Biometrics and Search Warrants: The Intersection of Your iPhone and the Fourth and Fifth Amendments

March 4, 2019

On January 19, 2019, federal Magistrate Judge Kandis Westmore of the Northern District of California denied the Government's application for a search warrant that sought:

1. "all digital devices" present at a California residence; (Order at 3), and
2. "any individual present at the time of the search to press a finger (including thumb) or utilize other biometric features…for the purposes of unlocking the digital devices found in order to permit a search of the contents," (Order at 1).

The request for the "use of biometrics" was stunning. Magistrate Judge Westmore denied the Government's initial request, but invited the Government to submit a new search warrant. A day later when the Government submitted an amended application, it omitted the request to use biometrics. The court granted that amended application. Since the Government's application named only two suspects in its affidavit, the Government's request to compel any other individual present at the time of the execution of the search warrant to unlock their digital device(s) was too expansive.

Judge Westmore also determined the Government's request to require all individuals present to provide their "biometrics" was not justified. Order at 2. "Courts that have addressed the passcode issue have found that a passcode cannot be compelled under the Fifth Amendment, because the act of communicating the passcode is testimonial." Order at 4. Judge Westmore explained the important differences between a suspect submitting his fingerprints and DNA, and the same suspect using his fingerprint to unlock a device that could otherwise only be unlocked by a passcode. Although such evidence can place a suspect in a physical location, the Fifth Amendment prevents the Government from compelling a suspect to divulge his passcode—an "expression of the contents of an individual's mind." Order at 4. While technology is moving at a faster pace than the law, the Order underscored the Supreme Court's emphasis that courts must "take account of more sophisticated systems that are already in use or development" when making decisions about what data is constitutionally protected. *Carpenter*, 138 S. Ct. at 2218-19 (citation omitted).

Judge Westmore's denial to compel the use of biometrics from individuals is an important recognition of the privacy issues inherent in electronic data collection. Relying on the Supreme Court's *Carpenter* decision, the court ruled that the Fifth Amendment precluded forcing a person to allow a fingerprint or other biometric feature it would be "compelling testimony." It would be no different than compelling a person to reveal a "password."

In response to Magistrate Judge Westmore's initial denial of its search warrant, the Government, has filed a Request for Review of the Duty Magistrate Judge's Denial of a Search Warrant Application. A hearing on this request is currently set for March 13, 2019.

For more information, please contact: Jonathan S. Feld at 312-627-5680 or jfeld@dykema.com, Ferdose al-Taie at 214-462-6432 or fal-taie@dykema.com, Jane Gerber at 214-462-6497 or jgerber@dykema.com, or your Dykema relationship attorney.

Attorneys

Jonathan S. Feld

Practice Areas

Privacy and Data Security