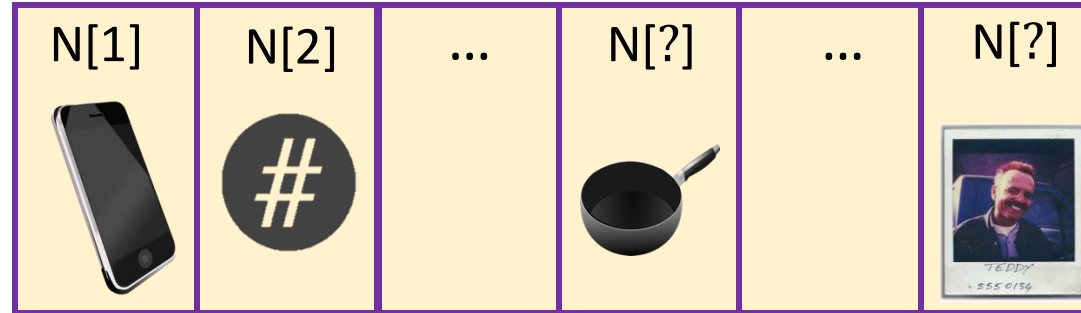
Respondent R

Step 1: Govt outputs

- Evidence E
- Compelled Action A*
- Simulator S



Government G



Nature N



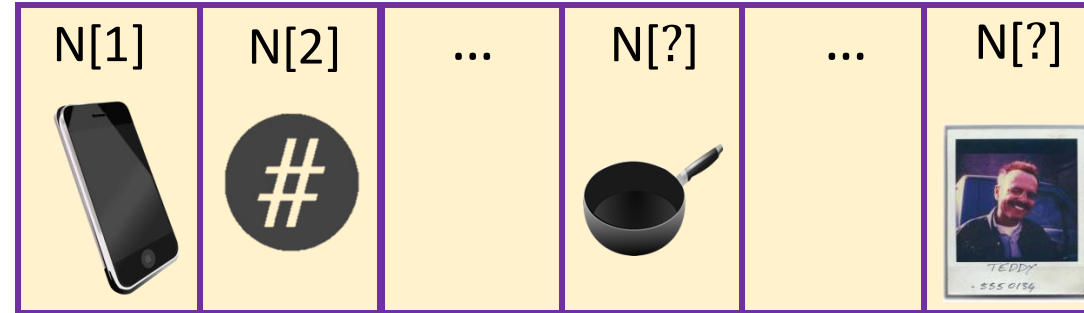
Respondent R

Step 1: Govt outputs

- Evidence E
- Compelled Action A*
- Simulator S



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

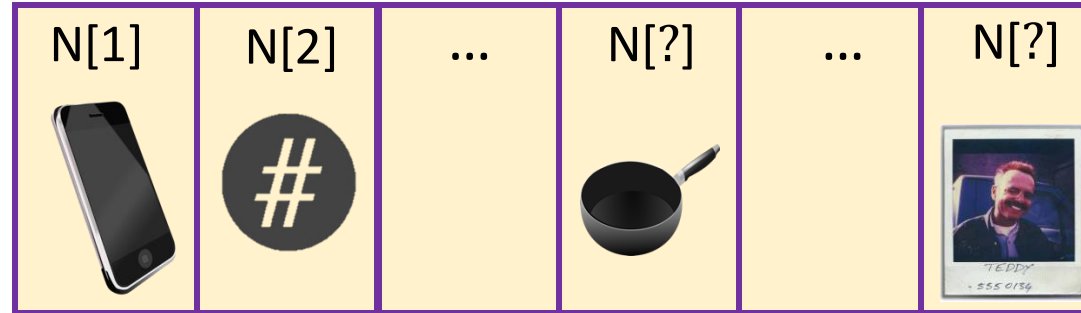
Evidence defines set of possible worlds (R' , N')

Step 1: Govt outputs

- Evidence E
- Compelled Action A*
- Simulator S



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R' , N')

Compelled Action A*

- $x \leftarrow R.\text{pwd}$
- $sk \leftarrow \$$
- $c \leftarrow \text{Enc}(sk, x)$
- $N[3].\text{put}(c)$

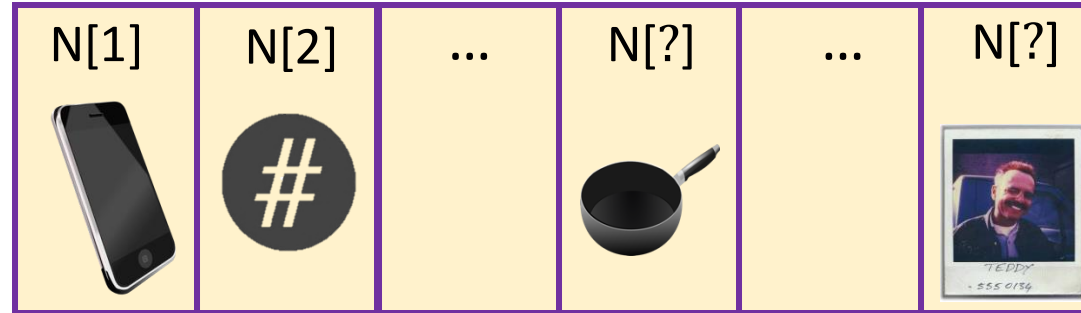
Compelled encryption

Step 1: Govt outputs

- Evidence E
- Compelled Action A*
- Simulator S



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R' , N')

Simulator S

- $sk' \leftarrow \$$
- $c' \leftarrow \text{Enc}(sk, 0)$
- $N[3].\text{put}(c')$

Compelled Action A*

- $x \leftarrow R.\text{pwd}$
- $sk \leftarrow \$$
- $c \leftarrow \text{Enc}(sk, x)$
- $N[3].\text{put}(c)$

Step 1: Govt outputs

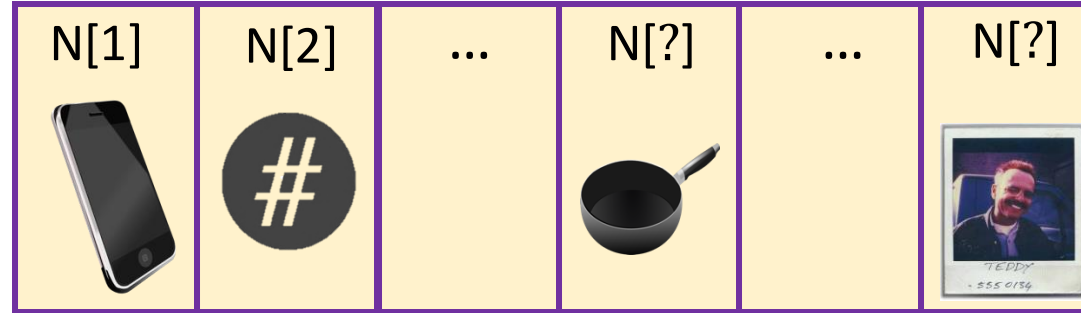
- Evidence E
- Compelled Action A*
- Simulator S

Step 2: Is A* **simulatable**?

