"THE FEDERAL CORNER"

Cell Phones, Computers, Fingerprints, Decryption Orders and Civil Contempt

Buck Files

Last Spring, I came across an article from the *Los Angeles Times* written by Matt Hamilton and Richard Winton and entitled "A New Frontier in Battle OverDigital Security." 2016 WLNR 13156357 (April 30, 2016). Because I had been interested in whether individuals can be required to unlock their iPhones and iPads by having their fingerprints involuntarily placed on these devices, I kept the article for another day – which is today. The article reads, in part, as follows:

> As the world watched the FBI spar with Apple this winter in an attempt to hack into a San Bernardino shooter's iPhone, federal officials were quietly waging a different encryption battle in a Los Angeles courtroom.
>
> There, authorities obtained a search warrant compelling the girlfriend of an alleged Armenian gang member to press her finger against an iPhone that had been seized from a Glendale home. The phone contained Apple's fingerprint identification system for unlocking, and prosecutors wanted access to the data inside it.
>
> It marked a rare time that prosecutors have demanded a person provide a fingerprint to open a computer, but experts expect such cases to become more common as cracking digital security becomes a larger part of law enforcement work.*The Glendale case and others like it are forcing courts to address a basic question: How far can the government go to obtain biometric markers such as fingerprints and hair?* (emphasis added)
>
> * * *
>
> In the Glendale case, the FBI wanted the fingerprint of PaytsarBkhchadzhyan, a 29-year-old woman from L.A. with a string of criminal convictions who pleaded no contest to a felony count of identity theft.
>
> She was sentenced in that case on Feb. 25 in a Van Nuys courtroom. Jail records and court documents show that about 45 minutes after Bkhchadzhyan was taken into custody, U.S. Magistrate Judge Alicia Rosenberg – sitting in a federal courtroom 17 miles away – signed off on the warrant for the defendant to press her finger on the phone.By 1 p.m., an FBI agent specializing in cybercrimes took her print, according to court papers.
>
> Why authorities wanted Bkhchadzhyan to unlock the phone is unclear. The phone was seized from a Glendale residence linked to SevakMesrobian, who according to a probation report was Bkhchadzhyan's boyfriend and a member of the

> Armenian Power gang with the moniker of '40.' Asst. U.S. Atty. Vicki Chou said the search was part of an ongoing probe. She declined to comment further.
>
> * * *
>
> George Mgdesyan, an attorney who has previously represented both Bkhchadzhyan and Mesrobian, said he was unsure why authorities were trying to unlock her phone. He said he was not representing Bkhchadzhyan in any federal criminal matter and believed the probe included hacking and possibly 'other issues.'

I was reminded of that article when I read *In re Application for a Search Warrant*, ___F.Supp.3d___, 2017 WL 758218 (N.D. Ill. Feb. 16, 2017) [Opinion by United States Magistrate Judge M. David Weisman]. This case presents anattempted extension of what we saw in the *LA Times* article. Judge Weisman's opinion reads, in part, as follows:

> [An Overview of the Case]
>
> The government has presented an application for a search and seizure warrant to seize various items presumed to be located at a particularly identified location (hereinafter 'subject premises'). The warrant further requests the authority to seize various items (identified in Attachment B of the warrant application), including various forms of electronic storage media and computer equipment (hereinafter collectively 'electronic storage media').
>
> * * *
>
> … *in its warrant application, the government also seeks the authority to compel any individual who is present at the subject premises at the time of the search to provide his fingerprints and/or thumbprints 'onto the Touch ID sensor of any Apple iPhone, iPad, or other Apple brand device in order to gain access to the contents of any such device.' For the reasons set forth below, this aspect of the search warrant application is denied.* (emphasis added)
>
> * * *
>
> [The Issues Presented]
>
> The issues presented in this warrant application are at the cross section of protections provided by the Fourth and Fifth Amendments. Essentially, the government seeks an order from this Court that would allow agents executing this warrant to force 'persons at the Subject Premises' to apply their thumbprints and fingerprints to any Apple electronic device recovered at the premises. The request is neither limited to a particular person nor a particular device. And, as noted below, the request is made without any specific facts as to who is involved in the criminal conduct linked to the subject premises, or specific facts as to what particular Apple-branded encrypted device is being employed (if any).
>
> [The Probable Cause Issue]

First, the Court finds that the warrant does not establish sufficient probable cause to compel any person who happens to be at the subject premises at the time of the search to give his fingerprint to unlock an unspecified Apple electronic device.

* * *

[The Self-Incrimination Issue]

Second, and in addition to the Fourth Amendment concerns articulated above, the Court believes that the government's warrant application raises concerns under the Fifth Amendment's protection prohibiting compelled self-incrimination. In its submission, the government argues that '[b]ecause depressing a fingerprint to a device results in no "testimonial communication" it does not implicate the Fifth Amendment rights of the user of device ... Here the finger is like the key to a strongbox, it is not a communication at all, let alone a testimonial one.' (Gvt. Mem. at 2) (*citing*Commonwealth v. Baust, 89 Va. Cir. 267 (Va.Cir.Ct. 2014)).

The government is generally correct that the production of physical characteristics generally do not raise Fifth Amendment concerns.

* * *

However, courts have raised Fifth Amendment concerns where the production of information is compelled, and the production itself is deemed incriminating.

