THE HILL

Report: Paris attackers relied on disposable phones, not encryption

Cory Bennett

March 21, 2016

The terrorists behind last November's Paris attacks relied on traditional cellular messages on disposable phones — instead of encrypted messaging apps — to help plan their deadly assault, according to a published report.

The details, which ran in *The New York Times* over the weekend, add to the growing debate over how much encryption, if any, the Paris assailants used to hide from authorities in the run-up to the attack, which left 130 people dead.

The Times described the planners as "disciplined" when it came to cellphone use, based on an extensive French police report, interrogation and court documents, and interviews with French officials.

"They used only new phones that they would then discard, including several activated minutes before the attacks, or phones seized from their victims," the newspaper reported.

Days later, when police raided an apartment where the suspected attackers were hiding, authorities found "several dozen boxes of unused cellphones still in their wrappers," The Times said.

Notably, these phones apparently were never used to send encrypted online chats or emails.

"Not a single email or online chat from the attackers has surfaced so far," the Times reported.

The information has been picked up privacy advocates as further evidence that encryption was not the main mechanism that allowed the terrorists to avoid detection for the months leading up to the attack.

But investigators and some U.S. lawmakers believe the opposite. They argue that since intelligence agencies were not able to pick up any of the Paris group's online chatter, it must have been using encryption. That was the conclusion of a French police report obtained by the Times.

Officials think Friday's capture of Salah Abdeslam — believed to be the last surviving participant from the attacks — could help shed light on this matter.

The Paris attacks have been used by policymakers and law enforcement officials as evidence that encryption is making it harder to detect terrorist plots before they can be carried out. On Capitol Hill, legislators are moving forward with a bill that would give authorities guaranteed access to secure data.

But digital rights groups and privacy advocates have accused these lawmakers of fear mongering, arguing there is scant evidence the Paris attackers relied on encryption. They believe robust encryption is necessary to maintain global security and online privacy.

The Times report offered some brief evidence that encryption software was in use on at least one of the attackers' laptops. A witness during the attack recounted seeing one of the terrorists pull out a laptop.

"It was bizarre — he was looking at a bunch of lines, like lines of code. There was no image, no Internet," the witness said.

"Her description matches the look of certain encryption software, which ISIS claims to have used during the Paris attacks," the Times said.

However, tech experts were quick to criticize the connection.

Julian Sanchez, a tech and privacy-focused senior fellow at the Cato Institute, tweeted that the incident is more "suggestive of a verbose boot," which starts up a device in a single-user mode.

"Using encryption looks like 'reading a message' because you decrypt it first," he added