The New York Times http://nyti.ms/1k2b8mu

TECHNOLOGY | NYT NOW

Internet Giants Erect Barriers to Spy Agencies

By DAVID E. SANGER and NICOLE PERLROTH JUNE 6, 2014

MOUNTAIN VIEW, Calif. — Just down the road from Google's main campus here, engineers for the company are accelerating what has become the newest arms race in modern technology: They are making it far more difficult — and far more expensive — for the National Security Agency and the intelligence arms of other governments around the world to pierce their systems.

As fast as it can, Google is sealing up cracks in its systems that Edward J. Snowden revealed the N.S.A. had brilliantly exploited. It is encrypting more data as it moves among its servers and helping customers encode their own emails. Facebook, Microsoft and Yahoo are taking similar steps.

After years of cooperating with the government, the immediate goal now is to thwart Washington — as well as Beijing and Moscow. The strategy is also intended to preserve business overseas in places like Brazil and Germany that have threatened to entrust data only to local providers.

Google, for example, is laying its own fiber optic cable under the world's oceans, a project that began as an effort to cut costs and extend its influence, but now has an added purpose: to assure that the company will have more control over the movement of its customer data.

A year after Mr. Snowden's revelations, the era of quiet cooperation is over. Telecommunications companies say they are denying requests to volunteer data not covered by existing law. A.T.&T., Verizon and others say that compared with a year ago, they are far more reluctant to cooperate with the United States government in "gray areas" where there is no explicit requirement for a legal warrant.

But governments are fighting back, harder than ever. The cellphone giant Vodafone reported on Friday that a "small number" of governments around the world have demanded the ability to tap directly into its communication networks, a level of surveillance that elicited outrage from privacy advocates.

Vodafone refused to name the nations on Friday for fear of putting its business and employees at risk there. But in an accounting of the number of legal demands for information that it receives from 14 companies, it noted that some countries did not issue warrants to obtain phone, email or web-searching traffic, because "the relevant agencies and authorities already have permanent access to customer communications via their own direct link."

The company also said it had to acquiesce to some governments' requests for data to comply with national laws. Otherwise, it said, it faced losing its license to operate in certain countries.

Eric Grosse, Google's security chief, suggested in an interview that the N.S.A.'s own behavior invited the new arms race.

"I am willing to help on the purely defensive side of things," he said, referring to Washington's efforts to enlist Silicon Valley in cybersecurity efforts. "But signals intercept is totally off the table," he said, referring to national intelligence gathering.

"No hard feelings, but my job is to make their job hard," he added.

In Washington, officials acknowledge that covert programs are now far harder to execute because American technology companies, fearful of losing international business, are hardening their networks and saying no to requests for the kind of help they once quietly provided.

Robert S. Litt, the general counsel of the Office of the Director of National Intelligence, which oversees all 17 American spy agencies, said on Wednesday that it was "an unquestionable loss for our nation that companies are losing the willingness to cooperate legally and voluntarily" with American spy agencies.

"Just as there are technological gaps, there are legal gaps," he said, speaking at the Wilson Center in Washington, "that leave a lot of gray area"

governing what companies could turn over.

In the past, he said, "we have been very successful" in getting that data. But he acknowledged that for now, those days are over, and he predicted that "sooner or later there will be some intelligence failure and people will wonder why the intelligence agencies were not able to protect the nation."

Companies respond that if that happens, it is the government's own fault and that intelligence agencies, in their quest for broad data collection, have undermined web security for all.

Many point to an episode in 2012, when Russian security researchers uncovered a state espionage tool, Flame, on Iranian computers. Flame, like the Stuxnet worm, is believed to have been produced at least in part by American intelligence agencies. It was created by exploiting a previously unknown flaw in Microsoft's operating systems. Companies argue that others could have later taken advantage of this defect.

Worried that such an episode undercuts confidence in its wares, Microsoft is now fully encrypting all its products, including Hotmail and Outlook.com, by the end of this year with 2,048-bit encryption, a stronger protection that would take a government far longer to crack. The software is protected by encryption both when it is in data centers and when data is being sent over the Internet, said Bradford L. Smith, the company's general counsel.

Mr. Smith also said the company was setting up "transparency centers" abroad so that technical experts of foreign governments could come in and inspect Microsoft's proprietary source code. That will allow foreign governments to check to make sure there are no "back doors" that would permit snooping by United States intelligence agencies. The first such center is being set up in Brussels.

Microsoft has also pushed back harder in court. In a Seattle case, the government issued a "national security letter" to compel Microsoft to turn over data about a customer, along with a gag order to prevent Microsoft from telling the customer it had been compelled to provide its communications to government officials. Microsoft challenged the gag order as violating the First Amendment. The government backed down.

Hardware firms like Cisco, which makes routers and switches, have found their products a frequent subject of Mr. Snowden's disclosures, and their business has declined steadily in places like Asia, Brazil and Europe over the last year. The company is still struggling to convince foreign customers that their networks are safe from hackers — and free of "back doors" installed by the N.S.A. The frustration, companies here say, is that it is nearly impossible to prove that their systems are N.S.A.-proof.

Most American companies said they never knowingly let the N.S.A. weaken their systems, or install back doors. But Mr. Snowden's documents showed how the agency found a way.

In one slide from the disclosures, N.S.A. analysts pointed to a sweet spot inside Google's data centers, where they could catch traffic in unencrypted form. Next to a quickly drawn smiley face, an N.S.A. analyst, referring to an acronym for a common layer of protection, had noted, "SSL added and removed here!"

Google was already suspicious that its internal traffic could be read, and had started a program to encrypt the links among its internal data centers, "the last chink in our armor," Mr. Grosse said. But the slide gave the company proof that it was a regular target of the N.S.A. "It was useful to have proof, in terms of accelerating a project already underway," he said.

Facebook and Yahoo have also been encrypting traffic among their internal servers. And Facebook, Google and Microsoft have been moving to more strongly encrypt consumer traffic with so-called Perfect Forward Secrecy, specifically devised to make it more labor intensive for the N.S.A. or anyone to read stored encrypted communications.

One of the biggest indirect consequences from the Snowden revelations, technology executives say, has been the surge in demands from foreign governments that saw what kind of access to user information the N.S.A. received — voluntarily or surreptitiously. Now they want the same.

At Facebook, Joe Sullivan, the company's chief security officer, said it had been fending off those demands and heightened expectations.

Until last year, technology companies were forbidden from acknowledging demands from the United States government under the

Foreign Intelligence Surveillance Act. But in January, Google, Facebook, Yahoo and Microsoft brokered a deal with the Obama administration to disclose the number of such orders they receive in increments of 1,000.

As part of the agreement, the companies agreed to dismiss their lawsuits before the Foreign Intelligence Surveillance Court.

"We're not running and hiding," Mr. Sullivan said. "We think it should be a transparent process so that people can judge the appropriate ways to handle these kinds of things."

The latest move in the war between intelligence agencies and technology companies arrived this week, in the form of a new Google encryption tool. The company released a user-friendly, email encryption method to replace the clunky and often mistake-prone encryption schemes the N.S.A. has readily exploited.

But the best part of the tool was buried in Google's code, which included a jab at the N.S.A.'s smiley-face slide. The code included the phrase: "ssl-added-and-removed-here-; -)"

Steve Lohr contributed reporting from New York and Mark Scott from London.

A version of this article appears in print on June 7, 2014, on page A1 of the New York edition with the headline: Internet Giants Erect Barriers to Spy Agencies.