* * *

This concern of compelled production often arises in the context of grand jury subpoenas, where the production of requested information may have incriminatory value.

* * *

[Producing the Contents of the Phone]

In the instant case, the government argues that the presentation of a fingerprint is not testimonial because under *Doe v. United States*, 487 U.S. 201, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988), '[t]o be testimonial, an act must involve communication and "an accused communication must itself, explicitly or implicitly, relate a factual assertion or disclose information."' (Gvt. Mem. at 2.) Yet, the connection of the fingerprint to the electronic source that may hold contraband (in this case, suspected child pornography) does 'explicitly or implicitly relate a factual assertion or disclose information.'*Doe*, 670 F.3d at 1342. The connection between the fingerprint and Apple's biometric security system, shows a connection with the suspected contraband. By using a finger to unlock a phone's contents, a suspect is *producing* the contents on the phone. With a touch of a finger, a suspect is testifying that he or she has accessed the phone before, at a minimum, to set up the fingerprint password capabilities, and that he or she currently has some level of control over or relatively significant connection to the phone and its contents.

* * *

[The Uniqueness of the Cell Phone]

In fact, the Supreme Court has said '[t]he term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.'*Riley v. California*, ––U.S. ––, 134 S.Ct. 2473, 2489, 189 L.Ed.2d 430 (2014).

[The Fourth and Fifth Amendment Concerns]

The societal concerns of privacy raised in *Riley* provide an important backdrop to the issue presented in the instant case. The *Riley* court recognized that the modern day cell phone, based in part on the personal and intimate information regularly stored on such devices, is subject to higher Fourth Amendment protections than other items that might be found on a person. The considerations informing the Court's Fourth Amendment analysis of a cell phone's role in modern day life, we believe raise Fifth Amendment concerns as well. We do not believe that a simple analogy that equates the limited protection afforded a fingerprint used for identification purposes to forced fingerprinting to unlock an Apple electronic device that potentially contains some of the most intimate details of an individual's life (and potentially provides direct access to contraband) is supported by Fifth Amendment jurisprudence.

[At Least the Government was Candid]

In closing, upon presentation of the warrant application to this Court, the government identified for this Court that the warrant application was seeking the forced fingerprinting discussed herein.

* * *

[The Court is not Saying, "Never"]

This opinion should not be understood to mean that the government's request for forced fingerprinting will always be problematic. *In circumstances where the existence and nature of the electronic information sought is a 'foregone conclusion,' Fifth Amendment jurisprudence tells us that the concerns noted above may be obviated.* Similarly, under Fourth Amendment jurisprudence where there is an individualized showing more firmly establishing a connection between an individual and criminal conduct, the Fourth Amendment concerns raised herein may fall to the wayside. Indeed, after the execution of this warrant, the government may garner additional evidence that addresses both of these concerns such that the government can promptly apply for additional search warrants. We simply are not there yet. (emphasis added)

[My Thoughts]

- After I read the *LA Times* article, I called the lawyer in George Mgdesyan's firm who had represented Bkhchadzhyan in the state case that resulted in his confinement. No Fourth or Fifth Amendment issue was ever raised on his behalf because no additional cases were filed against him.

- Near the end of his opinion in *In re Application for a Search Warrant*, Magistrate Judge Weisman uses the term "*foregone conclusion."* The "*foregone conclusion rule*" was enunciated in *Fisher v. United States,* 425 U.S. 391, 411 (1976) and recently cited in a Sixth Circuit case:

  > Under this rule, the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a 'foregone conclusion' that 'adds little or nothing to the sum total of the Government's information.'For the rule to apply, the Government must be able to 'describe with reasonable particularity' the documents or evidence it seeks to compel.*United States v. Apple MacPro Computer*, 851 F.3d 238 (3d Cir. 2017)

- In *Apple MacPro Computer*, a panel of the United States Court of Appeals [Circuit Judges Jordan, Vanaskie and Nygaard] affirmed the order of United States District Judge L. Felipe Restrepo of the United States District Court for the Eastern District of Pennsylvania holding John Doe in *civil contempt* for his failure to comply with an order of a Magistrate Judge (unnamed in the opinion) "…requiring Doe to produce his iPhone 6 Plus, his MacPro computer, and his two attached external hard drives in a *fully unencrypted state*." (emphasis added).

  After federal agents, pursuant to a search warrant hadseized these devices, Doe voluntarily gave them the password for the iPhone; however, he refused to provide the passwords to decrypt the Apple MacPro computer or the external hard drives. The Magistrate Judge found that he had sufficient facts presented to him to conclude that "…for the purposes of the Fifth Amendment, any testimonial component of the production of decrypted devices added little or nothing to the information already obtained by the Government. The Magistrate Judgedetermined that any testimonial component would be a *foregone conclusion*." He entered his Decryption Order and, when Doe refused to comply, the Government filed a motion requesting that Judge Restrepo order Doe to show cause why he should not be held in civil contempt. After a hearing, he found Doe to be in civil contempt and ordered that he be held in custody *until he complies with the Decryption Order*.

- So, now we have to worry whether federal agentscan compel our clients to use their fingerprints to open their devices and about judges holding our clients in civil contempt for failure to provide these same devices in an unencrypted state. Wow! And we thought that we had interesting search issues before the era of cell phones and computers.