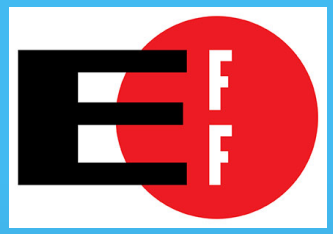


Defending Against the Digital Dragnet

Stephanie Lacambra
Criminal Defense Staff Attorney
Electronic Frontier Foundation

Fighting Compelled Password Disclosure and Decryption

Alphanumeric v. Biometric PWs

- Circuit Ct of VA: VA v. David Baust, 89 VA. Cir. 267, 2014 WL 10355635 (Oct. 28, 2014) - Defendant can't be compelled to produce passcode or decrypt device with PW, but can be compelled to produce fingerprint;
- CDCA: US v. Paytsar Bkhchadzhyan (Feb 25, 2016) - You can be compelled to give your fingerprint to unlock your cell phone

Is Decryption protected by 5th Amend?

YES

1. *US v. Doe*, 465 U.S. 605 (1984)
2. 11th Circuit: US v. John Doe, 670 F.3d 1335 (2012)
3. Circuit Ct of VA: VA v. David Baust, 89 VA. Cir. 267, 2014 WL 10355635 (Oct. 28, 2014)
4. EDPA: SEC v. Bonan Huang, et al., 2015 WL 5611644 (2015)
5. CAAF: US v. Mitchell, No. 17-0153 (Aug 30, 2017)

NO

1. *Fisher v. US*, 425 U.S. 391 (1976)
2. *Doe v. US*, 487 U.S. 201 (1988)
3. Dist of CO: *US v. Fricosu*, 841 F.Supp.2d 1232 (2012)
4. FL Court of Appeal, 2nd District: *FL State v. Stahl*, 206 So.3d 124 (Dec 7, 2016)

PWs not protected by 5th Amend:

- *Fisher v. US*, 425 U.S. 391 (1976):
  1. enforcement against a taxpayer's lawyer wouldn't "compel" taxpayer to do anything and certainly wouldn't compel him to be a "witness" against himself
  2. taxpayers' Fifth Amendment privilege is therefore not violated by enforcement of the summonses directed toward their attorneys
  3. compliance with a summons directing taxpayers to produce accountants' documents, which were not taxpayers' "private papers," would involve no incriminating testimony within protection of Fifth Amendment

PWs not protected by 5th Amend:

- *Doe v. United States*, 487 U.S. 201 (1988)
  1. court order compelling target of grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, does not violate target's Fifth Amendment privilege against self-incrimin.
  2. See Stevens' dissent: "In my opinion that [5th Am] protection gives John Doe the right to refuse to sign the directive authorizing access to the records of any bank account that he may control." P. 221

Decryption not protected by 5th Am:

- *US v. Fricosu*, 841 F.Supp.2d 1232 (D. CO 2012)
  1. Court ordered defendant to give her laptop PW after cops got a search warrant
  2. Court held 5th Amendment privilege against self-incrimination was not implicated by requiring her to produce the unencrypted contents of her computer.

PWs not protected by 5th Amend:

- *FL State v. Stahl*, 206 So.3d 124 (FL Ct App., 2nd Dist. Dec 7, 2016)
  1. You can be forced to give up your password
  2. No meaningful distinction between an alphanumeric passcode and a fingerprint in the context of safeguarding cell phone data:
     "we are not inclined to believe that the Fifth Amendment should provide greater protection to individuals who passcode protect their iPhones with letter and number combinations than to individuals who use their fingerprint as the passcode" p. 135
  3. Neither PW or FP are testimonial

PWs not protected by 5th Amend:

- Miami-Dade Cir: Hencha Voigt & Wesley Victor (May 2017):
  1. Judge Charles Johnson ruled that Hencha Voigt and Wesley Victor must unlock phones.
  2. "For me, this is like turning over a key to a safe-deposit box," Johnson said

PWs ARE protected by 5th Amend:

- *US v. Doe*, 465 U.S. 605 (1984)
  1. contents of business records were not privileged,
  2. but act of producing records was privileged and could not be compelled without a statutory grant of use immunity
  3. Unlike the Court in *Fisher*, we have the explicit finding of the District Court that the act of producing the documents would involve testimonial self-incrimination

5th Amend covers foundational links

- *Hoffman v. US*, 341 US 479, 486 (1951): "The privilege afforded not only extends to answers that would in themselves support a conviction under a federal criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime."

