Giving Cops the Finger: Compelled Device Decryption and the Fifth Amendment

Riana Pfefferkorn
@Riana_Crypto

Crypto & Privacy Village
DEF CON 27
August 9, 2019
Before we dive in...

Disclaimers:
- IAALBIANYL
- This is not legal advice
- These are my own opinions, not my employer’s

This Talk Is NOT About:
- Searches at the U.S. border
- The Fourth Amendment
  - Different rights than 5th Am.: search & seizure, warrants
  - Let’s assume there’s a warrant for the device
- See Suggested Resources at end of talk
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.
What’s the 5th Am. Got to Do with Encryption?

- Encryption can impede execution of warrant
- Options for law enforcement:
  - Seize cloud backups?
  - Make Apple or Google unlock the phone?
  - Use a data extraction tool, e.g. Cellebrite, GreyKey?
  - Try to force the device owner to decrypt it?
    - This is where the Fifth Amendment comes in.
A Brief History of Encryption & the 5th Am.

Cypherpunks: 1990s

First court decision on 5th Am. & compelled decryption: 2007

More relevant now:
- FDE is now prevalent, especially on smartphones
- FDE is often the default or very easy to turn on
- Multiple means to decrypt: passcode, biometric

More court cases = general trends, but law is still unsettled & evolving
Is There a General Rule?

Does the 5th Amendment protect you* from being compelled to decrypt your encrypted device/files?

Generally:
- Biometric → you CAN be compelled to unlock, because biometric = something you are
- Passcode → you CANNOT be compelled to unlock, because passcode = something you know
- But, exceptions to each

* Defendants, victims, witnesses, etc.
Key Concepts

- “Act of Production” Doctrine
- “Foregone Conclusion” Doctrine
Act of Production Doctrine

- 5A protects you from being *incriminated* by your own “*compelled testimonial* communications”

- You can testify through an act, not just words
  - Producing evidence can have communicative aspects
  - Testifies to: existence, possession, authenticity

- Not all acts of production are protected – must be:
  - Compelled (if it’s voluntary, no 5A protection)
  - Incriminating (compliance puts you in legal danger)
  - Testimonial
When is an act “testimonial”? 

- If it discloses the contents of the individual’s mind → testimonial
- If the act “gives no indication of a person’s thoughts or knowledge” → not testimonial
- Courts have had trouble with this in the context of compelled decryption
Example: Testimonial vs. Not Testimonial

- Compare 2 compelled acts:
  - Surrendering key to strongbox: NOT testimonial
  - Revealing combo to a wall safe: IS testimonial
Foregone Conclusion Doctrine

- Act of production not protected if the info the act conveys is a “foregone conclusion” that “adds little or nothing to the sum total of the Govt’s info”

- That is: the act isn’t telling the govt anything it doesn’t already know, so the act can be compelled

- Example: IRS already knows that certain business papers exist, that you possess them, & that they’re authentic
Biometric: NOT testimonial

- Not testimonial because it’s something you are (face, fingerprint)

- ≈ compelled exhibition of bodily characteristic (blood sample, voice exemplar, donning clothing), which is not testimonial

- More like strongbox key than combo to safe
Minority view: Biometric IS testimonial

- Only 4 judges; 2 overturned on appeal so far
- Touching finger to sensor = testimonial
  - It testifies to possession/control of device
  - Not like fingerprinting; more like polygraph
- On appeal: Not testimonial, because agents pick the finger
  - Then, no need to engage the person’s thought process
  - No different than surrendering a key
- In sum: Use a biometric? You’re probably SOL
Testimonial because it’s something you know

Seems pretty open and shut! Right? Well, maybe...

Foregone Conclusion Doctrine

- Will defeat 5th Am. claim if govt can show it already knows the info that would be conveyed by the defendant’s compelled act of decryption

- Courts don’t agree on proper focus of analysis
  - Govt must show it knows incriminating files exist, vs.
  - Govt must show that defendant knows the passcode
Establishing foregone conclusion

- Defendant talked to agent, admitted device is his
- Admitted to agent there’s illegal stuff on device
- Voluntarily decrypted device in front of agent, let agent go through unlocked device & see incriminating files (but then device locked again)
- Showed/told other people about the illegal files, and they told the cops
Does the Fifth Amendment protect you from being compelled to decrypt your device?

Answer: It depends.

- If you use a passcode, better odds than biometric (but foregone conclusion exception might get you)
- Hard to predict whether 5th Am. claim will succeed
- Law is still evolving, courts don’t all use the same analysis, outcome often very fact-dependent
Specific facts matter

- What the cops already know
- Wording of the warrant or court order that authorizes the compulsion
- How cops execute the warrant
- Which court you’re prosecuted in
  - Federal (3rd & 11th Circuits)
  - State (MA, MN; soon: IN, PA, NJ)
  - FL: State or federal? Which part of state?
There Oughtta Be a Rule

- No uniform rule until Supreme Court weighs in
- Single rule = predictability, consistency
- Constitutional rights shouldn’t depend on whether you happened to pick biometric or passcode
- Your threat model might not be the police

CULTURE

Child uses sleeping mom's fingerprints to buy Pokemon gifts

(CNET, Dec. 27, 2016)
What to Do?
* (Again, not legal advice.)

Common-sense stuff:

✶ Think twice before showing off/blabbing about incriminating stuff on your device

✶ Especially to the cops

✶ Stay out of Florida

DO YOU WANT FOREGONE CONCLUSION?

BECAUSE THAT'S HOW YOU GET FOREGONE CONCLUSION
Passcode > biometric (for now)

- Risk of arrest (e.g. protests)? Switch to passcode
- “Panic button” (iOS 11+) / “Lockdown mode” (Android 9 Pie+) → brings up option to temporarily disable biometric

HONG KONG — The police officers wrestled with Colin Cheung in an unmarked car. They needed his face.

They grabbed his jaw to force his head in front of his iPhone. They slapped his face. They shouted, “Wake up!” They pried open his eyes. It all failed: Mr. Cheung had disabled his phone’s facial-recognition login with a quick button mash as soon as they grabbed him.

(New York Times, July 26, 2019)
If the cops have a warrant & demand you decrypt...

- Get a lawyer
- Consider trade-offs before consenting to decrypt
- If you want to invoke your 5th Am. right, say so!
- If the court rules against you on the 5th Am. claim, contempt is possible if you still refuse to comply
Thank You!
& Suggested Resources

- Wendy Knox Everette talk at ShmooCon 2018: https://www.youtube.com/watch?v=vnyQeQyaN5E

- Nat’l Ass’n of Criminal Defense Lawyers Compelled Decryption primer: https://www.nacdl.org/compelleddecryptionprimer/

- NACDL Border Search primer: https://www.nacdl.org/bordersearches

- EFF Border Search talk at 34C3: https://media.ccc.de/v/34c3-9086-protecting_your_privacy_at_the_border


- Ping me for more! @Riana_Crypto or riana@law.stanford.edu