BUSINESS CRIMES BULLETIN

FEBRUARY 2020

Biometrics and the Fifth Amendment: A New Frontier

By Jonathan S. Feld, Jason Ross and Amelia Marquis

In recent years, new questions have arisen regarding privacy and the scope of certain constitutional protections, stemming from the dramatic increase of use of electronic devices, such as smartphones, tablets, and laptop computers, to conduct business. The Government's interest in accessing such devices is increasing and unsurprising: electronic devices often contain a goldmine of communications of interest to law enforcement, including text messages, email, and social networking applications. Additionally, some of the most frequently used "apps" store highly sensitive data, including financial records, health records, photographs, and evidence of internet activity, just to name a few.

When used for work, mobile devices routinely contain employers' proprietary and confidential data. The struggle between Government requests for access to such data and constitutional protections — including the Government's ability to compel the turnover of biometric "keys" to unlock mobile devices — create areas of concern for employers. How the protections of the Fourth Amendment against unreasonable seizures and the Fifth Amendment against self-incrimination will apply to information stored on their employees' personal and business mobile devices is starting to unfold.

The Legal Landscape Surrounding Biometrics Continues to Evolve

Apple began the smartphone era with the release of the iPhone in June 2007. *See*, Stephen Silver, "Apple Details History of App Store on its 10th Anniversary," *Appleinsider* (Jul 5, 2018). Currently, new apps — with new methods of tracking and storing users' personal data — are constantly released and the amount of information stored on mobile devices is rapidly increasing. To protect the vast quantity of sensitive data stored on mobile devices, mechanisms to secure devices have also rapidly progressed since smartphones were first introduced.

For years, numeric or alphanumeric passcodes served as the primary security feature on cellphones. Now, many smartphones allow owners' biometrics — unique physical characteristics including fingerprints, irises and facial features — to be used to unlock the phone, thereby providing access and control of the device. *See*, "Biometrics," U.S. Department of Homeland Security. In particular, fingerprint recognition and facial recognition technologies are frequently used as biometric "keys" to unlock mobile devices and decrypt sensitive information stored on devices.

As the use of biometric keys has increased, some states have enacted laws to protect the collection, use, and retention of biometric data. Indeed, some states have created private rights of action for misuse of biometric data. Illinois, Texas, Washington and California have biometric privacy laws in place, while Arizona, Florida and Massachusetts have proposed biometric privacy legislation. *See*, "The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States," *The National Law Review* (Mar. 25, 2019). However, state laws do not use a uniform definition of "biometric information" or "biometric identifier" As civil litigation continues to grow with the advent of biometric privacy laws, federal district courts and state courts are grappling with whether biometric keys are entitled to protection under the Fifth Amendment.

Lack of Guidance on the Fifth Amendment Protections

The Fifth Amendment protection against self-incrimination is a murky area for biometrics. The Fifth Amendment privilege protects against "directly or indirectly" providing information that may be a "link in the chain" to show criminal conduct. *See*, *United States v. Hubbell*, 530 U.S. 27, 38 (2000); *Doe v. United States*, 487 U.S. 201, 207, n. 5 (1988). However, the privilege is limited to communications that are "testimonial" in nature. *Hubbell*, 530 U.S. at 36. While the accused may be compelled to surrender a physical key to a strongbox containing incriminating documents without implicating Fifth Amendment protections, the privilege would prohibit compelling the accused to reveal the combination to a wall safe, which would require the accused to express the contents of his mind. *Doe*, 487 U.S. at 210, n. 9. In other words, does the Government request of a biometric key lead to "testimonial" acts that fall within the scope of the Fifth Amendment?

The U.S. Supreme Court has established that other types of physical evidence, including a handwriting or voice exemplar, are not testimonial in nature. *Hubbell*, 530 U. S. at 35. Yet, the Court has also held that the act of producing documents is, in certain instances, testimonial. In *Hubbell*, the Court considered whether compelling the subject of a grand jury investigation to respond to a subpoena requesting documents, but not testimony, was barred by the Fifth Amendment. *Id*. at 31. The Court held that the production of documents was "testimonial" and, therefore, subject to Fifth Amendment protection. The rationale is because the act of identifying responsive documents forced the respondent to use "the contents of his own mind," *id*. at 43, it is "testimonial." Therefore, it was akin to giving the Government the combination to a wall safe as opposed to the surrendering of a physical key. *Id*.

