JUNE 27, 2016

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

IN PRACTICE

The law's breakable protections for unbreakable encryption

By David W. Fermino and Louis P. Feuchtbaum

A client comes to you because FBI agents seized his iPhone pursuant to a search warrant, which seeks particular records that are stored within it. The client has kept his iPhone locked at all times because it contains sensitive data that may be incriminating to him, and the government is now seeking to compel his assistance in unlocking that device. The client wants to know whether he can be forced to assist the FBI's investigation against him in this manner. Surprisingly, the answer to that question may depend upon which mechanism the client used to lock his iPhone: An unbreakable electronic "lock," such as a thumbprint or other biometric, may be less secure than a four-digit password that could be easily cracked because the law may treat differently the compelled production of each "key."

If an electronic device is secured with a password, the government sometimes may not be able to compel production of the password required to unlock the device because doing so could violate a person's Fifth Amendment right against making self-incriminatory statements, as that has been recognized in *United States v. Hubble*, 530 U.S. 27 (2000). However, as evidenced by a recent warrant issued by a magistrate judge in the United States District Court for the Central District of California, where an electronic device is secured by a biometric lock, a person may be required to assist the government's investigation by unlocking the device because the law doesn't provide Fifth Amendment protection against compelled disclosure of a biometric "key," such as a thumbprint.

To be sure, courts across the country will be called upon to make decisions about biometrics as the use of encrypted devices by consumers continues to rise. Today, our data is protected by everything from iris scans at airports to heartbeat measurements and ear-print Smartphone locks. A recent order issued by a federal magistrate in Los Angeles ordering a defendant to unlock an iPhone with her fingerprint is a fresh example of what can happen when a 225-year-old law is applied to a field as rapidly changing as digital security.

In the Central District case, the FBI wanted the fingerprint of Paytsar Bkhchadzhyan, a 29 year-old woman from Los Angeles who pleaded no contest to a felony count of identity theft. Court records reveal that after Ms. Bkhchadzhyan was taken into custody, U.S. Magistrate Judge Alicia Rosenberg issued a warrant for the defendant to press her finger on a phone that had been seized from the residence of her boyfriend—a reputed member of the Armenian Power gang. The phone is secured by Apple's fingerprint identification system, and prosecutors wanted the data inside of it.

To date only a few written decisions have been issued dealing with whether a defendant can be forced to unlock his or her iPhone with a fingerprint. Not surprisingly, legal scholars are split on the constitutional implications of forced disclosure of biometric keys. Some argue that there should be a higher bar for biometric data since the act of pressing a finger to a phone breaches an individual's Fifth Amendment protection against self-incrimination because the act is equivalent to authenticating the contents of the phone. Others argue that a fingerprint is not testimonial as its use does not force an individual to state what is in their mind.

When the government seeks to compel a target or criminal defendant to produce or enter a password to unlock a device, the Fifth Amendment is implicated to the extent that : 1) the act is "testimonial"; and 2) the facts about which the act is testimonial might tend to incriminate the witness. An act is testimonial if it requires the witness to reveal the contents of his mind, and in so doing to communicate something—in this case the existence, possession, and authenticity of the data behind the locked door. See *United States v. Hubbell*, 530 U.S. 27, 36 (2000) (testimonial nature of "act of production" in a non-digital context). In *United States v. John Doe*, the Eleventh Circuit found that a defendant, who possessed a hard drive protected by encryption, could not be compelled to disclose his decryption password because the Fifth Amendment protected him from having to provide information that could "lead the government to evidence that would incriminate him."

It is important to note that while *Hubble* immunity may sometimes protect a target from having to provide an encryption key, that is not always the case. In *United States v. Fricosu*, a federal court in Colorado ruled that Fifth Amendment protections did not apply to compelled disclosure of an encryption key where it was a foregone conclusion that the defendant's password-locked data was incriminating. In *United States v. Apple MacPro Computer*, a case pending before the Third Circuit, a John Doe defendant has been jailed in contempt of court for nine months because he has refused to provide an encryption key that would unlock hard drives on which law enforcement believes there is evidence of child pornography. John Doe remains

in jail while the Third Circuit considers his appeal.

While the federal courts in this state have yet to issue a written decision on this issue in the digital context, decisions from other states shed light on how California courts might rule. In *Commonwealth of Virginia v. Baust*, the court ruled that fingerprints are not protected by the Fifth Amendment. The ruling stemmed from a case involving David Baust, who was accused of strangling his girlfriend. Prosecutors believed Baust may have stored video of the attack on his phone. However, the phone was locked and could only be entered using a passcode or fingerprint. The court found that Baust could not be compelled to provide his passcode to access the smartphone, but could be compelled to produce his fingerprint to access the phone. Producing the passcode would require the defendant to divulge knowledge -- information from his own mind, placing it in the testimonial realm. However, the court concluded that a fingerprint does not require any similar knowledge—it is equivalent to a key that fits into a lock. The Court required Baust to provide his thumbprint and unlock his iPhone.

Traditional analogies of providing a "key" to open a "lock" do not seem to fit modern-day electronic devices. The United States Supreme Court recently made clear in *Riley v. California*, 134 S.Ct. 2473, 2477 (2014) that a cell phone is different from a lockbox. Although the issue in *Riley* was grounded in Fourth Amendment analysis, the court's recognition of the ever increasing functionality of cell phones merits discussion here. The court observed that even calling a cell phone a "phone" was likely a misnomer. Our phones store vast amounts of uniquely personal information—a virtual diary. In describing cell phones thusly, the court reasoned that they cannot be treated like any other object. It follows then that the circumstances under which the police may unlock a person's phone have deep implications for our privacy rights because of their wide use, vast data storage, and seemingly unbounded capabilities. In the days before smartphones, people did not carry vast amounts of paper information on or near their person, as is now typical of most cell phone users. In this changing landscape, perhaps neither a passcode nor fingerprint should be compelled under the Fifth Amendment.

The scope of the Fifth Amendment's protections against self-incrimination is far from clearly defined when it comes to encrypted devices. This places the security question squarely in the hands of each individual user. Your choice of security method depends on who you're more worried about having access to your phone. If it is a question of protecting your device against theft, then a fingerprint might suffice. But if it is the long reach of the government that you are seeking protection against,a password or digital encryption key may be more secure.


David Fermino is a partner at Sideman & Bancroft in San Francisco focused on white-collar criminal defense, cybercrimes and data security incidents, intellectual property, and complex criminal and civil appeals in the state and federal courts. Louis Feuchtbaum is a partner at Sideman & Bancroft in San Francisco focused on white-collar criminal defense, protecting intellectual property rights and complex civil litigation. A former assistant district attorney in the Bronx, Mr. Feuchtbaum specialized in investigating and prosecuting organized crime and official corruption cases.