Encryption as privacy messiah and public menace: an assessment after the Paris attacks

Maria Helen Murphy, Maynooth University

From the summer of 2013, the Snowden revelations have been hailed as a turning point in the global debate on privacy and surveillance. Following an initial scramble, internet companies were identified as important anti-surveillance allies of privacy advocates. A key area of focus has been the commitment of many internet companies to the protection of strong encryption. While this paper considers the ongoing UK debate concerning the Investigatory Powers Bill, it focuses on the US situation.

In October 2015, the FBI's James Comey went so far as to suggest that the pendulum on privacy issues had "swung too far" against surveillance interests. Earlier that year, Michael Vatis opined that there was "zero chance" of any domestic restrictions on encryption in the US "absent a catastrophic event which clearly could have been stopped if the government had been able to break some encryption." While legislation may not be forthcoming from the fractured United States Congress, the spectre of terrorist use of encryption tools loomed large in the aftermath of the November attacks in Paris. Senate Intelligence Committee Chairman Richard Burr described the attacks as a "wake-up call" and called for a global debate on encrypted networks. Calling the current situation "unacceptable", Senator John McCain argued for the introduction of legislation on the matter.

While anti-encryption rhetoric was rife following the Paris attacks, on investigation, the significance of encryption tools in the organisation of the attacks appeared overstated. Such opportunism is not a new phenomenon. The manner in which the PATRIOT Act was rushed through Congress following the September 11 attacks is often cited as an example of intelligence interests capitalising on "security at all costs" sentiment that strengthens in times of crisis.

This paper considers the shift in the encryption debate following the Paris attacks and assesses the potential directions the encryption discussion may now take. A questioning approach will be adopted and the focus on encryption by intelligence agencies will be examined. Due to the inherent secrecy of surveillance activities and the promise of safety that surveillance offers to a fearful public, the area is ripe for misrepresentation and hidden motives.