PWs ARE protected by 5th Amend:

- *U.S. v. Djibo*, 151 F.Supp.3d 297 (E.D. N.Y. 2015): Defendant traveler in secondary screening was "in custody" so phone passcode "statement" prior to being *Mirandized* was suppressed; data from phone was further suppressed as "fruit" of non-*Mirandized* statement

PWs ARE protected by 5th Amend:

- *SEC v. Bonan Huang, et al.*, 2015 WL 5611644 (E.D.PA 2015)
  1. held that you may invoke 5th Am to avoid giving up your cell phone passcode
  2. 5th Am protects your PW even to an employer's phone because your PW is personal and producing it requires you to speak or testify against yourself

PWs protected by 5th Am Rt to counsel

- US v. Mitchell, No. 17-0153 (CAAF Aug 2017)
  1. asking for device PW after client invokes violates 5th Amendment right to counsel
  2. After client invoked, agent asks: "if you could unlock it, great, if you could help us out. But if you don't, we'll wait for a digital forensic expert to unlock it" – CAAF found tantamount to interrogation – p.3
  3. "'can you give us your PIN?' – is an express question, reasonably likely to elicit an incriminating response." - P.7

PWs protected by 5th Am Rt to counsel

- US v. Mitchell, No. 17-0153 (CAAF Aug 2017)
  4. "By asking Appellee to enter his passcode, the Government was seeking an "answer[]…which would furnish a link in the chain of evidence needed to prosecute" in the same way that *Hoffman* and *Hubbell* used the phrase. …Appellee's response constitutes an implicit statement 'that [he] owned the phone and knew the passcode for it.'" -P.8
  5. "badgering an unrepresented suspect into granting access to incriminating information threatens the core Fifth Amendment privilege, even if the government already knows that the suspect knows his own password." P. 9

PWs protected by 5th Am Rt to counsel

- US v. Mitchell, No. 17-0153 (CAAF Aug 2017)
  6. Foregone conclusion doctrine doesn't apply
     a) "Govt's eventual access to the phone's contents was not inevitable, but rather 'a matter of mere speculation and conjecture.'" P. 11 (citing US v. Maxwell, 45 M.J. 406, 422 (CAAF 1996)).
  7. Looking for briefing? See EFF amicus: http://www.eff.org/Mitchell - Passcode based decryption is inherently testimonial - not a mere physical act - and absolutely privileged by 5th Amendment
  8. Beware dissent's arg that giving PW is act, not testimonial

Decryption protected by 5th Amend:

- *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012):
  1. Held: decryption and production of device content is testimonial and protected by 5th Am
  2. Foregone conclusion doctrine doesn't apply where govt doesn't know what is hidden behind encryption at time it sought to compel
  3. Court may compel decryption only where govt grants both use and derivative use immunity

Decryption protected by 5th Amend:

- *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335 (11th Cir. 2012):

4. Doe's decryption and production of the contents of the drives would be testimonial, not merely a physical act;
5. the explicit and implicit factual communications associated with the decryption and production are not foregone conclusion
6. govt must show w/ reasonable particularity that it seeks "a certain file and is aware, based on other information, that . . . the file exists in some specified location"

Decryption protected by 5th Amend:

- *VA v. David Baust*, 89 VA. Cir. 267, 2014 WL 10355635 (Circuit Ct of VA Oct. 28, 2014):
  1. compelling production of PW & decrypting recording of assault that may have been transmitted to defendant's encrypted cell phone would violate defendant's Fifth Amendment privilege against self-incrimination
  2. reasoning: the recording is not a foregone conclusion, Defendant's production of the unencrypted recording would be testimonial because Defendant would be admitting the recording exists, it was in his possession and control, and that the recording is authentic.
  3. State could not compel Defendant to produce PW or decrypt the recording

Beware “foregone conclusion”

- *US v. Gavegnano*, 305 F.Appx 954, 956 (4th Cir. 2009) Post-invocation PW requests don’t violate 5th Amendment because any self-incriminating testimony is a “foregone conclusion” where the Government can independently prove that the suspect was the sole user and possessor of the device

Beware PW as "non-testimonial" consent:

