JIM COMEY'S CONFUSED DEFENSE OF FRONT DOOR BACK DOORS AND STORAGE INTERCEPTS

I said somewhere that those wailing about Apple's new default crypto in its handsets are either lying or are confused about the difference between a phone service and a storage device.

For the moment, I'm going to put FBI Director Jim Comey in the latter category. I'm going to do so, first, because at his Brookings talk he corrected his false statement — which I had pointed out — on 60 Minutes (what he calls insufficiently lawyered) that the FBI cannot get content without an order. Though while Comey admitted that FBI can read content it has collected incidentally, he made another misleading statement. He said FBI does so during "investigations. They also do so during "assessments," which don't require anywhere near the same standard of evidence or oversight to do.

I'm also going to assume Comey is having service/device confusion because that kind of confusion permeated his presentation more generally.

There was the confusion exhibited when he tried to suggest a "back door" into a device wasn't one if FBI simply called it a "front door."

> We aren't seeking a back-door approach. We want to use the front door, with clarity and transparency, and with clear guidance provided by law. We are completely comfortable with court orders and legal process—front doors that provide the evidence and information we need to investigate crime and prevent terrorist attacks.

And more specifically, when Comey called for rewriting CALEA, he called for something that would affect only a tiny bit of what Apple had made unavailable by encrypting its phones.

> Current law governing the interception of communications requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance. But that law, the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago—a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide *lawful intercept* capabilities to law enforcement. [my emphasis]

As I have noted, the main thing that will become unavailable under Apple's new operating system is iMessage chats if the users are not using default iCloud back-ups (which would otherwise keep a copy of the chat).

But the rest of it — all the data that will be stored only on an iPhone if people opt out of Apple's default iCloud backups — will be unaffected if what Comey is planning to do is require intercept ability for every message sent.

Now consider the 5 examples Comey uses to claim FBI needs this. I'll return to these later, but in almost all cases, Comey seems to be overselling his case.

First, there's the case of two phones with content on them.

> In Louisiana, a known sex offender posed as a teenage girl to entice a 12-year-old boy to sneak out of his house to meet the supposed young girl. This predator, posing as a taxi driver,

> murdered the young boy, and tried to alter and delete evidence on both his and the victim's cell phones to cover up his crime. Both phones were instrumental in showing that the suspect enticed this child into his taxi. He was sentenced to death in April of this year.

On first glance this sounds like a case where the phones were needed. But assuming this is the case in question, it appears wrong. The culprit, Brian Horn, was IDed by multiple witnesses as being in the neighborhood, and evidence led to his cab. There was DNA evidence. And Horn and his victim had exchange texts. Presumably, records of those texts, and quite possibly the actual content, were available at the provider.

Then there's another texting case.

> In Los Angeles, police investigated the death of a 2-year-old girl from blunt force trauma to her head. There were no witnesses. Text messages from the parents' cell phones to one another, and to their family members, proved the mother caused this young girl's death, and that the father knew what was happening and failed to stop it.
>
> Text messages also proved that the defendants failed to seek medical attention for hours while their daughter convulsed in her crib. They even went so far as to paint her tiny body with blue paint—to cover her bruises—before calling 911. Confronted with this evidence, both parents pled guilty.

This seems to be another case where the texts were probably available in other places, especially given how many people received them.

Then there's another texting story — this is the only one where Comey mentioned warrants, and therefore the only real parallel to what he's pitching.

> In Kansas City, the DEA investigated a drug trafficking organization tied to heroin distribution, homicides, and robberies. The DEA obtained search warrants for several phones used by the group. Text messages found on the phones outlined the group's distribution chain and tied the group to a supply of lethal heroin that had caused 12 overdoses—and five deaths—including several high school students.

Again, these texts were likely available with the providers.

Then Comey lists a case where the culprits were first found with a traffic camera.

> In Sacramento, a young couple and their four dogs were walking down the street at night when a car ran a red light and struck them—killing their four dogs, severing the young man's leg, and leaving the young woman in critical condition. The driver left the scene, and the young man died days later.
>
> Using "red light cameras" near the scene of the accident, the California Highway Patrol identified and arrested a suspect and seized his smartphone. GPS data on his phone placed the suspect at the scene of the accident, and revealed that he had fled California shortly thereafter. He was convicted of second-degree murder and is serving a sentence of 25 years to life.

It uses GPS data, which would surely have been available from the provider. So traffic camera, GPS. Seriously, FBI, do you think this makes your case?

Perhaps Comey's only convincing example involves exoneration involving a video — though that too would have been available elsewhere on Apple's default settings.

> The evidence we find also helps exonerate innocent people. In Kansas, data from a cell phone was used to prove the innocence of several teens accused of rape. Without access to this phone, or the ability to recover a deleted video, several innocent young men could have been wrongly convicted.

Again, given Apple's default settings, this video would be available on iCloud. But if it was only available on the phone, and it was the only thing that exonerated the men, then it would count.

Update: I'm not sure, but this sounds like the Daisy Coleman case, which was outside Kansas City, MO, but did involve a phone video that (at least as far as I know) was never recovered. I don't think the video ever was found. The guy she accused of raping her plead guilty to misdemeanor child endangerment — he dumped her unconscious in freezing weather outside her house.

I will keep checking into these, but none of these are definite cases. All of this evidence would normally, given default settings, be available from providers. Much of it would be available on phones of people besides the culprit. In the one easily identifiable case, there was a ton of other evidence. In two of these cases, the evidence was important in getting a guilty plea, not in solving the crime.

But underlying it all is the key point: Phones are storage devices, but they are primarily communication devices, and even as storage devices the default is that they're just a localized copy of data also stored elsewhere. That means it is very rare that evidence is only available on a phone. Which means it is rare that such evidence will only be available in storage and not via intercept or remote storage.