

JIM COMEY MAY NOT BE A MANIAC, BUT HE HAS A POOR UNDERSTANDING OF EVIDENCE

Apparently, Jim Comey wasn't happy with his stenographer, Ben Wittes. After having Ben write up Comey's concerns on encryption last week, Comey has written his own explanation of his concerns about encryption at Ben's blog.

Here are the 3 key paragraphs.

2. There are many benefits to this. Universal strong encryption will protect all of us—our innovation, our private thoughts, and so many other things of value—from thieves of all kinds. We will all have lock-boxes in our lives that only we can open and in which we can store all that is valuable to us. There are lots of good things about this.

3. There are many costs to this. Public safety in the United States has relied for a couple centuries on the ability of the government, with predication, to obtain permission from a court to access the “papers and effects” and communications of Americans. The Fourth Amendment reflects a trade-off inherent in ordered liberty: To protect the public, the government sometimes needs to be able to see an individual's stuff, but only under appropriate circumstances and with appropriate oversight.

4. These two things are in tension in many contexts. When the government's ability—with appropriate predication and court oversight—to see an individual's stuff goes away, it will affect public

safety. That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment. But the tension could as well be illustrated in criminal investigations all over the country. There is simply no doubt that bad people can communicate with impunity in a world of universal strong encryption.

Comey admits encryption lets people lock stuff away from criminals (and supports innovation), and admits “there are lots of good things about this.” He then introduces “costs,” without enumerating them. In a paragraph purportedly explaining how the “good things” and “costs” are in tension, he raises the ISIL threat as well as – as an afterthought – “criminal investigations all over the country.”

Without providing any evidence about that tension.

As I have noted, the recent wiretap report raises real questions, at least about the “criminal investigations all over the country,” which in fact are not being thwarted. On that ledger, at least, there is no question: the “good things” (AKA, benefits) are huge, especially with the million or so iPhones that get stolen every year, and the “costs” are negligible, just a few wiretaps law enforcement can’t break.

I conceded we can’t make the same conclusions about FISA orders – or the FBI generally – because Comey’s agency’s record keeping is so bad (which is consistent with all the rest of its record-keeping). It may well be that we’re

not able to access ISIL communications with US recruits because of encryption, but simply invoking the existence of ISIL using end-to-end encrypted mobile messaging apps is not evidence (especially because so much evidence indicates that sloppy end-user behavior makes it possible for FBI to crack this).

Especially after the FBI's 0-for-40 record about making claims about terrorists since 9/11.

It may be that the FBI is facing increasing problems tracking ISIL. It may even be – though I'm skeptical – that those problems would outweigh the value of making stealing iPhones less useful.

But even as he calls for a real debate, Comey offers not one bit of real evidence to counter the crappy FBI reporting in the official reports to suggest this is not more FBI fearmongering.