For all E-consistent (R', N') :
 $\text{transcript}\langle G \leftrightarrow A^* \rangle_{R', N'} \approx_{N'} S^N$



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R', N')

Simulator S

- $sk' \leftarrow \$$
- $c' \leftarrow \text{Enc}(sk, 0)$
- $N[3].\text{put}(c')$

Compelled Action A*

- $x \leftarrow R.\text{pwd}$
- $sk \leftarrow \$$
- $c \leftarrow \text{Enc}(sk, x)$
- $N[3].\text{put}(c)$

Step 1: Govt outputs

- Evidence E
- Compelled Action A*
- Simulator S

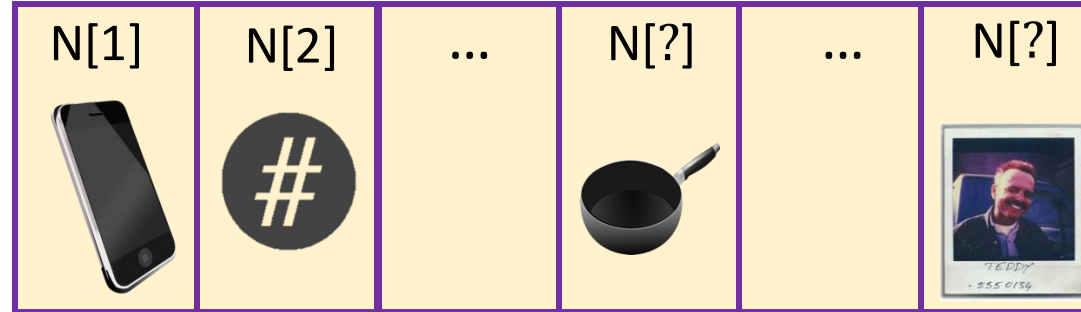
Step 2: Is A* **simulatable**?

For all E-consistent (R', N') :
 $\text{transcript}\langle G \leftrightarrow A^* \rangle_{R', N'} \approx_{N'} S^N$

Step 3: R performs A*



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R', N')

Simulator S

- $sk' \leftarrow \$$
- $c' \leftarrow \text{Enc}(sk, 0)$
- $N[3].\text{put}(c')$

Compelled Action A*

- $x \leftarrow R.\text{pwd}$
- $sk \leftarrow \$$
- $c \leftarrow \text{Enc}(sk, x)$
- $N[3].\text{put}(c)$



But what about decryption?

Step 1: Govt outputs

- Evidence E
- Compelled Action A*
- Simulator S

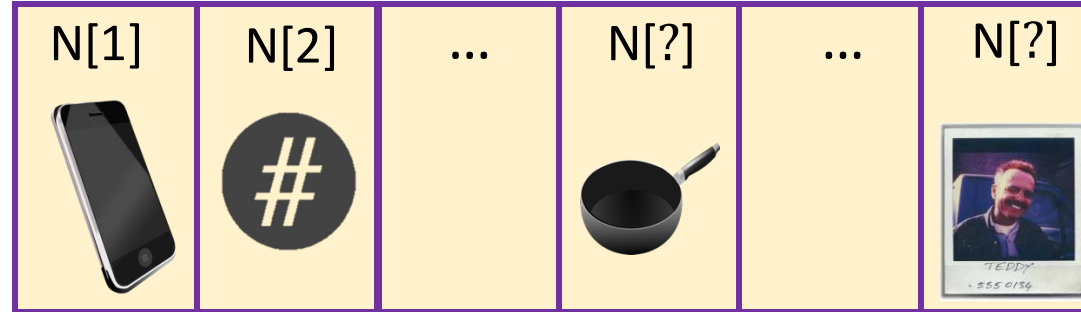
Step 2: Is A* simulatable?

For all E-consistent (R', N') :
 $\text{transcript}(G \leftrightarrow R', N') \approx_{N'} S^N$

Step 3: perform A*



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R', N')

Compelled Action A*

- $x \leftarrow R.\text{pwd}$
- $N[1].\text{Unlock}(x)$

Compelled decryption

Simulation-based foregone conclusion

“adds little or nothing” (Fisher v US, 1976)



Verification-based foregone conclusion

“in no way relying on the truth-telling” (Fisher v US, 1976)

A new goal: Constructive foregone conclusion

Holy grail:

- For a given act, determine whether all implicit testimony is foregone.

Instead:

- Specify acts such that all implicit testimony is foregone.

Hand over your pan

Unlock the phone by
entering a password

Implicit testimony

What is testimony?

Disclosure of the
contents of your mind

Relying on your
truthtelling

"I have a pan / pwd"

"This is my actual
pan / pwd
not some other one"

It's a foregone
conclusion if...

Govt already knows

Govt can verify

Ability

Conformity



Perform action A*

Implicit testimony

What is testimony?

Disclosure of the
contents of your mind

Relying on your
truth-telling

"I can do A*"

"I did do A* (not
something else)"

It's a foregone
conclusion if...

Govt can show
you **can** do A*

Govt can **verify**
whether you do A*




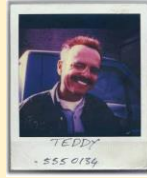
Ability

Conformity





Government G

N[1]	N[2]	...	N[?]	...	N[?]
					

