Google, Facebook, Twitter bolster digital defenses in wake of NSA revelations

December 17 2013, by Brandon Bailey

Quietly at first, but more vocally in recent months, Google Inc., Facebook Inc. and other leading Internet companies have been beefing up their digital defenses in response to reports that the National Security Agency has tracked online communications without the companies' knowledge or cooperation.

While Google has led the way in encrypting users' data, privacy advocates say recent moves by other companies are long overdue.

And some warn that the companies' efforts may not be a permanent safeguard, as encryption technology continues to evolve.

"Computer security is a very fast-moving field," said Kurt Opsahl of the Electronic Frontier Foundation. "New vulnerabilities get discovered, even as new and better standards get promulgated."

Tech companies initially were circumspect about their encryption efforts in relation to government surveillance, which they viewed as a sensitive topic. Google and Facebook both quietly increased their defenses over the summer, in some cases expediting programs that were already in the works, soon after the first news reports about the NSA's online data-gathering.

But more recently, top executives at Google, Microsoft Corp. and Yahoo Inc. have touted their efforts - in a reflection of both growing outrage over government surveillance and a desire to convince users that the

companies are doing all they can to safeguard information.

"We have tightened the security between all of our operations, and we're working hard to make it tighter," Google Executive Chairman Eric Schmidt said during a recent public appearance in London. "One way to say it is that we're now protected against the Chinese and the NSA."

Google first added standard encryption to its Web-based Gmail service in 2010; over the years, it has added protections for other kinds of files that users send and receive from Google's servers.

But over the summer, the company began expediting a more ambitious plan to add encryption for data sent between computer centers that Google operates around the globe.

Tech companies had assumed the transmissions between their computer centers were safe from interception because they are carried on cables the companies own or lease for exclusive use. But NSA had found a way to tap into those transmissions and similar links between Yahoo's computer centers, according to documents revealed by the Washington Post.

The report outraged many in the tech industry, since it indicated a surveillance that occurred without the companies' knowledge, and went further than the individual data requests that authorities submitted to the companies under national security laws.

Facebook, Twitter Inc., Yahoo and Microsoft have now followed Google in saying they will encrypt links between their computer centers.

The NSA has said it only targets overseas subjects, although critics say it invariably collects data involving many U.S.-based Internet users.

A Facebook spokesman said the company began work on several encryption efforts before the NSA revelations, but the reports "validated our efforts and encouraged us to press forward."

At Yahoo, meanwhile, CEO Marissa Mayer went out of her way to cite reports of NSA surveillance when she announced new encryption programs in mid-November.

Similarly, Twitter cited an Electronic Frontier Foundation report about NSA surveillance when announcing that it is implementing an advanced form of encryption called "forward secrecy." Google, Facebook and Microsoft also are adopting the method, which uses a different digital key to encode each transmission - so even if an outsider manages to obtain one key, it can't be used to decipher other messages.

Privacy advocates praise those efforts, but some say they are overdue. Critics say Yahoo, in particular, has lagged other companies in adopting standard encryption. A Yahoo spokeswoman declined to comment.

Officials at several companies say implementing encryption can be complicated and costly, both in dollars and performance: It can cause slight delays in transmitting a message, which might frustrate users, so it's often phased in gradually as companies work to reduce those delays.

And experts note that encryption can be hacked. That's why most companies are switching from an industry standard known as 1024-bit encryption to one that uses a longer, 2048-bit encryption key, which would require far more time and processing power to decipher.

Encryption doesn't stop authorities from invoking national security laws that allow them to demand data from Internet companies, experts add, but it becomes more difficult to conduct mass surveillance without the companies' cooperation.