LOS ANGELES
Daily Journal
www.dailyjournal.com
THURSDAY, MAY 26, 2016
PERSPECTIVE

The United States v. iPhone User

By Dan Terzian

Virtually everyone reading this knows that the U.S. Department of Justice recently sought court orders forcing Apple to decrypt iPhones, including one used by a gunman in the San Bernardino shootings last year. But you might not know that the DOJ is seeking the same thing from iPhone users and that such a case is currently pending before the 3rd U.S. Circuit Court of Appeals (*United States v. Apple Macpro Computer*, 15-3537). The DOJ's cases against Apple and against Apple users are similar: Both seek unlocked iPhones.

The similarities end there. Legally, they could not be more different. The cases against Apple pend principally on interpreting a statute, the All Writs Act. Contrast that with the cases against users: They depend on interpreting the Fifth Amendment to the U.S. Constitution.

This distinction is important. Congress ultimately controls issues under the All Writs Act, not the courts. Even if the U.S. Supreme Court one day concludes that the government can force Apple to decrypt phones under the act, Congress can pass a law prohibiting it — or vice versa.

Not so with the Fifth Amendment. Congress does not interpret the Constitution; courts do. And Congress is left with whatever decision the courts give it.

So, who's going to win the Fifth Amendment question, the government or iPhone users?

Part of this question can be answered. The government can legally take your fingerprint without your consent. If that fingerprint unlocks your iPhone, the government wins (it gets your unencrypted data). This answer stems from a long line of authority, beginning with *Schmerber v. California*, 384 U.S. 757 (1966), recognizing that the government can constitutionally compel you to undertake physical acts like fingerprinting. More recently, a Virginia trial court in *Commonwealth v. Baust* applied this authority and held that the government can compel production of the defendant's fingerprint where that fingerprint would be used to attempt accessing the defendant's phone.

New York Times

> Everyone knows the DOJ recently sought court orders forcing Apple to decrypt iPhones. But you might not know that the DOJ is seeking the same thing from iPhone users

But what if your fingerprint doesn't unlock it? The answer's debatable.

Many have argued, and the 11th U.S. Circuit Court of Appeals held as much in *In re Grand Jury Subpoena*, 670 F.3d 1335 (11th Cir. 2012), that the self-incrimination clause of the Fifth Amendment protects against these acts. Under this clause, the government generally (there are exceptions) cannot force you to say anything that might incriminate you. Arguably, being forced to enter a passcode is just that.

Or maybe not. The government can legally force you to undertake physical acts. Plus, under the foregone conclusion exception, the government can force you to produce records the government already knows exist. This exception could arguably apply to producing an unlocked iPhone: If the government knows you own an iPhone and sees that phone's lock screen, it also knows that an unlocked iPhone exists. The Massachusetts Supreme Court in *Commonwealth v. Gelfgatt*, 11 N.E. 3d 605 (Mass. 2014), appears to adopt this view. A per curiam 4th U.S. Circuit Court of Appeals decision may also adopt it, *United States v. Gavegnano*, 305 Fed. App'x 954 (2009), but that court's discussion is too brief to say for sure.

Another consideration is the nature of encrypted data. The Electronic Frontier Foundation has argued that, technically, encrypted files are just "scrambled data" and that "decryption creates new files — it does not simply handle over pre-existing files." Those sympathetic with this view would be more likely to conclude that the Fifth Amendment bars the government from forcing you to decrypt your phone because the Fifth Amendment generally bars the government from forcing you to create evidence. Yet it's unknown how many would agree with this hyper-technical argument. Such an argument would likely fare poorly in civil litigation: "Your Honor, but there are no responsive documents. All we have is scrambled data."

There's no objectively right answer to this debate. Every case deciding the question ultimately hinges on interpreting a Supreme Court decision (*United States v. Hubbell*, 530 U.S. 27 (2000)) on the constitutionality of compelling the production of documents from nearly two decades ago. Much has changed since then. For one, *Hubbell* did not anticipate the rise of digital storage devices capable of essentially creating a safe so secure that not even law enforcement can access its contents. For another, only four justices who decided *Hubbell* remain on the Supreme Court. Who knows how today's Supreme Court would view the question, and there's no definitive answer until the Supreme Court weighs in.

Still, further guidance from the 3rd Circuit can be anticipated.

Dan Terzian *is an attorney in Duane Morris' Los Angeles office. He practices commercial litigation and insurance coverage.*


DAN TERZIAN
Duane Morris