Snowden leak: NSA helped British steal cell phone codes (Update)

February 19 2015, byKen Dilanian

In this June 6, 2013, file photo, a sign stands outside the National Security Administration (NSA) campus in Fort Meade, Md. Britain's electronic spying agency, in cooperation with the NSA, hacked into the networks of a Dutch company to steal codes that allow both governments to seamlessly eavesdrop on mobile phones worldwide, according to the documents given to journalists by Edward Snowden. (AP Photo/Patrick Semansky, File)

Britain's electronic spying agency, in cooperation with the U.S. National Security Agency, hacked into the networks of a Dutch company to steal

codes that allow both governments to seamlessly eavesdrop on mobile phones worldwide, according to the documents given to journalists by Edward Snowden.

A story about the documents posted Thursday on the website The Intercept offered no details on how the intelligence agencies employed the eavesdropping capability—providing no evidence, for example, that they misused it to spy on people who weren't valid intelligence targets. But the surreptitious operation against the world's largest manufacturer of mobile phone data chips is bound to stoke anger around the world. It fuels an impression that the NSA and its British counterpart will do whatever they deem necessary to further their surveillance prowess, even if it means stealing information from law-abiding Western companies.

The targeted company, Netherlands-based Gemalto, makes "subscriber identity modules," or SIM cards, used in mobile phones and credit cards. One of the company's three global headquarters is in Austin, Texas. Its clients include AT&T, T-Mobile, Verizon and Sprint, The Intercept reported.

The Intercept offered no evidence of any eavesdropping against American customers of those providers, and company officials told the website they had no idea their networks had been penetrated. Experts called it a major compromise of mobile phone security.

Gemalto said in a statement Friday it could not immediately confirm the reported hack and "had no prior knowledge that these agencies were conducting this operation." The company said it "will devote all resources necessary to fully investigate" the reported hack.

A spokeswoman for Sprint Nextel said Thursday that her company had no comment on the report, while a spokeswoman for T-Mobile said her company was referring reporters to Gemalto and declined further

comment.

In addition to SIM cards, Gemalto is a leading maker of encryption systems for other business and industrial uses, including electronic payment processing and "smart" key cards that businesses and government agencies use to restrict access to computers or other sensitive facilities. "Their SIM cards would be used by most of the major telecom operators," said Linley Gwennap, principal analyst at the Linley Group, a Silicon Valley tech research firm.

The NSA did not immediately respond to a request for comment. In the past, former agency officials have defended using extra-legal techniques to further surveillance capabilities, saying the U.S. needs to be able to eavesdrop on terrorists and U.S. adversaries who communicate on the same networks as everyone else. The NSA, like the CIA, breaks the espionage and hacking laws of other countries to get information that helps American interests.

Still, the methods in this case may prove controversial, as did earlier Snowden revelations that the NSA was hacking transmissions among Google's data centers. The Intercept reported that British government hackers targeted Gemalto engineers around the world much as the U.S. often accuses Chinese government hackers of targeting Western companies—stealing credentials that got the hackers into the company's networks. Once inside, the British spies stole encryption keys that allow them to decode the data that passes between mobile phones and cell towers. That allows them to ungarble calls, texts or emails intercepted out of the air.

At one point in June 2010, Britain's Government Communications Headquarters, or GCHQ, as its signals intelligence agency is known, intercepted nearly 300,000 keys for mobile phone users in Somalia, The Intercept reported. "Somali providers are not on GCHQ's list of

interest," the document noted, according to the Intercept. "(H)owever, this was usefully shared with NSA."

Earlier in 2010, GCHQ successfully intercepted keys used by wireless network providers in Iran, Afghanistan, Yemen, India, Serbia, Iceland and Tajikistan, according to the documents provided to The Intercept. But the agency noted trouble breaking into Pakistan networks.