Nature N



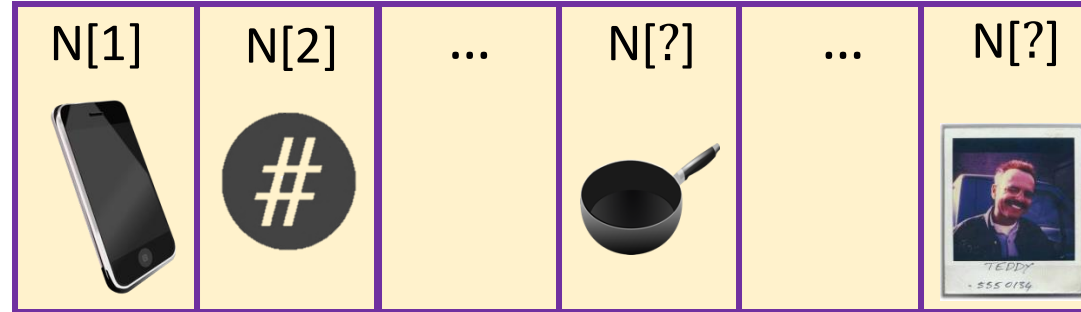
Respondent R

Step 1: Govt outputs

- Evidence E
- Exemplar Action A*
- Verifier V



Government G



Nature N



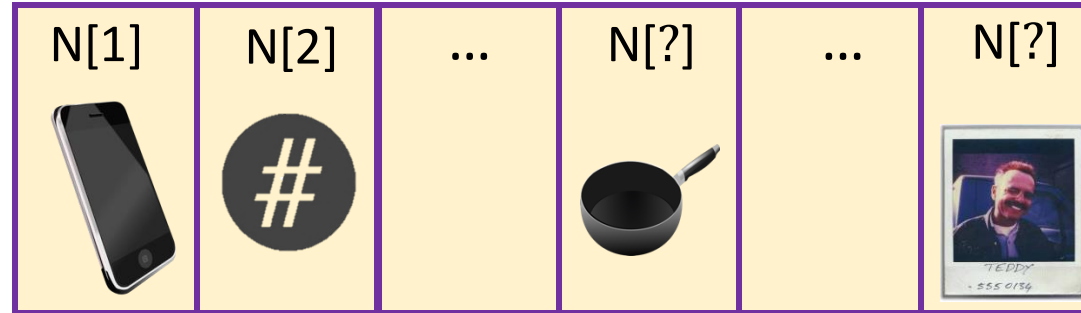
Respondent R

Step 1: Govt outputs

- Evidence E
- Exemplar Action A*
- Verifier V



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

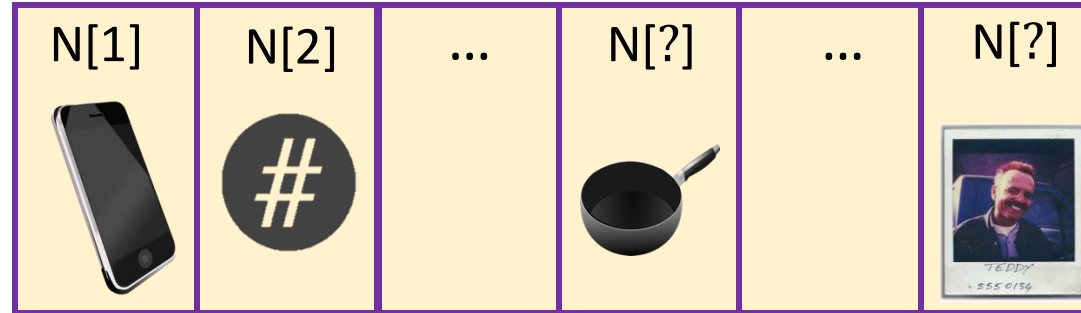
Evidence defines set of possible worlds (R' , N')

Step 1: Govt outputs

- Evidence E
- Exemplar Action A*
- Verifier V



Government G



Nature N



Respondent R

Evidence E

R knows the password

- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R' , N')

Exemplar Action A*

- $x \leftarrow R.\text{pwd}$
- $N[1].\text{Unlock}(x)$

Exemplar A*

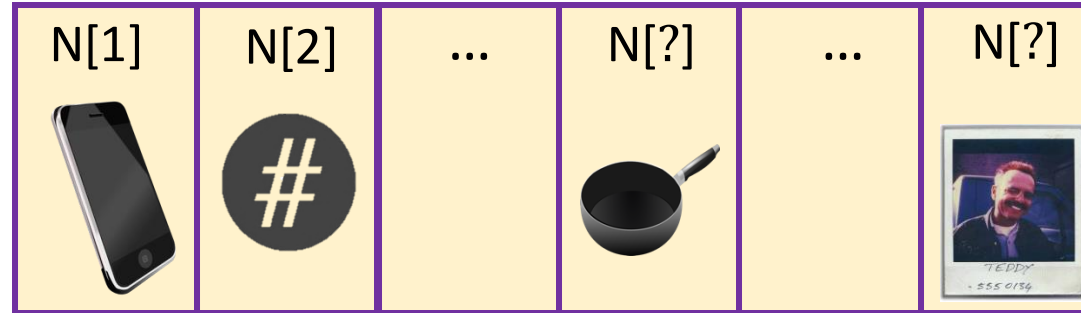
What G wants R to do

Step 1: Govt outputs

- Evidence E
- Exemplar Action A*
- Verifier V



Government G



Nature N



Respondent R

Evidence E

- R knows the password
- $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of possible worlds (R' , N')

Verifier V

- If $N[1]$ is unlocked: Return 1
- Else: Return 0

Exemplar Action A*

- $x \leftarrow R.\text{pwd}$
- $N[1].\text{Unlock}(x)$

Exemplar A*

What G wants R to do

Step 1: Govt outputs

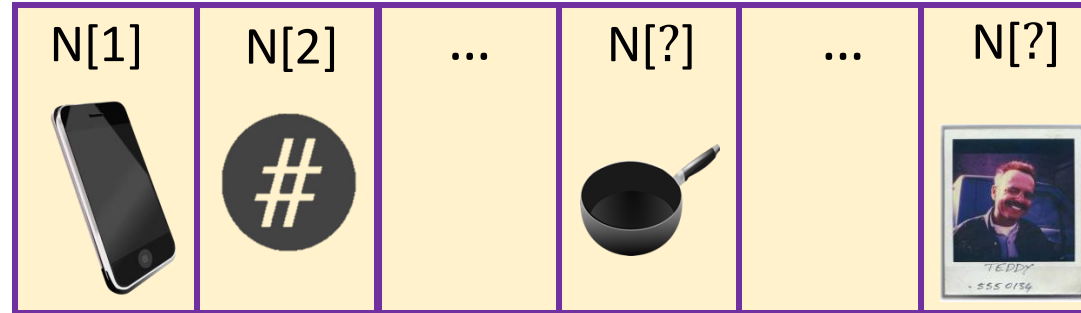
- Evidence E
- Exemplar Action A*
- Verifier V

Step 2: Is V demonstrable?

