USDOJ: MAKE APPLE FIX THEIR 'BRAND MARKETING STRATEGY' FOR OUR NEEDS

(Note: I drafted the following piece Friday after the USDOJ filed its latest motion, but before the latest revelation of law enforcement's handling of the iPhone at the heart of the case. I've added an additional remark set off with emphasis after the disclosure. And now this afternoon's new development? I can't with this stuff. ~smh~)

You may imagine me agog after reading the Department of Justice's motion filed today in the case of San Bernardino shooter Syed Farook's iPhone. USDOJ believes Apple's repudiation of its demands to write code in order to allow USDOJ to access the phone's content by brute forcing the pin "to be based on its concern for its business model and public brand marketing strategy …"

Does the USDOJ understand what a smartphone is, and how it differs from a plain old telephone or even a vanilla cellphone? Are they just screwing with us, or do they simply not understand that smartphones aren't just communications tools?

<<— For example, this device is designed to contain materials that

are important and valuable to its user, including identity documentation, money and other means of payment, keys to access other devices and locations, possibly papers with important notes.

Imagine the USDOJ insisting the wallet's designer must allocate personnel and resources to redesign and apply a new closure on a single device so that content caught in it will not be destroyed when the closure is opened by USDOJ.

Ridiculous.

.

.

<<— Compare now to this device, designed to contain materials that are important and valuable to its user, including identity documentation, money and other means of payment, keys to access other devices and locations, possibly papers with important notes. Only this device may contain entire libraries and businesses.

Imagine the USDOJ insisting the device's designer must allocate personnel and resources to redesign and apply a new closure on a single device so that content caught in it will not be destroyed when the closure is opened by USDOJ.

Users rely on this device's inherent closure

integrity to secure its contents. This is not merely a “public brand strategy” – it is the essence of the device’s utility, its fundamental nature. The only thing different between these devices is communications capability in the latter, not the former. But users rely on the content of messages to be treated like the content of notes one might put in their wallet or purse – private and secure. Users seeking wallets and smartphones don’t buy them because they are insecure. Smartphone buyers aren’t shelling out $20 for a wallet, and they’re not buying just a communications device. They’re spending hundreds of dollars buying a digital portmanteau to replace their wallet/purse containing their laptop/books/files/photo album/audio player/more. It must be secure for that reason. The investment of time and money reflects this.

Which is why it seems to me – and I am not a lawyer – the government’s demands on Apple to allocate business resources to create an insecurity in a device designed to be secure is unreasonable, even if the insecurity demanded will be used one time as the USDOJ claims.

Worse, this demand by USDOJ is an attempt to remedy a case of bad device management. The specific iPhone in question, used by Syed Farook, was issued by his employer – San Bernardino County. Why didn’t the county issue devices with an administrative override? It’s like issuing a company car but not retaining a spare set of keys if the employee was suddenly terminated. Why should Apple undermine the inherent integrity of its product to resolve a poor case of asset management?

EDIT: And why should Apple invest private resources into compelled speech as software to rectify a screw-up on the part of San Bernardino County and the USDOJ in their inept handling of the single iPhone in question once the device had been retrieved from the suspect?

It doesn’t matter if, as USDOJ swears, this compelled reverse engineering is written and

applied only once. That it would have been done at all establishes a precedent, allowing the U.S. government (and others!) a foothold to demand companies allocate resources to service the government, while undermining the inherent integrity of their products.

What might this do over the long run to Apple's investment in Apple Pay — literally a wallet-alternative payment technology based on iPhone?

A wallet that retains its contents isn't just "brand marketing strategy." It's the innate purpose of a wallet — and the same with devices we now use as digital wallets.

There is another larger conversation we must have about the evolution of technology and the inability of our laws to keep apace. Consider Maryland Attorney General Brian E. Frosh's recent brief in which he maintained persons carrying a cellphone into a store had no expectation of privacy, "because [the suspect Andrews] chose to keep his cell phone on, he was voluntarily sharing the location of his cell phone with third parties." But cellphones — more specifically, smartphones — are the convergence of our entire desks. We do not expect by keeping them turned on that we have given third parties entrée to our desks unless we have pointedly been asked and given permission. People don't just walk around holding their wallets and backpacks open for inspection by anyone who chooses to snoop.

But smartphones are the convergence of our entire desks. We do not expect by keeping them turned on that we have given third parties entrée to our desks unless we have pointedly been asked and given permission. People don't just walk around holding their wallets and backpacks open for inspection by anyone who chooses to snoop.

Unfortunately, we the people have not negotiated our expectations by way of legislation. Law enforcement and the military both are operating in the gap we've left in our social contract,

a hole where our expectations have not been established. Are we suffering from future shock about the technology we expect and use? More than likely, and our legal system is slower than we are, suffering even more so. But because no law clearly tells them, "This is a personal desk with access to remote files – both node ends and the transmission between are private," law enforcement and the military will simply assume they can ask anything they want.

This includes demanding a smartphone manufacture to create an insecurity in digital wallet technology.

_____

Here are a few articles related to the USDOJ's demand on Apple I find particularly interesting:

- Preliminary thoughts on the Apple iPhone order in the San Bernardino case (Part 1) (Orin Kerr, Volokh Conspiracy-WaPo)
- Preliminary thoughts on the Apple iPhone order in the San Bernardino case: Part 2, the All Writs Act (Orin Kerr, Volokh Conspiracy-WaPo)
- Apple, the FBI, iPhones, and the Extended Mind Hypothesis (Gordon Hull, New Apps Blog)
- Not a Slippery Slope, but a Jump of the Cliff (Nicholas Weaver, Lawfare)
- Can the Government Compel Apple to Speak? (Andrew Keane Woods, Lawfare)
- Apple, the FBI, and the San Bernadino iPhone (Dan Wallach, Freedom to Tinker)

- Why Tim Cook is right to call court-ordered iPhone hack a “backdoor” (Dan Goodin, Ars Technica)
- [Update from emptywheel] Why This iPhone? (me! Slate)

(*Disclosure: I own shares of AAPL. Adder: IMO, the embedded video is already anachronistic, behind technological evolution. Many of us, including myself, do most of their work on smartphones/phablets/tablets.*)