Due to the lack of precedent specifically addressing whether compelling the use of biometric keys is testimonial in nature, courts have reached different conclusions when applying the Fifth Amendment. In two recent cases involving biometrics, the federal district courts in California and the District of Columbia considered Chief Justice Roberts' instruction in *Carpenter* to "take account of more sophisticated systems that are already in use or in development" in order to not leave individuals "at the mercy of advancing technology." *See*, *Carpenter v. United States*, 138 S. Ct. 2206, 2214, 2218-19 (2018). The two district courts reached opposite conclusions.

In the District of Columbia case, the Government sought a search warrant for premises and to seize cellphones and computers as well as authorization to compel biometric features of any individuals involved in the alleged criminal activity in order to unlock such devices. *In re Search of*, 317 F. Supp. 3d 523, 525-26 (D.D.C. 2018) (extortion). The court found that the subject's biometric features were not testimonial communications under the Fifth Amendment because the owner of the device "would be required to communicate nothing" by unlocking the device. *Id*. at 538. The court explained that, unlike the *subpoena duces tecum* in *Hubbell*, which required assembling and selecting hundreds of documents, "[t]he biometric feature collection process outlined in the Affidavit requires no comparable cognitive exertion by the Subject here." *Id*. at 539.

In contrast, the Northern District of California found biometric features are protected under the Fifth Amendment. The court considered an application for a search and seizure warrant seeking to compel

any individual present to use their biometric features to unlock electronic devices found during the search. *Matter of Residence in Oakland, California*, 354 F.Supp.3d 1010, 1013 (N.D. Cal. Jan. 10, 2019) (fraudulent activity involving computers). The court reasoned that biometrics are "analogous to the nonverbal, physiological responses elicited during a polygraph test, which are used to determine guilt or innocence, and are considered testimonial." *Id*. at 1016. It also noted that unlocking a phone with a finger or thumb scan "exceeds the 'physical evidence' created when a suspect submits to fingerprinting to merely compare his fingerprints to existing physical evidence … because there is no comparison or witness corroboration required to confirm a positive match." *Id*.

Other federal district courts, including the Northern District of Illinois, the United States District Court for the District of Nevada, and the District of Idaho, and state courts have wrestled with this analysis and reached different conclusions. *See*, *e.g.*, *In re Search Warrant Appl.*, 279 F. Supp. 3d 800 (N.D. Ill. 2018) (holding that an application to compel the fingerprints of four residents of a home subject to search did not violate the Fifth Amendment protection against self-incrimination); *State v. Diamond*, 905 N.W.2d 870, 875 (Minn. 2018) ("But producing a fingerprint to unlock a phone, unlike the act of producing documents, is a display of the physical characteristics of the body, not of the mind, to the police."). Until there is guidance from the federal Courts of Appeals, lower courts will likely continue to reach inconsistent results based on specific circumstances and leave biometrics vulnerable to compulsion.

The Use of Biometric Keys to Gain Access to Electronic Devices Raises Concerns for Employers

Biometric keys provide opportunities for third parties to "unlock" smart devices and employers are now vigilant to safeguard sensitive company data stored on devices owned by employees. Smart devices may contain confidential and proprietary company data, and even confidential information owned by customers or clients, which is shared with the expectation that it will be protected from disclosure.

In granting access to traditional computers, courts have emphasized the need for law enforcement to describe with particularity the specific files within the computer that will be subject to seizure because the computer itself may contain a "huge array" of information beyond the scope of the Government's search and seizure request. *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). While smart devices may contain a similar array of information, companies should take steps to limit the chances that such data is swept up in a law enforcement seizure. Implementing Bring Your Own Device (BYOD) policies that require two-factor authentication to access apps containing employer-owned data; prohibiting work-related use of apps that commingle personal and company information — such as photo-storing apps and "notes" apps; and enacting document retention protocols that automatically delete older company files on smart devices are a few ways to limit risk.

Conclusion

As smart devices become smarter, the methods of unlocking devices are likely to become more difficult to parse under the traditional "testimonial" and "non-testimonial" criteria. Courts will continue to reach different conclusions until clear directions emerge from the Courts of Appeal or legislatures. Until then, the applicability and scope of constitutional protections will be in flux.

*****

Jonathan S. Feld is the Leader of Dykema's Governmental Investigations Group and a member of this newsletter's Board of Editors. **Jason Ross** is a Member of the firm in the Governmental

Investigations Group. **Amelia Marquis** is an Associate in the Business Litigation Group.