For all E-consistent (R',N') the
interaction of V and A* returns 1
 $\langle V \leftrightarrow A^* \rangle_{R',N'} = 1$



Government G



Nature N



Respondent R

Evidence E

- R knows the password
- N[1].Unlock(R.pwd)
⇒ N[1] is unlocked

E-consistency

Evidence defines set of
possible worlds (R', N')

Verifier V

- If N[1] is unlocked: Return 1
- Else: Return 0

V demonstrable

Exemplar A* verifies

Exemplar Action A*

- $x \leftarrow R.pwd$
- N[1].Unlock(x)

Exemplar A*

What G wants R to do

Step 1: Govt outputs

- Evidence E
- Exemplar Action A*
- Verifier V

Step 2: Is V demonstrable?

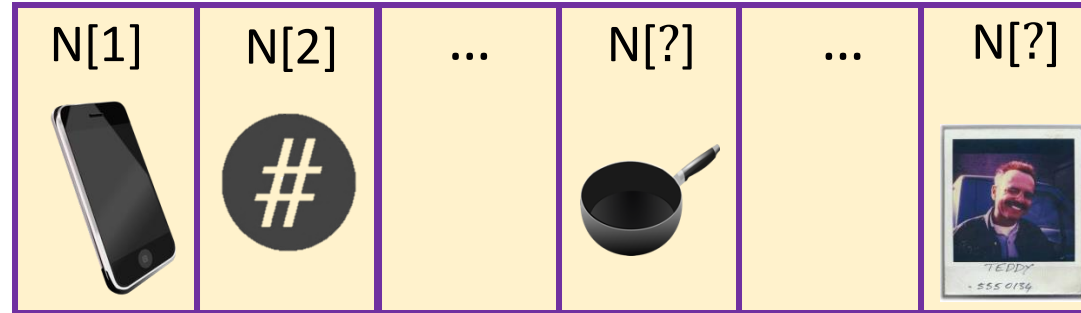
For all E-consistent (R', N') the
interaction of V and A* returns 1
 $\langle V \leftrightarrow A^* \rangle_{R', N'} = 1$

Step 3: R performs any conforming A

Interaction of V and A returns 1
 $\langle V \leftrightarrow A \rangle_{R, N} = 1$



Government G



Nature N



Respondent R

Evidence E

- R knows the password
- N[1].Unlock(R.pwd)
⇒ N[1] is unlocked

E-consistency

Evidence defines set of
possible worlds (R', N')

Verifier V

- If N[1] is unlocked: Return 1
- Else: Return 0

V demonstrable

Exemplar A* verifies

Exemplar Action A*

- $x \leftarrow R.pwd$
- N[1].Unlock(x)

Exemplar A*

What G wants R to do

Action A

Eg: Unlock N[1]
using fingerprint

A conforms

A verifies in the real world

Step 1: Govt outputs

- Evidence E
- Exemplar Action A*
- Verifier V

Step 2: Is V demonstrable?

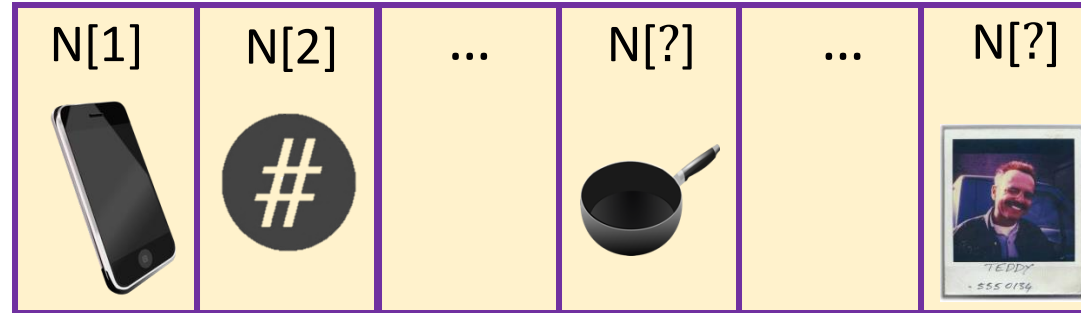
For all E-consistent (R', N') the
interaction of V and A* returns 1
 $\langle V \leftrightarrow A^* \rangle_{R', N'} = 1$

Step 3: R performs any conforming A

Interaction of V and A returns 1
 $\langle V \leftrightarrow A \rangle_{R, N} = 1$



Government G



Nature N



Respondent R

Evidence E

R knows the password
• $N[1].\text{Unlock}(R.\text{pwd})$
 $\Rightarrow N[1]$ is unlocked

E-consistency

Evidence defines set of
possible worlds (R', N')

Verifier V

- If N[1] is unlocked: Return 1
- Else: Return 0

V demonstrable

Exemplar A* verifies

Exemplar Action A*

- $x \leftarrow R.\text{pwd}$
- $N[1].\text{Unlock}(x)$

Exemplar A*

What G wants R to do

Action A

Eg: Unlock N[1]
using fingerprint

A conforms

A verifies in the real world

Review

Step 1: Govt outputs

E, A^*, V



Government G

Step 2: Is V **demonstrable**?

Exemplar A^* verifies in any world

Step 3: R performs any **conforming A**

A verifies in the real world



Respondent R

Evidence E

Possible worlds (R', N')

Verifier V

How to check R's action

Exemplar Action A^*

What G wants R to do

Action A

What R actually does

The framework

Step 1: Govt outputs

E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world

Step 3: R performs any conforming A

A verifies in the real world

Implicit testimony is constructively a foregone conclusion

- Step 2 \Rightarrow **Ability** foregone
- R can satisfy V by performing A^* in all possible worlds



Respondent R

Evidence E

Possible worlds (R', N')

Verifier V

How to check R 's action

Exemplar Action A^*

What G wants R to do

Action A

What R actually does

The framework

Step 1: Govt outputs

E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world

Step 3: R performs any **conforming** A

A verifies in the real world

Implicit testimony is constructively a foregone conclusion

- Step 3 \Rightarrow **Conformity** foregone
- R can perform any act A that satisfies V ... “truthfulness” is meaningless
- If Govt wants A^* but not A , it needs a better V



Respondent R

Evidence E

Possible worlds (R', N')

Verifier V

How to check R's action

Exemplar Action A^*

What G wants R to do

Action A

What R actually does

The framework

Step 1: Govt outputs

E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world

Step 3: R performs any conforming A

A verifies in the real world

Distinguishes ...

