LAW ENFORCEMENT'S APPLE SECURITY HYSTERIA: ABOUT BORDER SEARCHES?

As I noted the other day, Apple just r olled out — and Google plans to match with its next Android release — passcode protected encryption for its cell phone handsets.

Last night WSJ had a story quoting some fairly hysterical law enforcement types complaining mightily not just that Apple is offering its customers security, but that it is a marketing feature.

> Last week's announcements surprised senior federal law-enforcement officials, some of whom described it as the most alarming consequence to date of the frayed relationship between the federal government and the tech industry since the Snowden revelations prompted companies to address customers' concerns that the firms were letting—or helping—the government snoop on their private information.
>
> Senior U.S. law-enforcement officials are still weighing how forcefully to respond, according to several people involved in the discussions, and debating how directly they want to

> challenge Apple and Google.
>
> One Justice Department official said that if the new systems work as advertised, they will make it harder, if not impossible, to solve some cases. Another said the companies have promised customers “the equivalent of a house that can’t be searched, or a car trunk that could never be opened.”
>
> Andrew Weissmann, a former Federal Bureau of Investigation general counsel, called Apple’s announcement outrageous, because even a judge’s decision that there is probable cause to suspect a crime has been committed won’t get Apple to help retrieve potential evidence. Apple is “announcing to criminals, ‘use this,’ ” he said. “You could have people who are defrauded, threatened, or even at the extreme, terrorists using it.”

I think the outrage about the stated case – that law enforcement will not longer be able to have Apple unlock a phone with a warrant – is overblown. As Micah Lee points out, the same data will likely be available on Apple’s Cloud.

> But despite these nods to privacy-conscious consumers, Apple still strongly encourages all its users to sign up for and use iCloud, the internet syncing and storage service where Apple has the capability to unlock key data like backups, documents, contacts, and calendar information in response to a government demand. iCloud is also used to sync photos, as a slew of celebrities learned in recent weeks when hackers reaped nude photos from the Apple service. (Celebrity iCloud accounts were compromised when hackers answered security questions correctly or tricked victims into giving up their credentials via “phishing” links, Cook has said.)

And the stuff that won't be on Apple's Cloud will largely be available from a user's phone provider — AT&T and Verizon will have call records and texts, for example. So one effect of this will be to put warrant decisions into a review process more likely to be scrutinized (though not in the case of AT&T, which has consistently proven all to happy to share data with the Feds).

Which is why I think the hysteria is either overblown or is about something else.

It may be that this prevents NSA from getting into handsets via some means we don't understand. Matthew Green lays out how this change will bring real security improvement to your phone from all matter of hackers.

But the most immediate impact of this, I suspect, will be seen at borders — or rather, the government's expansive 100 mile "border zone," which incorporates roughly two-thirds of the country's population. At "borders" law enforcement works under a warrant exception that permits them to search devices — including cell phones — without a warrant, or even any articulable suspicion.

And while it is the case that really aggressive security wonks can and do encrypt their phones now, it is not the default. Which means most people who cross an international border — or get stopped by some authority in that border zone — have their phone contents readily available to those authorities to search. Authorities routinely use their expanded border authority to obtain precisely the kinds of things at issue here, without any suspicion. The terrorist watchlist guidelines (see page 68), for example, note that border encounters may provide evidence from "electronic media/devices observed or copied," including cell phones.

In 2011, DHS whipped out similarly hysterical language about what horribles actually requiring suspicion before searching a device might bring about.

> [A]dding a heightened [suspicion-based] threshold requirement could be operationally harmful without concomitant civil rights/civil liberties benefit. First, commonplace decisions to search electronic devices might be opened to litigation challenging the reasons for the search. In addition to interfering with a carefully constructed border security system, the litigation could directly undermine national security by requiring the government to produce sensitive investigative and national security information to justify some of the most critical searches. Even a policy change entirely unenforceable by courts might be problematic; we have been presented with some noteworthy CBP and ICE success stories based on hard-to-articulate intuitions or hunches based on officer experience and judgment. Under a reasonable suspicion requirement, officers might hesitate to search an individual's device without the presence of articulable factors capable of being formally defended, despite having an intuition or hunch based on experience that justified a search.

That is, DHS thinks it should be able to continue to search your phone at the border, because if it had to provide a rationale — say, to get a warrant — it might have to disclose the dodgy watchlisting policies that it uses to pick whose devices to search without any cause.

In other words, I'm arguing that the most immediate impact of this will be to lessen the availability of data increasingly obtained without a warrant, and given that the alternate means — administrative orders and warrants — require actual legal process, may mean these things will not be available at all.

If I'm right, though, that's not a technical impediment. It's a legal one, one which probably

should be in place.

Update: Argh! This is even worse fear-mongering. A former FBI guy says he used intercepted communications to find kidnappers.

> Once we identified potential conspirators, we quickly requested and secured the legal authority to intercept phone calls and text messages on multiple devices.

Then claims losing an entirely unrelated ability to search — for data stored on, and only on, handsets — would have prevented them from finding that kidnap victim.

> Last week, Apple and Android announced that their new operating systemswill be encrypted by default. That means the companies won't be able to unlock phones and iPads to reveal the photos, e-mails and recordings stored within.
>
> It also means law enforcement officials won't be able to look at the range of data stored on the device, even with a court-approved warrant. Had this technology been used by the conspirators in our case, our victim would be dead.

Instead of proving this guy would be dead, the story instead proves that this is not the most pressing information.