Behind FBI's Data-Access Fight with Apple

FBI Director James Comey gained his reputation for integrity by standing up to George W. Bush's White House on a domestic spying issue but the fight was more tactical than principled, raising doubts about his current dispute with Apple over government accessing encrypted phone data, writes ex-FBI official Coleen Rowley.

By Coleen Rowley

Knowing even a little of James Comey's post 9/11 background, it becomes rather hard to believe the FBI Director is sincerely leveling with the American public in his latest quest to compel Apple (and other encrypted communication companies) to create a mechanism for government access, that he is solely motivated by his desire to "look the (San Bernardino) survivors in the eye" and tell them the FBI has followed up on all investigative leads.

It should be recalled that Comey gained his reputation for legal integrity based on one dramatic night (in March 2004), during his 20 months as deputy attorney general, confronting Bush Administration officials in Attorney General John Ashcroft's hospital room. Even though almost no one understood "what the Ashcroft 'hospital showdown' on NSA spying was all about" until a couple weeks after Comey was confirmed as FBI Director in July 2013 – see this article that seems to finally piece it all together – it was known that no Justice Department official, including Comey, generally opposed the illegal warrantless monitoring program that went into effect just days after the 9/11 attacks.

Except for a few whistleblowers, the only internal debate that developed was ***how*** to do it. In addition to the illegal "Presidential Program" monitoring of Americans, Comey supported and signed off on the George W. Bush Administration's torture tactics as well as years-long indefinite detentions that denied some American citizens their right to counsel and other constitutional rights.

But Comey's reputation as a man of law, albeit mostly false, preceded him. Other than some grilling about the torture he had approved of, almost none of the hard questions I suggested in this *New York Times* opinion piece for Judiciary Committee senators were asked of Comey during his Senate confirmation hearings. Maybe Apple could still ask him some of them!

If the FBI Director is truly concerned about the "proper balance" in upholding the law as well as effectively investigating crimes, reducing terrorism and helping crime victims, how could he let himself fall so far off balance after

9/11? What integrity exists in going along with the Bush Administration when it "went to the (lawless) dark side" and when it ginned up war on Iraq, a country that had nothing to do with the 9/11 attacks and which has only served to increase worldwide terrorism that led to the terrible creation of ISIS, all of which served to inspire the San Bernardino shooters?

Don't Comey and his colleagues who shilled for war on Iraq, who support the other "regime changes" and aerial bombing campaigns targeting Syria, Libya, Yemen, Pakistan and other countries of the Mideast, understand how blowback works?!

I would think it would indeed be hard for any official who went along with the architects of the illegal wars and the Middle East destabilization plans to face the poor victims of the ensuing blowback whether or not able to get into terrorists' phones after an attack.

Maybe most disingenuous of all is Comey's new assertion that he is not trying to set a precedent. Does he not know that the government's "Plan B" secret agenda to create "work-a-rounds" to defeat encryption recently came to light? Does he expect us to believe that he was not part of the secret White House meeting last fall where senior national security officials ordered agencies to find ways to counter encryption software and gain access to the most heavily protected user data on the most secure consumer devices, including Apple Inc.'s?

If it's only a "narrow" legal issue at play, then why has the FBI Director spent so much time lately giving scary speeches that law enforcement is "going dark," arguing that encrypted private communications are inherently dangerous, that the government needs ways to counter such privacy?

The truth is that there is little likelihood, from everything we already know about the San Bernardino couple's lack of actual connectedness to Islamic extremist groups, that the Apple iPhone of one of the San Bernardino shooters holds any real clues to future attacks. Comey is good to mention, in his *Lawfare* piece, this potential for nothing of value residing on this particular Apple phone. Yet he disingenuously claims the legal issue is a narrow one when the only reason the case has been seized upon is due to the public relations impact of the San Bernardino shootings as the best example to open the door.

FBI and Justice Department Dspeakers were previously more honest pointing to the wider danger of child predators, serial killers, members of criminal organizations along with terrorists all potentially able to freely communicate via secure encryption, to justify the need to establish a wider precedent.

Speaking of opening the door to wider applications, we should recall what was

said after National Security Agency whistleblower Edward Snowden's disclosures informed Americans about the massive data collection taking place and after the subsequent discovery that key intelligence officials lied when they tried to justify their illegal monitoring by claiming that the bulk collection of mostly non-relevant data had proven effective in preventing terrorist attacks.

Officials ultimately could only come up with one flimsy example showing how their bulk collection, despite being able to defeat privacy worldwide and despite billions of dollars spent, had detected a taxi driver sending $8,500 in "material support" to Somalia. Some of us have tried for years to refute the notion that adding more hay to the haystack somehow helps to find the needle but nothing has deterred the FBI from its haystack mindset.

It sent a Deputy Assistant Director to inform the Judiciary Committee of just the opposite, that in that one Somalian case, "In order to find the needle, … we needed the haystack." Some Senators then seized upon this upside-down logic to justify the NSA's massive data collection.

So I cannot help be skeptical that, instead of a narrow focus to get phone companies to help the government in discrete terrorism investigations where probable cause exists, it's actually their admitted mindset of wanting to create ever bigger haystacks, by vacuuming up more and more communication data, that fuels the government's drive to defeat communication privacy. In fact it was exactly that mindset behind the extension (beyond any common sense interpretation) of Section 215 of the Patriot Act, which Comey and others supported and helped engineer, just a few months after the famous hospital room standoff.

Although the Patriot Act section on its face permitted only the collection of records deemed "relevant" to an "authorized" national security case, these government officials secretly decided and were able to get the FISA court's secret approval, to stretch that narrow language to mean collection of all phone records, whether relevant or not.

Despite the above reasons for skepticism, I would nonetheless agree that unbreakable encrypted criminal communications do pose serious problems for law enforcement and serious issues for society as a whole. Since he's leading the charge, I only wish the current FBI Director could be more honest about his past and current actions some of which were egregiously illegal and counterproductive, helping increase the level of terrorism in the world.

For James Comey is undoubtedly correct when he writes, "It should be resolved by the American people deciding how we want to govern ourselves in a world we have never seen before. We shouldn't drift to a place – or be pushed to a place by

the loudest voices – because finding the right place, the right balance, will matter to every American for a very long time.”

He should know.

Coleen Rowley is a retired FBI agent and former chief division counsel in Minneapolis. [This item first appeared at HuffingtonPost.]