- A^* What the government wants R to do
- A What R chooses to do



Respondent R

Evidence E

Possible worlds (R', N')

Verifier V

How to check R 's action

Exemplar Action A^*

What G wants R to do

Action A

What R actually does

The framework

Step 1: Govt outputs

E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world

Step 3: R performs any **conforming** A

A verifies in the real world

Distinguishes ...

- Contents of R 's mind (and properties of devices in Nature)
- Govt's evidence of the same



Respondent R

Evidence E

Possible worlds (R', N')

Verifier V

How to check R 's action

Exemplar Action A^*

What G wants R to do

Action A

What R actually does

The framework

Step 1: Govt outputs

E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world

Step 3: R performs any conforming A

A verifies in the real world

Distinguishes ...

- Contents of R 's mind
- Action that R takes



Respondent R

Evidence E

Possible worlds (R', N')

Verifier V

How to check R 's action

Exemplar Action A^*

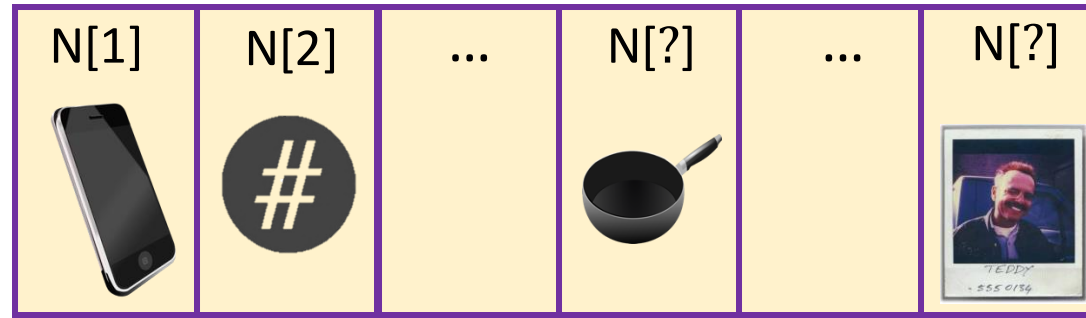
What G wants R to do

Action A

What R actually does

The framework

Compelling cryptography:
Entailment

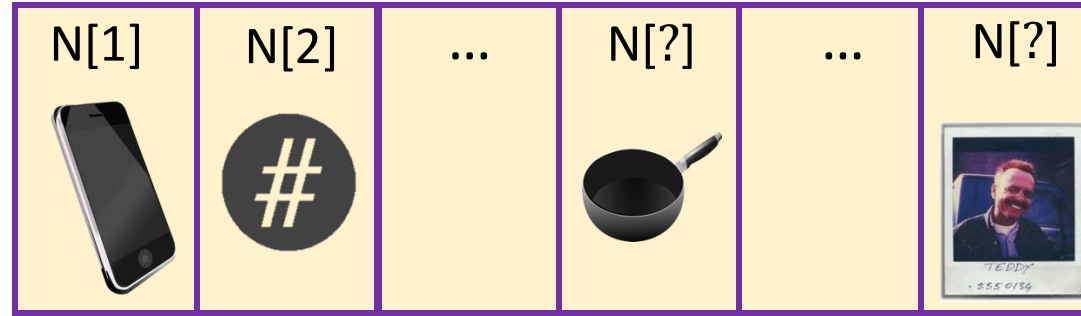


Nature N

Hash Preimage

Step 1: Govt outputs

E, A^*, V



Nature N

Evidence E

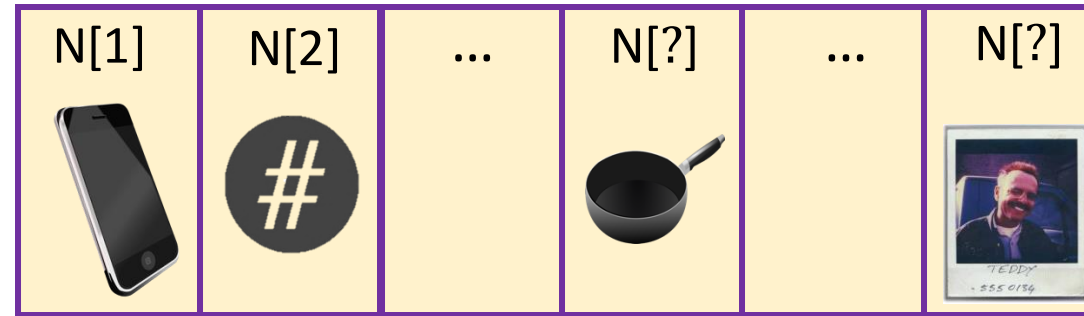
R can produce a hash preimage

- $\text{Hash}(N[R.loc_{pic}]) = N[2]$

Hash Preimage

Step 1: Govt outputs

E, A^*, V



Nature N

Evidence E

R can produce a hash preimage

- $\text{Hash}(N[R.loc_{pic}]) = N[2]$

Verifier V

- Input: loc
- $x = N[loc]$
- Is $\text{Hash}(x) = N[2]$?

Exemplar Action A^*

- Output $R.loc_{pic}$

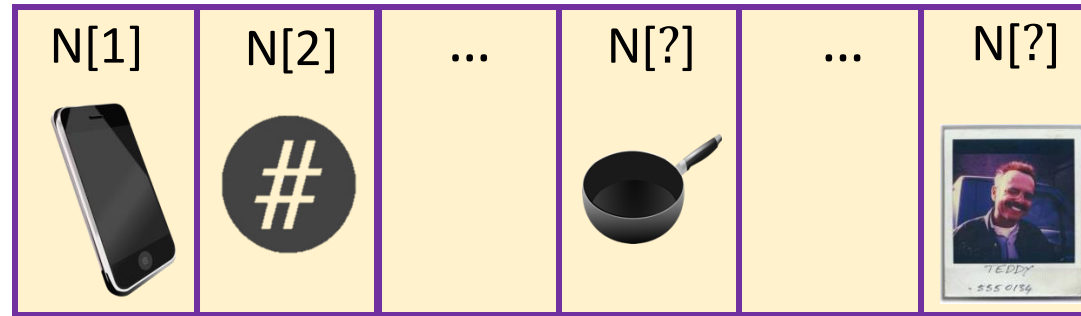
Hash Preimage

Step 1: Govt outputs

E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world



Nature N

Evidence E

R can produce a hash preimage

- $\text{Hash}(N[R.loc_{pic}]) = N[2]$

Verifier V

- Input: loc
- $x = N[loc]$
- Is $\text{Hash}(x) = N[2]$?

