

# The Washington Post

## The phone of choice for the pedophile?

By David Post

September 26, 2014

Today's Washington Post has a front page story ("FBI blasts Apple, Google for locking police out of phones") quoting FBI Director James Comey, and other law enforcement officials, criticizing Apple's recent decision (with Google apparently following suit shortly) to use encryption on their new iPhones that makes it impossible for Apple itself to unlock the data stored locally on an iPhone, even in the face of a lawful warrant to do so. ["'Apple will become the phone of choice for the pedophile,' said John J. Escalante, chief of detectives for Chicago's police department."]

Without meaning to interrupt the very interesting conversation that Orin Kerr has begun here on the VC about the wisdom of such a move, and the trade-offs between personal privacy and the needs of law enforcement, I was struck by what Comey said:

"Comey added that FBI officials already have made initial contact with the two companies, which announced their new smartphone encryption initiatives last week. He said he could not understand why companies would "market something expressly to allow people to place themselves beyond the law."

Really? Does he really not understand this?

But even if, more plausibly, it's just a rhetorical device, and he "understands" it perfectly well, why choose to characterize it this way? It's the kind of tone-deafness that helps push a lot of people (myself included) into Apple's corner on this. Many people – including me – pointed out, in the wake of the Snowden revelations and related news over the past couple of years, that the one absolutely certain result of all of the attention being paid to government snooping was going to be the development and widespread deployment of more powerful encryption mechanisms for ordinary folks like you and me to use. It would be nice to think that the FBI Director had some awareness of the general sense of unease that has accompanied these revelations, that he might say something more along the lines of:

"OK, I get it. Law-enforcement and national security operatives may well have overstepped the bounds in recent years, and our citizens are genuinely concerned about the government's ability to peek into the most private corners of their lives. And I get it that while access to that

information may be useful for the purposes of ferreting out evildoers, it has a substantial cost for personal privacy and free expression. We can and should and will deal with that as a society – but that’s not what the Apple move is about. The Apple move is about making information unavailable to law enforcement even when their access has been authorized by a judicially-supervised warrant . . . a very different thing. . . ” [The sort of argument that Orin is quoted as making in the article].

If our highest law-enforcement officials still don’t get it – well, that’s precisely what makes us so nervous. And that helps explain why Apple – which, incidentally, has shown itself in the past to be pretty good at judging the market and figuring out what people care about in their devices — might find it profitable to do what it did.

*David Post taught intellectual property and Internet law at Georgetown Law Center and Temple University Law School until his recent retirement. He is the author of "In Search of Jeffersons Moose: Notes on the State of Cyberspace" (Oxford, 2009), a Fellow at the Center for Democracy and Technology, and an Adjunct Scholar at the Cato Institute.*