Burner phones, not encryption, kept Paris terrorists off the authorities' radar

Glyn Moody

March 21, 2016

New details of the Paris attacks carried out last November reveal that it was the consistent use of prepaid burner phones, not encryption, that helped keep the terrorists off the radar of the intelligence services.

As an article in *The New York Times* reports: "the three teams in Paris were comparatively disciplined. They used only new phones that they would then discard, including several activated minutes before the attacks, or phones seized from their victims."

The article goes on to give more details of how some phones were used only very briefly in the hours leading up to the attacks. For example: "Security camera footage showed Bilal Hadfi, the youngest of the assailants, as he paced outside the stadium, talking on a cellphone. The phone was activated less than an hour before he detonated his vest." The information come from a 55-page report compiled by the French antiterrorism police for France's Interior Ministry.

Outside the Bataclan theatre venue, the investigators found a Samsung phone in a dustbin: "It had a Belgian SIM card that had been in use only since the day before the attack. The phone had called just one other number—belonging to an unidentified user in Belgium."

As police pieced together the movements of the attackers, they found yet more burner phones: "Everywhere they went, the attackers left behind their throwaway phones, including in Bobigny, at a villa rented in the name of Ibrahim Abdeslam. When the brigade charged with sweeping the location arrived, it found two unused cellphones still inside their boxes." At another location used by one of the terrorists, the police found dozens of unused burner phones "still in their wrappers."

As *The New York Times* says, one of the most striking aspects of the phones is that not a single e-mail or online chat message from the attackers was found on them. That seems to be further evidence that they knew such communications were routinely monitored by intelligence agencies. But rather than trying to avoid discovery by using encryption—which would in itself have drawn attention to their accounts—they seem to have stopped using the Internet as a communication channel altogether, and turned to standard cellular network calls on burner phones.

That authorities are only now discovering this fact shows how well the strategy worked.

As Ars has reported, along with other countries the UK government is pushing for ways to circumvent or weaken encryption because it claims strong crypto creates a "safe space" for terrorists. This new information that the Paris attackers did not routinely use encryption, if at all, but turned instead to the tried-and-tested technique of burner phones, undermines the argument that everyone's communications must be weakened in order to tackle terrorism.

The New York Times article suggests that there was some evidence of encryption software being used elsewhere. A witness reported seeing a terrorist with a laptop, and told the investigators that as the computer powered up, "she saw a line of gibberish across the screen: "It was bizarre—he was looking at a bunch of lines, like lines of code. There was no image, no Internet," she said." *The New York Times* writes: "Her description matches the look of certain encryption software, which ISIS claims to have used during the Paris attacks."

But as many were quick to point out online, the witness probably wasn't looking at some encryption software in action, because such systems show the decrypted message, not the encrypted form. The former Ars Technica editor Julian Sanchez wrote on Twitter: "It's suggestive of a verbose boot. Using encryption looks like 'reading a message' because you decrypt it first."

Until we have stronger evidence to the contrary, it seems likely that encryption played little or no part in the Paris terrorist attacks.