GlobalResearch
Center for Research on Globalization

“Free Speech” and Privacy Foregone in the UK: Reading Your Text Messages. David Cameron’s Move Against Encryption

By Dr. Binoy Kampmark
Global Research, January 14, 2015

Region: Europe
Theme: Police State & Civil Rights

“With the rapid increase in sophisticated and effective cyber attacks, what we need is more and better security tools, not fewer and weaker ones.” – Lance Cottrell, Chief Scientist at Ntrepid, Jan 14, 2015.

This week, British Prime Minister, David Cameron, decided to throw a confused cat among even more confused pigeons. He made comments suggesting that end-to-end encryption should be a thing of the past, a necessary measure to combat that ever woeful virus many deem terrorism. “Are we going to allow a means of communication between people which even in extremis, with a signed warrant from the Home Secretary personally, that we cannot read?” Naturally for him, the answer was no. “The first duty of any government is to keep our country and our people safe.”

The statements prompted some commentators to wonder what had gotten into Cameron. Certainly, he is moving the gear into electoral mode, with a general poll set for May. And there were the Paris killings, with various decrepit responses from politicians to out bid each other in terms of who could look tough on terrorism. Cameron, evidently, felt he could outdo all of them with a spike of hawkishness. For all of that, Twitter went into apoplectic overdrive, drumming with WebCameronClangers or #CameronCryptoBollox (TechCrunch, Jan 13).

The free speech imperative is aligned with the notions of privacy – these are the Siamese twins of political and social practice in the democratic realm. Central to this is the messaging phenomenon in which encryption is king, be it such services as ChatSecure, Cryptocat, Signal/Redphone, Silent Phone and Silent Text, to name but a few star performers outlined by the EFF (TechCrunch, Jan 13). The British Prime Minister is showing a rather scant knowledge of their workings, not to mention the way technology plays out. Then again, he may simply be playing the cheapest of populist cards.

No matter – the victims of *Charlie Hebdo*, a satirical magazine that should, given the chance, lampoon Cameron for his anti-encryption fantasy, have become the excuses for firm prying from overly sensitive authorities. Be careful what you say, and to whom you say things to, which is, in essence, the fundamental rationale of police state politics.

Various key areas are of importance, and it would seem that the Cameron government is getting busy undermining privacy in each one of them. Home Secretary Theresa May has cobbled a code of practice covering the use of police surveillance powers under the Regulation of Investigatory Powers Act 2000 (RIPA).

The measures contained therein have been deemed inadequate in curbing sweeping powers regarding the access of "phone and email records of professionals such as journalists, lawyers, doctors, MPs and priests who handle privileged, confidential information" (*The Guardian*, Jan 13).

Cameron's anti-encryption agenda conform to that spirit of rampant, and ultimately futile intrusiveness. They prove to be suggestions of an astoundingly counter-productive nature, undermining a constituency vital for his party: the corporate dimension. For a party that fancies The City of London and all that it does – hefty financial transfers, fat loans, the energy of the big wheeling and dealing – removing firm encryption settings will be an unwelcome development.

Companies operating in Britain, using central privacy settings for their services, such as Apple with its iMessage or FaceTime, are less likely to alter their privacy settings to placate a small market when they can move operations elsewhere (*The Guardian*, Jan 13).

"If introduced," Brian Honan, CEO of BH Consulting and Special Advisor to the Europol Cybercrime Centre, "this could have a devastating impact on businesses within the United Kingdom" (Help Net Security, Jan 14). It would effectively encourage "competitive disadvantage against products developed in other countries which can employ more robust encryption."

Honan has another accusation. Rather than forking out for security services, Cameron is choosing an undermining, and lazy route, treating "the symptoms of a problem and not the root causes of that particular problem". Provide, in other words "proper funding, training and resources to law enforcement agencies."

Lance Cottrell, Chief Scientist at Ntrepid, also points out the plan's redundant nature. "Such a proposal is unlikely to have significant impact on the ability of law enforcement or intelligence organisations to track the serious terrorists" (Help Net Security, Jan 14). The reason being that open source encryption tools were plentiful and readily available for all, criminal or otherwise.

Cameron's move, should it materialise, will trickle down. In giving the backdoor keys to government, hacking will be a breeze and distinctly less challenging. Ironically, it will not only make it easier for British security services to access unencrypted communications – it will make it easier for everybody else. Internationally recognised privacy settings, reflected in EU guidelines and those of the domestic Information Commissioner's Office (ICO), risk being violated by companies adopting compromised data protection measures.

"Slow clap for David Cameron," posed former White House employee and current CEO of Digg and Instapaper Andrew McLaughlin, "whose proposal to ban encrypted comms (leaving UK wide open to hacking, spying etc.) is colossally stupid" (Twitter, Jan 13).

The security dimension in a world free of encryption will create an information free-for-all that would strike terror at the heart of any property minded Tory. Not to mention the customers of any communication service.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

---

Articles by: Dr. Binoy Kampmark