All Thumbs?

Mobile biometrics, your data, and the law.

BY TOM KULIK

With all the commotion revolving around the Apple/FBI dispute and accessing encrypted data in the iPhone iOS, it should come as no surprise that mobile device makers and application providers have been ramping up efforts to better protect content from unauthorized access.

The WhatsApp secured messaging service owned by Facebook now encrypts voice calls,[1] in addition to its existing privacy features. Not to be outdone, Snapchat is reportedly working on a secure messaging system,[2] while Twilio, a cloud-based communications platform, announced a partnership with Virgil Security[3] that will enable developers to build strong encryption into their messaging services.

Notwithstanding this flurry of activity, such accelerated development ignores a critical component for protection of user content on the mobile device—and it has your fingerprints all over it.

The Fifth Amendment of the U.S. Constitution guarantees "no person shall be compelled in any criminal case to be a witness against himself." The founders intended this protection as an important check on governmental power in collecting evidence directly from a defendant, essentially prohibiting the government from forcing you to provide testimony against yourself that may incriminate you or "otherwise provide the State with evidence of a testimonial or communicative nature."[4]

The key point here is the word "testimony"—something the courts have interpreted as "when the accused is forced to reveal his knowledge of facts relating him to the offense or from having him share his *thoughts or beliefs* with the government."[5] So, compelling you to divulge *knowledge* of something that may incriminate you (such as the passcode on a mobile device) is prohibited; compelling you to provide a *physical characteristic* (such as presenting yourself in a lineup, being required to use your voice to provide an identifying characteristic, or being compelled to provide a *fingerprint*) is not.

Transposing this line of precedent to today's technology, Hon. Steven C. Frucci, a judge of the 2nd Judicial Circuit in Virginia, recently ruled that, unlike passcodes, using fingerprints to unlock a mobile phone does not constitute "compelled testimony" under the Fifth Amendment. Basically, the judge ruled, "exhibiting such physical characteristics is not the same as a sworn communication"[6]—so compelling the defendant to use his or her fingerprint to unlock the iPhone equates to the presentation of a physical characteristic, *not* compelled testimony under this ruling. Ironically, compelling a defendant to provide a passcode violates the Fifth Amendment but compelling the use of a fingerprint to get to the same content does not.

This is not to say that everyone should be ignoring Touch ID on their iPhones in favor of passcodes to circumvent law enforcement—quite the contrary. Companies should be aware of this security gap and stay abreast of developments so that it cannot be exploited:

- Where your company permits employees to "bring your own device," or BYOD, the protection that comes with requiring fingerprint identifiers must be carefully weighed against the inherent vulnerability of fingerprint IDs, which cannot be changed and can be stolen. In many cases, your company may find it best *not* to permit BYOD whatsoever or otherwise significantly restrict BYOD use (i.e., prohibit connection to the network, email servers, etc.).
- If your company has determined that the balance tips in favor of using fingerprint (or other biometric) identifiers, company policies should ensure that employees using mobile devices for company communications have such identifiers enabled (where available). If a situation should ever arise where an employee is charged with criminal conduct (i.e., embezzlement from your company) and the content on his or her mobile device may hold relevant evidence, the availability of this access control mechanism may be key.
- Notwithstanding the current state of the law, this issue is far from settled—the fact that a fingerprint performs the same function as a passcode to provide access to the same information on the mobile device cannot be ignored and may influence future court decisions—so you will need to stay abreast of developments through qualified counsel.

I would not be surprised if mobile device makers close this gap by allowing passcodes to be tied to biometric identifiers so that governmental access cannot be easily compelled. That said, the evolution of technology might reach the point where the underlying physical characteristic rises to the level of a "communication."

Although ultrasonic fingerprint sensors, retinal scanners, and DNA fit into the current legal framework, what about hybrid methodologies that incorporate some other "passkey" intervention? At what point will biometrics cross the line into testimony that fits within Fifth Amendment protections (if at all)?

As technology continues to rapidly advance, the answer to these questions becomes less clear and, at a minimum, will depend on the nature of the biometric technology at issue and (potentially) the content sought. Without question, such biometrics are already making a statement, but for now, just not the kind protected by the Fifth Amendment. **TBJ**

Notes

1. Danny Yadron, *Facebook, Google and WhatsApp plan to increase encryption of user data,* The Guardian, https://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increase-encryption-fbi-apple (Mar. 14, 2016).
2. *Id.*
3. Kate Conger, *Adding end-to-end encrypted messaging to your app just got a lot easier,* Tech Crunch, https://techcrunch.com/2016/05/03/adding-end-to-end-encrypted-messaging-to-your-app-just-got-a-lot-easier/ (May 3, 2016).
4. *United States v. Wade,* 388 U.S. 218, 87 S.Ct. 1926, 18 L.Ed.2d. 1149 (U.S., 1967).
5. *United States v. Kirschner,* 823 F.Supp.2d 665 (E.D. Mich., 2010) (emphasis added).
6. Hon. Steven C. Frucci, Order re: Motion to Compel the Production of the Passcode or Fingerprint to Encrypted Smartphone, *Commonwealth of Virginia v. David Charles Baust,* CR14-1439.

This article, which originally appeared on Kulik's blog, has been updated, edited, and reprinted with permission.

TOM KULIK *is an intellectual property and technology partner at Scheef & Stone, a full-service commercial law firm based in Texas. He uses his award-winning industry experience in technology to creatively help his clients navigate the complexities of law and technology in their businesses. Read more about his thoughts on the intersection of law, business, and technology at legalintangibles.com.*