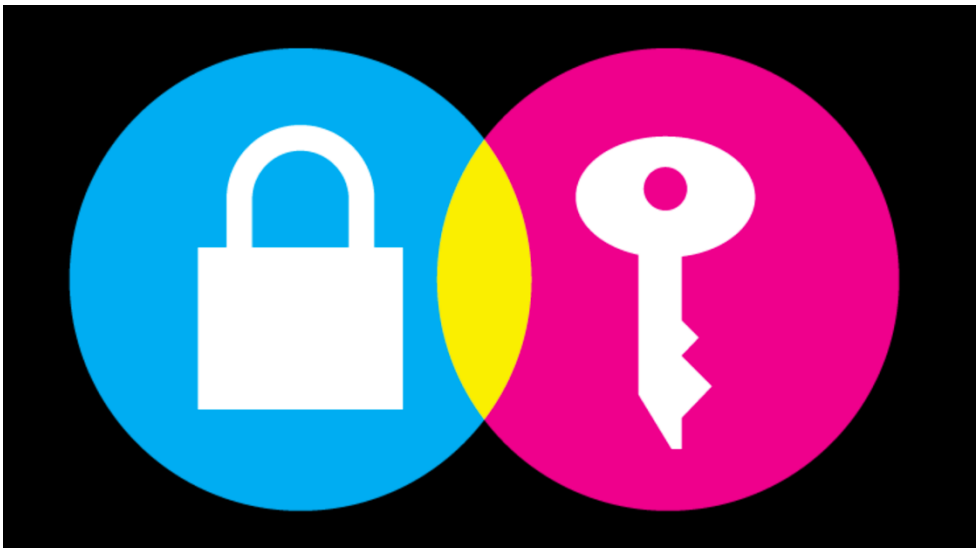
ELECTRONIC FRONTIER FOUNDATION

Compelled Use & Disclosure of Passwords

A Guide for Criminal Defense Attorneys



EFF One-Pager
Revised
4.25.18

Support our work on Compelled PWs & Decryption: eff.org/donate

What are they?

- A password is a secret word, phrase, string of characters or physical attribute that must be used to gain access to a digital device, computer, interface or system.
    - Alphanumeric – PWs made up of some combination of alphabetical, numerical, and/or special characters or other symbols
    - Biometric – PWs based on physical identifiers like fingerprint, iris or face scans;
- For Fifth Amendment purposes, the main distinction between alphanumeric and biometric PWs is whether the PW is stored in the mind or is a part of the body
- Passwords are commonly used to encrypt devices.
- Computer-assisted encryption uses sophisticated algorithms to transform readable data into a code of seemingly random information meant to prevent unauthorized access to encoded data.
- Decryption is the process of translating that encoded text into a format that can be read and understood by computers or people.

How does it work?

- PW compulsion generally arises in two contexts:

    1. During the course of an arrest or investigation where law enforcement demands access (without a court order) or asks for consent to search, either by asking for the passcode or for the target to unlock the phone
    2. Overt, court-ordered compulsion where a device is locked or encrypted and the government seeks a court order compelling the target to unlock or decrypt the device

Compelled PW disclosure Cases:

- Passwords used or disclosed during the course of an arrest or interrogation:
    1. *US v. Mitchell*, 76 M.J. 413, 419 (CAAF Aug 2017): govt violates 5th Am when asking for PW in absence of counsel (in military context)("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.")
    2. *U.S. v. Djibo*, 151 F.Supp.3d 297 (E.D. N.Y. 2015): Def. in secondary screening is "in custody" so passcode = "statement" b4 *Miranda* and must be suppressed along with data seized
    3. *But see US v. Gavegnano*, 305 F.Appx 954, 956 (4th Cir. 2009): Post-invocation PW requests ≠ 5th Am. viol. b/c any self-incriminating testimony is a "foregone conclusion" where govt can independently show target was sole user/possessor of the device
    4. *But see US v. Ashmore* (W.D. Ark 2016) – PW obtained in viol. of Miranda suppressed, but evidence seized from devices was admissible under the independent source (though was really inevitable discovery) exception to exclusionary rule b/c devices not encrypted.
- Court-ordered compelled use or disclosure of passwords
    A. *Alphanumeric PW disclosure is testimonial:*
        1. *US v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010): subpoena for PWs violated 5th Am. because it comes from target's "mental processes"
        2. *SEC v. Bonan Huang, et al*., 2015 WL 5611644 (E.D.PA 2015): 5th Am protects PW even to employer's phone because producing PW is testimonial
        3. *VA v. David Baust*, 89 VA. Cir. 267 (Cir Ct of VA 2014): can't compel alphanumeric PW production or decryption; but can compel FP
        4. *But see FL State v. Stahl*, 206 So.3d 124 (FL Ct App. 2016): can compel PW because no meaningful difference between FP & PW, thus decryption order doesn't violate 5th Am
    B. *Password use and decryption is privileged testimonial act, and **not** a foregone conclusion:*
        1. *In re Grand Jury SDT Dated March 25, 2011*, 670 F.3d 1335(11th Cir. 2012): decryption of device content is testimonial and protected by 5th Am
    C. *Password use and decryption is privileged testimonial act, but **was** a foregone conclusion:*
        1. *US v. Apple Macpro Computer*, 851 F.3d 238 (3rd Cir. 2017): applying similar standard to 11th Circuit, but allowing compelled decryption under different facts
        2. *US v. Fricosu*, 841 F.Supp.2d 1232 (D. CO 2012): suspect compelled to decrypt computer after jailhouse recording of her admitting files were on computer
        3. *Matter of Search of a Residence in Aptos, California 95003*, 2018 W: 1400401 (N.D. CA 2018): Ct orders PW disclosure b/c "testimonial value of decryption …is a 'foregone conclusion'"
    D. *Biometric PWs can be compelled:*
        1. *VA v. David Baust*, 89 VA. Cir. 267 (Cir Ct of VA 2014): FP can be compelled
        2. *US v. Paytsar Bkhchadzhyan* (C.D. CA 2016): FP can be compelled
    E. *Biometric PWs can't be compelled*
        1. *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (E.D. IL 2017) – boilerplate, open-ended SW to seize FPs of any individuals on scene to unlock devices unjustified

- Note: Compelled Decryption (whether by PW or FP) should be protected by the 5th Am because decryption is always testimonial—whether accomplished through a memorized passcode or biometric—since it causes translation of unintelligible data into a format that law enforcement can read and understand; it isn't the mere surrender of data, but a translation of existing information

Stephanie Lacambra, Criminal Defense Staff Attorney 415-436-9333 x130, stephanie@eff.org