Exemplar Action A^*

- Output $R.loc_{pic}$

Hash Preimage

Step 1: Govt outputs

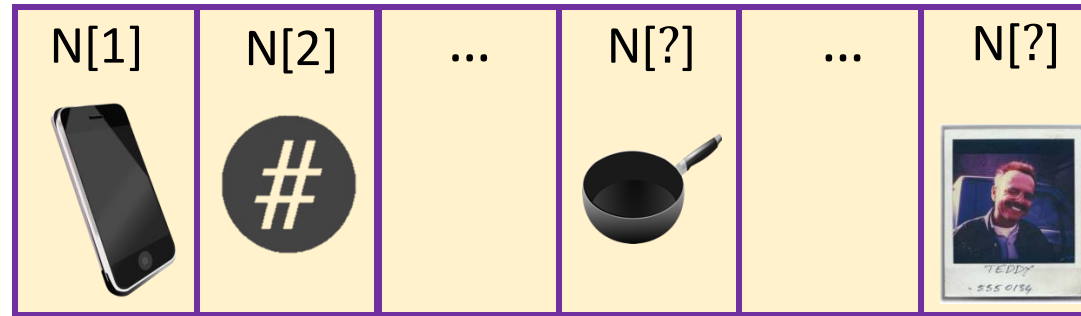
E, A^*, V

Step 2: Is V demonstrable?

Exemplar A^* verifies in any world

Step 3: R performs any **conforming** A

A verifies in the real world



Nature N

Evidence E

R can produce a hash preimage

- $\text{Hash}(N[R.loc_{pic}]) = N[2]$

Verifier V

- Input: loc
- $x = N[loc]$
- Is $\text{Hash}(x) = N[2]$?

Exemplar Action A^*

- Output $R.loc_{pic}$

Action A

????

Did G get what it wants?

Yes! A must output preimage.

V entails A^*

Any conforming A is “as good as” A^*

Hash Preimage

Entailment & password entering

Evidence E

R knows the password

Verifier V

Check if unlocked

Exemplar Action A*

Enter the password

Action A

???

Did G get what it wants?

Yes! A must unlock the phone.

Intuition: V entails T if any conforming A is "as good as" T.

Definition: V entails T with respect to E if exists post-processor P such that for all E-consistent (R,N) and V-conforming A:

$$P^N \circ \langle V \leftrightarrow A \rangle_{R,N} = T^{R,N}$$

Our definitions distinguish the fruits of act and act itself

Govt *really* wants (and gets) is the stuff on the phone

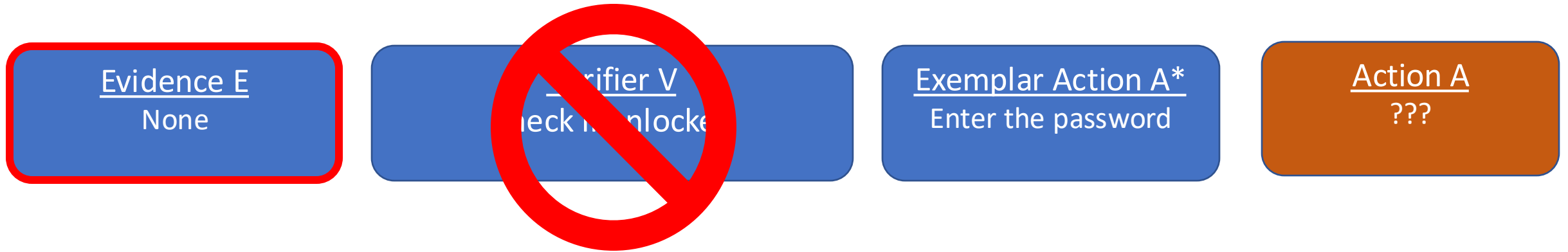
Target Action T

Produce phone's contents, decrypted

Theorem

- V entails T
- No demonstrable V has exemplar T!

Entailment & password entering

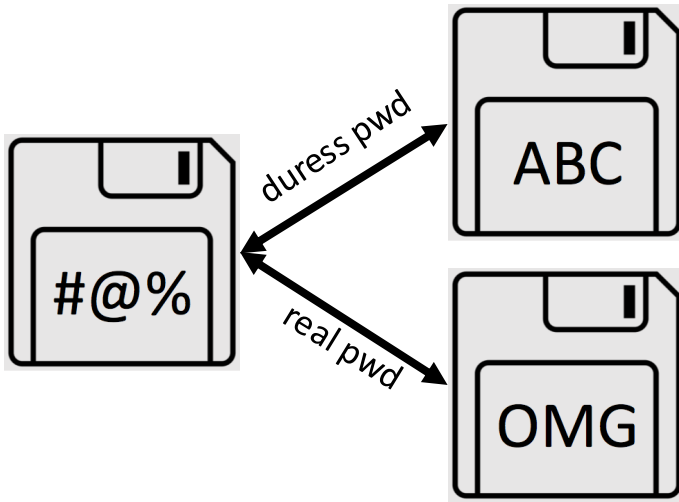


Theorem: **No** demonstrable V entails A*

We recover Kerr's "R knows the pwd" test!

- Enter-the-password is compellable \Leftrightarrow
Evidence shows R knows the password

Deniable Encryption



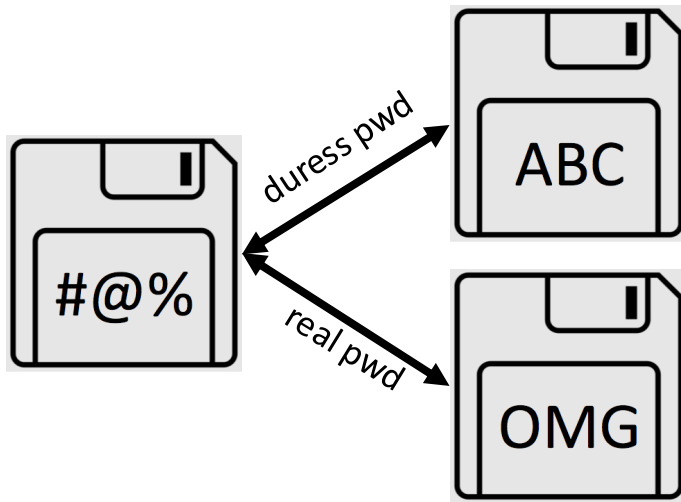
Prior approaches

- Commonwealth v Gelfgatt: ordered “not to enter a false or ‘fake’ password.”
- Kerr: “unlikely to raise significant Fifth Amendment issues”
- Sacharoff: “niche case because deniable encryption remains rare.”
- Cohen-Park: Govt can’t compel