- *US v. Patane*, 542 U.S. 630 (2004):
  1. Self-incrimination Clause cannot be violated by introduction of nontestimonial evidence obtained as result of voluntary statements
  2. failure to give Miranda warnings does not require suppression of physical fruits of suspect's unwarned but voluntary statements
- *US v. Venegas*, 594 F.Appx 822, 827 (5th Cir 2014)(per curiam) – "statement granting consent to a search…is neither testimonial nor communicative in the Fifth Amendment sense"

Beware PW as “non-testimonial” consent:

- US v. Hank Robinson, 76 M.J. 663 (AFCCA May 2017)
  1. Defendant consented to search of his cell phone
  2. Investigator's request for passcode for accused's cell phone after he invoked his right to counsel was not an interrogation and thus did not violate his rights under Fifth Amendment
  3. Because there was no dispute as to Appellant's ownership, dominion, or control over the phone, his knowledge of the passcode did not incriminate him.
  4. Investigators had no reason to believe that the passcode itself would be incriminating or communicate any information about the crime - p. 671

Beware PW as "non-testimonial" consent:

- US v. Chad Blatney, 2017 WL 2422807 (May 2017)
  1. Govt's appeal granted
  2. MJ's granting of MTS vacated
  3. case remanded to permit trial judge to analyze issue consistent with Robinson opinion, and to clarify whether the investigators' request to defendant to unlock his iPhone constituted interrogation

Counter argument: PW IS testimonial:

- US v. Kirschner, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010)
  1. Fact that a passcode emanates from “mental processes” is enough to deem it testimonial when it is spoken or subpoenaed.

Immunity for disclosure:

- *US v. Hubbell*, 530 U.S. 27 (2000) –
  1. Held immunity granted client in prior prosecution in exchange for his disclosure of broad categories of documents responsive to subpoena precluded subsequent, unrelated prosecution, to extent that testimonial aspect of defendant's act of producing documents was first, necessary step in discovery of evidence supporting 2nd prosecution
  2. significant difference between the use of compulsion to extort communications from a defendant and compelling a person to engage in conduct that may be incriminating p.34-35 – foreshadows PW v. FP

Immunity for disclosure

- *US v. Hubbell*, 530 U.S. 27 (2000) –

3. the act of producing documents in response to a subpoena may have a compelled testimonial aspect. … 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." P.36
4. long been settled that its protection encompasses compelled statements that lead to the discovery of incriminating evidence even though the statements themselves are not incriminating and are not introduced into evidence p.37

Contempt for Failure to disclose:

- *US v. Bright*, 596 F.3d 683 (9th Cir. 2010)
  1. sanction of contempt was justified for taxpayer wife with primary possession of documents for failure to respond to IRS summons for credit card accounts
  2. sanction of contempt was justified for taxpayer husband, even if he lacked primary possession documents

Contempt for Failure to disclose:

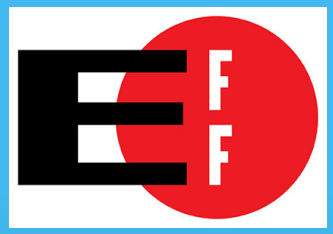
- *Apple v. John Doe*, 851 F.3d 238 (3rd Cir. Mar 2017)
  1. Refusing to decrypt your hard drive for authorities, even if you've allegedly forgotten the password, is still considered contempt of court.
  2. decryption order did not violate suspect's Fifth Amendment protection against self-incrimination because foregone conclusion rule was applicable since Government provided evidence to show both that files existed on encrypted portions of devices and that suspect could access the files

Contempt for Failure to disclose:

- Miami-Dade Cir: Hencha Voigt & Wesley Victor (May 2017):
  1. Voigt & Victor not held in contempt for failing to give correct passcodes because no way to prove that they actually remembered their passcodes more than 10 months after initial arrest
  2. BUT Israeli tech company Cellebrite helped state investigators finally hack into the iPhone.

Contempt for Failure to disclose:

- FL Broward Circuit: Christopher Wheeler (May 30, 2017)
  1. Hollywood video voyeur, taken into custody for 180 days for failing to give correct PW to his phone b/c judge didn't believe he had forgotten code.
  2. Wheeler insisted he had already provided the pass code to police investigating him for child abuse, although the number did not work



Questions?

Stephanie Lacambra
Criminal Defense Staff Attorney
Electronic Frontier Foundation
815 Eddy St., San Francisco, CA 94109
415-436-9333 x130
stephanie@eff.org