FBI Director Comey's false dilemma—"ban encryption or accept terrorism"

July 8 2015, by David Glance

James Comey, Director of the FBI is the latest to add his voice to the call for a ban on the use strong encryption. In a blog post, Comey outlines the potential costs to public safety that come with security services not being able to intercept communications. In particular, he uses the threat of ISIL (ISIS) recruiting "troubled" US citizens and convincing them, over encrypted messaging apps, to "kill people".

Comey's concerns about communications "going dark" or being unavailable to intercept by law enforcement organisations come after UK Prime Minister David Cameron also called for a ban of encryption in the UK for the same reasons.

This is not the first time that either Comey or Cameron have raised concerns over tech companies moving to improve the security and privacy features of their software. Indeed, as security specialist Bruce Schneier writes much of this rhetoric was used in the 1990's when the US gradually lifted controls on the export of encryption outside of the US and the White House dropped plans for the introduction of the "Clipper Chip". The Clipper Chip was a device that would provide encryption in telephones but would also allow the government access to the keys to un-encrypt communication at any time.

Then, as now, not allowing unfettered surveillance would result in security services not being able to deal with "paedophiles, kidnappers, drug dealers and terrorists". Since then however, it has not been encryption that has stopped security services preventing terrorist attacks

but the simple enormity of the task of producing reliable, fully cross-referenced, intelligence in sufficient time to actually do anything about it. There just isn't any evidence that global surveillance has led us to being any better at finding or preventing terrorist attacks.

What has increased however is the threat to nations from an increase in cyber attacks on commercial and national infrastructure.

One has to assume that even David Cameron would want as much security as possible applied to the UK's critical infrastructure such as its water and electricity supply, its defense systems and its financial markets.

Comey and Cameron would also presumably not want back doors put in systems that foreign and hostile governments or mere cyber-criminals could exploit to gain a strategic or even tactical advantage over their respective countries. In fact, it is not outside of the realm of possibility to suppose that terrorist groups could discover these secret entrances to communications and exploit them for their own ends.

It seems equally unlikely that either person really believes that adopting strategies of defence only tried (and not succeeded) by countries like Syria, Russia and Iran is any sort of example to aspire to?And finally, and most importantly as many have said already, trying to ban encryption is simply not something that could be achieved in any practical way.

When officials like Comey frame the suggestion of needing to end the use of encryption as a conversation that needs to be held, it is clear that they do not have a clear understanding of what they are suggesting. If we are to have this conversation, both Cameron and Comey could actually talk in tangible terms with specifics about how they would actually achieve what they think they want.

Source: The Conversation