Us

- If Govt can’t distinguish, free to use either password

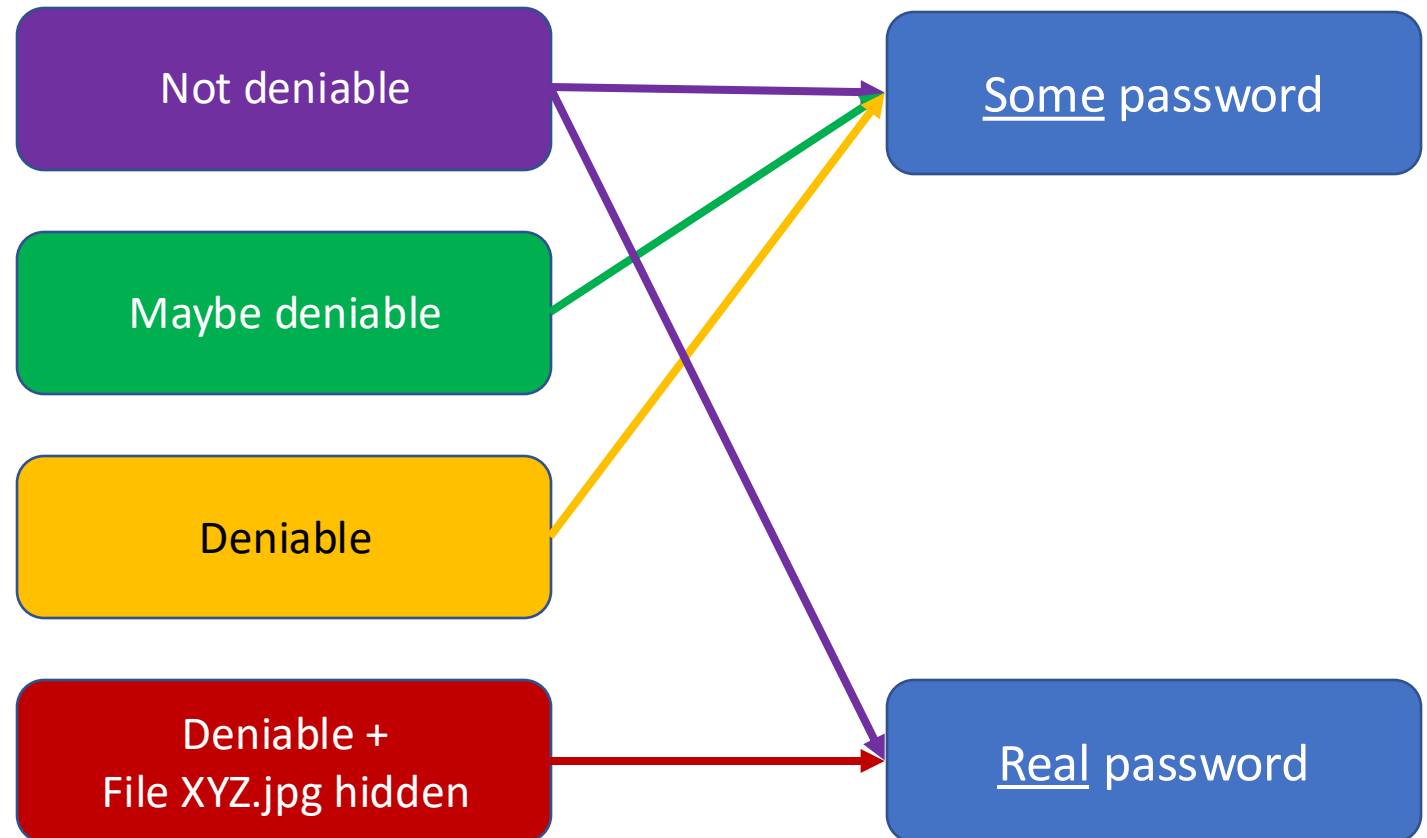
Entailment & Deniable Encryption



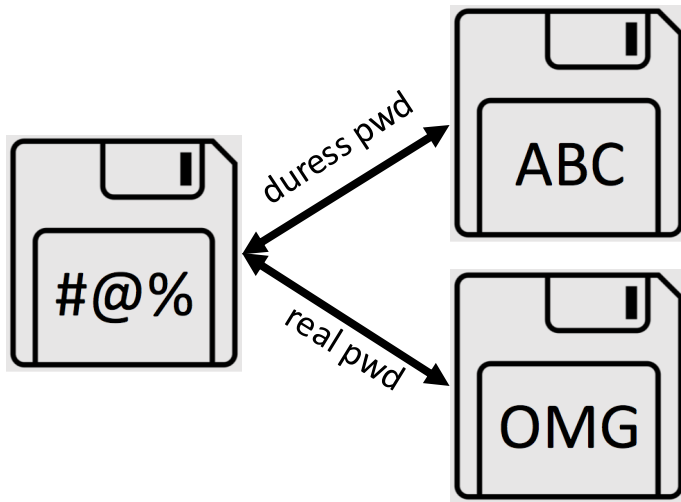
If Govt can't distinguish,
free to use either password

E states that R can
unlock, and...

Which password action A^*
can be entailed (compelled)



No “relying on the truth-telling”!



If Govt can't distinguish,
free to use either password

FN10. The Commonwealth's "protocol" is as follows:

"1. The defendant, in the presence of his counsel, shall appear at the Computer Forensics Laboratory of Massachusetts Attorney General Martha Coakley within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;

"2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;

"3. The defendant shall manually enter the password or key to each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';

"4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;

"5. 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;

"6. The Commonwealth shall not view or record the password or key in any way;

[and] "7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the

manner in which the digital media in this case was decrypted in its case in chief.

Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter."

At the hearing on the motion to compel decryption, the Commonwealth stated that it "would be seeking to introduce the fact of encryption in order to suggest consciousness of guilt."

Compelled cryptography!

