Posted 2/21/16

A DEAD MAN'S TALES

Apple extends posthumous protections to a dead terrorist's cell phone

By Julius (Jay) Wachtel. Here is something that never happened to your blogger during his ATF career:

> Jay and his colleagues pull into Orange U-Store, a garage rental business. They have a Federal search warrant for the unit rented by Billy Badass, who, after a long investigation, was arrested for peddling guns on the street.
>
> Jay approaches the main gate. He flashes his badge. "We've got a warrant for Badass's unit."
>
> Employee leaves, returns with his boss, Mr. Crook.
>
> Mr. Crook examines the warrant, snickers. "Sorry, boys. Can't let you in."
>
> Jay is astounded. He inspects his badge. It's only slightly tarnished. "Whaddaya mean...?"
>
> Mr. Crook sighs. "Look, letting you rummage through his stuff would break the bond between us and our clients, whose privacy we have pledged to protect, now and forever."
>
> Jay reddens. "But...we have a warrant! According to the Fourth Amendment..."
>
> Mr. Crook smiles impishly. "Orange U-Store treasures its standing in the community. We have real good lawyers, too. Are you aware of our market capitalization?"

Fast-forward to last week. That's when Tim Cook, Apple's COO (Chief Operating Officer, or His Majesty, for short) just said "no." Mr. Cook was responding to the FBI's request, backed by a court order, that Apple help unlock the iPhone used by the late Syed Farook. On December 2, 2015 Farook and his wife, Tashfeen Malik, murdered fourteen persons and wounded twenty at a workplace party in San Bernardino, California, then came out second in a vicious firefight with local cops.

Although the legal and technical aspects of the dispute between Apple and the Feds seem complex, the facts are disarmingly simple. After the shootout, the Feds recovered a cell phone used by Farook. Suspecting that other players might be involved, they want to scan the device for leads. Alas, they don't have Farook's password, and he's in no position to help. To be sure, a supercomputer could feed the phone an endless stream of possible passwords. Apple's new software, though, poses significant obstacles, as it creates delays between login attempts and wipes the unit's memory clean after ten unsuccessful tries.

Apple hasn't always been so recalcitrant. But in 2013, after fielding thousands of requests for cell phone data over the years, it introduced encryption, then upped the ante one year later by making it supposedly impossible for anyone other than a phone's owner to log in. Apple and its defenders scoffed at law

enforcement claims that these measures would benefit terrorists, calling the concerns wildly exaggerated. After all, there are plenty other places where cops can get what they need.

With Apple refusing to voluntarily cooperate, FBI agents turned to the "All Writs Act," a Federal statute that can be used to compel private persons to lend a hand. A magistrate promptly ordered Apple to create software that would allow an unlimited number of passwords to be run through Farook's phone without risk of purging its contents.

Despite the horrifying context of the phone's recovery, and the possibility that crucial leads rest in its memory, Apple demurred. According to its lawyers, the All Writs act is inapplicable. If the Government wants a law that forces technology companies to come to heel, let it pass one. What's more, Apple insists that its position isn't just about the law: it's about *principle*. An open letter, signed by Mr. Cook, argues that prying into the dead man's cell phone would "undermine decades of security advancements that protect our customers — including tens of millions of American citizens — from sophisticated hackers and cybercriminals." In an eloquent doomsday scenario, Apple's kingpin warns that helping the Feds would set a "dangerous precedent" with potentially catastrophic consequences:

> The implications of the government's demands are chilling. If the government can use the All Writs Act to make it easier to unlock your iPhone, it would have the power to reach into anyone's device to capture their data. The government could extend this breach of privacy and demand that Apple build surveillance software to intercept your messages, access your health records or financial data, track your location, or even access your phone's microphone or camera without your knowledge.

According to the Government, it's Apple's concerns that are wildly exaggerated. After all, the Fourth Amendment remains very much in effect. Non-consensual searches still require a warrant based on probable cause, while compelling third parties to release information or cooperate calls for at least a subpoena. No one's insisting that Apple redesign the phones or make its protective measures easier to defeat. Sure, a permanent back door would be nice, but the Fed's bottom line is that Apple help unlock this phone, then keep helping on a case-by-case basis, just like in the good old days.

But the iPhone no longer indisputably rules the roost. Android's big splash made privacy a highly competitive commodity. That, according to the Justice Department, is what really explains Apple's intransigence. It really *is* all about money. Meanwhile the rest of the tech industry remains mum but vigilant. On the one hand, no one wants to be branded as an enabler of crooks and terrorists. On the other, there is great uncertainty about the future. What will happen if Apple wins? If it loses?

> Back in the ATF office, Jay and his colleagues finish cataloguing dozens of guns found in Billy Badass's storage unit.
>
> Jay turns to Tom. "Did you see Mr. Crook's eyes bug out when you demonstrated our 'key'?"
>
> Tom fondles the group's treasured sledgehammer. "Well, I wasn't going to *beg* him to unlock the gate."
>
> Chuck walks in. He hands Jay a thick envelope. "We subpoenaed Billy Badass's bank statement."

Jay examines the contents, frowns. “It’s gibberish. Everything’s encrypted. Ever since Apple got away with it, everyone’s been demanding complete privacy about everything. Can you imagine working tax cases? Frauds?”

Tom returns the sledgehammer to the vault. “Good thing they can’t encrypt garages.”