WHY ISN'T FBI INVESTIGATING THE HACKERS WHO BROKE INTO GOOGLE'S CABLES?

At his Brookings event yesterday, Jim Comey claimed that there is a misperception, in the wake of the Snowden releases, about how much data the government obtains.

> In the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals.
>
> [snip]
>
> It frustrates me, because I want people to understand that law enforcement needs to be able to access communications and information to bring people to justice. We do so pursuant to the rule of law, with clear guidance and strict oversight.

He goes onto pretend that Apple and Google are default encrypting their phone solely as a marketing gimmick, some arbitrary thing crazy users want.

> Both companies are run by good people, responding to what they perceive is a market demand. But the place they are leading us is one we shouldn't go to without careful thought and debate as a country.

> [snip]
>
> Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection. It's the equivalent of a closet that can't be opened. A safe that can't be cracked. And my question is, at what cost?

He ends with a plea that "our private sector partners … consider changing course."

> But we have to find a way to help these companies understand what we need, why we need it, and how they can help, while still protecting privacy rights and providing network security and innovation. We need our private sector partners to take a step back, to pause, and to consider changing course.

There's something missing from Comey's tale.

An explanation of why the FBI has not pursued the sophisticated criminals who stole Google's data overseas.

At a recent event with Ron Wyden, the Senator asked Schmidt to weigh in on the phone encryption "kerfuffle." And Schmidt was quite clear: the reason Google and Apple are doing this is because the NSA's partners in the UK stole their data, even while they had access to it via PRISM.

> The people who are criticizing this should have expected this. After Google was attacked by the British version of the NSA, we were annoyed and so we put end-to-end encryption at rest, as well as through our systems, making it essentially impossible for interlopers — of any kind — to get that information.

Schmidt describes the default encryption on the iPhone, notes that it has been available for the last 3 years on Android phones, and will soon be standard, just like it is on iPhone.

> Law enforcement has many many ways of getting information that they need to provide this without having to do it without court orders and with the possible snooping conversation. The problem when they do it randomly as opposed to through a judicial process is it erodes user trust.

If everything Comey said were true, if this were only about law enforcement getting data with warrants, Apple — and Google especially — might not have offered their customers the privacy they deserved. But it turns out Comey's fellow intelligence agency decided to just go take what they wanted.

And FBI did nothing to solve that terrific hack and theft of data.

I guess FBI isn't as interested in rule of law as Comey says.