- Typically compellable (entailable)
 - Enter a password
 - Open a commitment
 - Produce hash preimage
 - Perform 2-factor authentication
- Not typically compellable
 - Enter non-duress password
 - Encrypt a secret
 - Commit to a secret
 - Sample from a distribution

EVIDENCE \mathcal{E}_{2fa} :

Data: DEVICELOC

Method: $\mathcal{R}.\text{PWD}()$, $\mathcal{R}.\text{FINDSECOND}()$

Oracle: $\mathcal{N}[\text{DEVICELOC}]$,
 $\mathcal{N}[\mathcal{R}.\text{FINDSECOND}()]$

assert: $D \leq \mathcal{N}[\text{DEVICELOC}]$;
 $S \leq \mathcal{N}[\mathcal{R}.\text{FINDSECOND}()]$;
 $\mathcal{R}.\text{PWD}() == D.\text{pwd}$; $D.m \neq \perp$

assert $D.\text{code} == c$ **after**

| $D.\text{PROMPTPWD}(D.\text{pwd})$

| $c \leftarrow S.\text{GETCODE}()$

PRIMARY DEVICE D :

Variables: pwd , m , code ,

$\text{decrypted} \leftarrow \text{FALSE}$,

$\text{gotPwd} \leftarrow \text{FALSE}$

Method $\text{PROMPTPWD}(x)$

| **if** $(x == \text{pwd})$ **then**

| | **set** $\text{code} \leftarrow x$

| | $S.\text{SETCODE}(\text{code})$

| | **set** $\text{gotPwd} \leftarrow \text{TRUE}$

Method $\text{PROMPTCODE}(c)$

| **if**

| | $(\text{gotPwd} == \text{TRUE}) \wedge (c == \text{code})$

| | **then set** $\text{decrypted} \leftarrow \text{TRUE}$

Method $\text{READ}()$

| **if** $(\text{decrypted} == \text{TRUE})$ **then**

| | **return** m

| **else return** \perp

SECONDARY DEVICE S :

Variables: c

Method $\text{SETCODE}(\text{code})$

| **set** $c \leftarrow \text{code}$

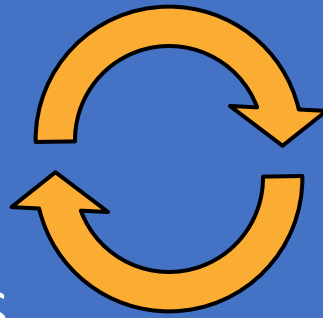
Method $\text{GETCODE}()$

| **return** c

Compelled decryption

1. **Extract** relevant text
and examples

4. **Draw** legal conclusions



2. **Formalize** mathematically

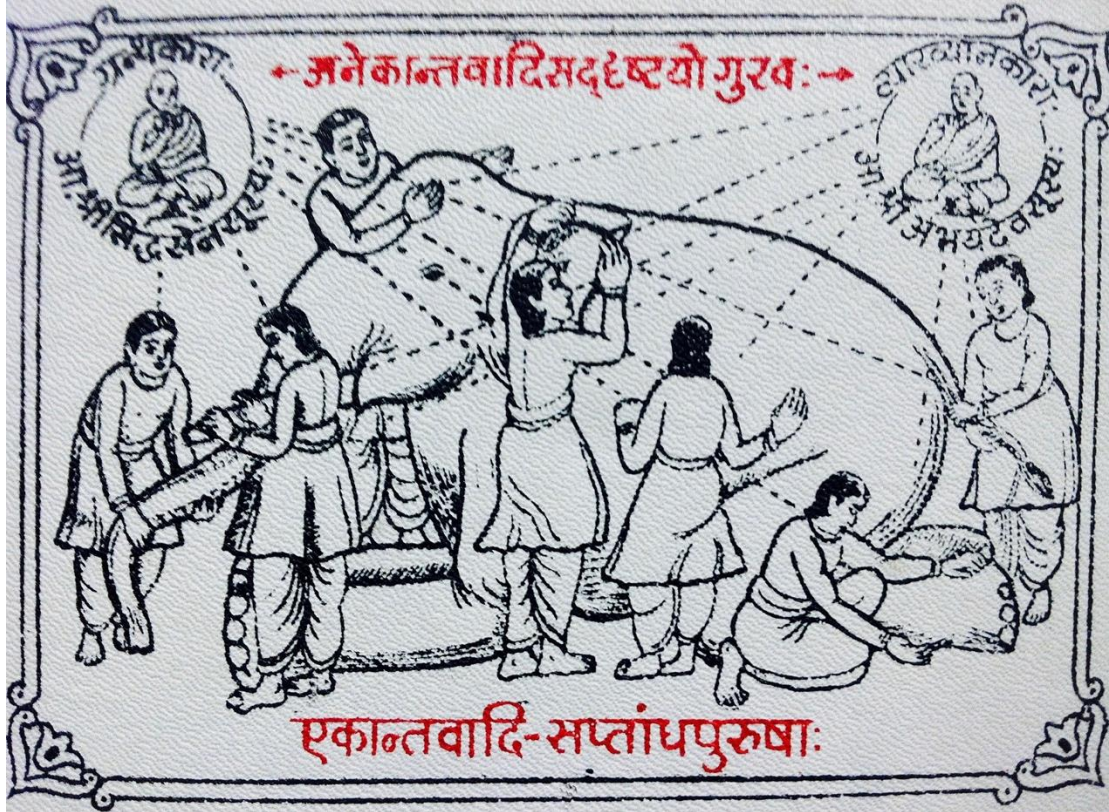
3. **Analyze**, alone and in
relation to other notions

Some legal conclusions

- Coherent doctrine possible, but subtle
- Current discourse overfits today's tech → deniable by default?
- Authenticity (conformity) is a real, non-theoretical challenge for compelled decryption. Prior approaches inadequate
- New criminal procedure (no technology needed!)
 - Govt submits evidence, verification procedure, exemplar action
 - Court finds respondent can perform exemplar action (ability)
 - Court orders respondent to satisfy the verification procedure (conformity)

What worked?

- Setting aside my initial disbelief
- Steeping myself in the caselaw
- Testing formalism against caselaw / doctrine



- ACM CS&Law conference
 - <https://computersciencelaw.org/>
 - (First) deadline: Sept 30
 - Conference: March 2025 in Munich
- CS+Law Workshop
 - <https://www.cslawworkshop.org/>
 - monthly on Zoom
- GenLaw
 - <https://www.genlaw.org/>