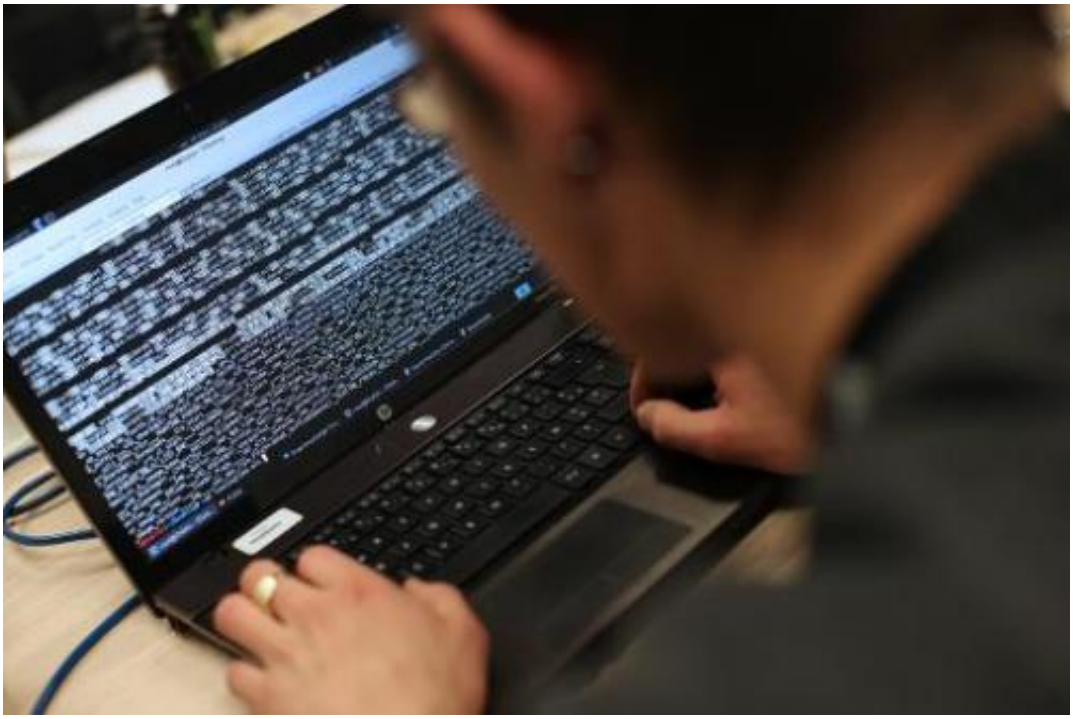
# Encryption companies rise as anxiety over data mounts

March 29 2014, by John Biers



Investors are pumping millions of dollars into encryption as unease about data security drives a rising need for ways to keep unwanted eyes away from personal and corporate information

Investors are pumping millions of dollars into encryption as unease about data security drives a rising need for ways to keep unwanted eyes away from personal and corporate information.

Major data breaches at Target and other retailers that have made data

security a boardroom issue at companies large and small.

And stunning revelations of widespread snooping by US intelligence agencies have also rattled companies and the public.

For venture capital, that has opened up a new area of growth in the tech business.

In February, Google Ventures led a $25.5 million round of venture funding for Atlanta-based Ionic Security, a three-year old company that works in encryption, which scrambles data before it is shipped or stored.

Other encryption companies, including Toronto-based PerspecSys and San Jose, California-based CipherCloud, have announced major fundings.

The funding rush could hearken a "golden age" of encryption, as one expert puts it. But the industry also faces barriers to a tool that until recently was not a hot commodity.

Concerns about encryption range from practical challenges, such as the difficulty users have to search their encoded data, to government opposition towards encryption.

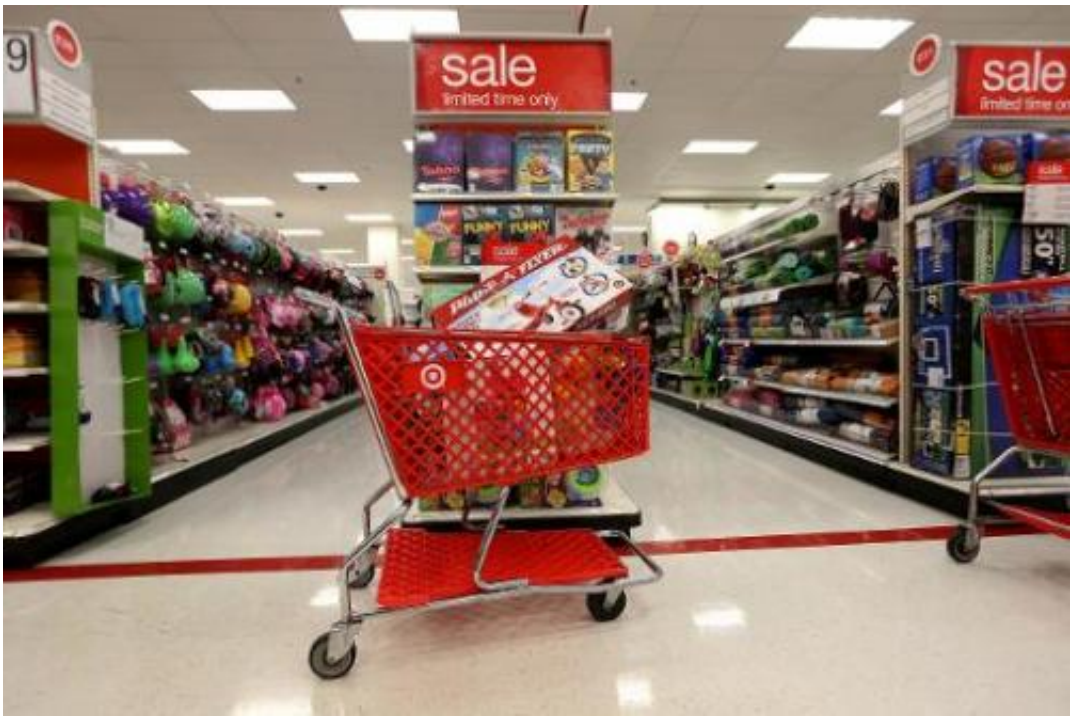
"People are afraid of it because they don't understand it," John Kindervag, a vice president and principal analyst at Forrester Research But he called the wider use of encryption "inevitable, because there's no other way to solve the problem."

Kindervag said the industry is between one and two years away from "some big revolutions" in the field. "It just needs to happen."

But Venky Ganesan, a managing director with venture capital firm

Menlo Ventures, believes major advances are further off.

"Encryption slows down," Ganesan said. "Just imagine if every room in your house was locked and you had to open and close it every time you go in. You would be frustrated."




A shopping cart is seen in a Target store on December 19, 2013 in Miami, Florida

Another problem is "the government is sensitive," said Ganesan.

"They don't want encryption technology to be open so that anybody can use it, because their goal is to make sure they can always get access to the information."

He said governments have frequently insisted that they be given a master

key to decrypt files, Ganesan said.

## Snowden seal of approval

The need for better encryption vaulted to the top of the tech industry's agenda earlier this month by fugitive intelligence contractor Edward Snowden, who last year exposed the massive spying capabilities of the US National Security Agency.

Snowden urged industry leaders to make a "moral commitment" to safeguard customer data by integrating encryption into devices in a user-friendly way.

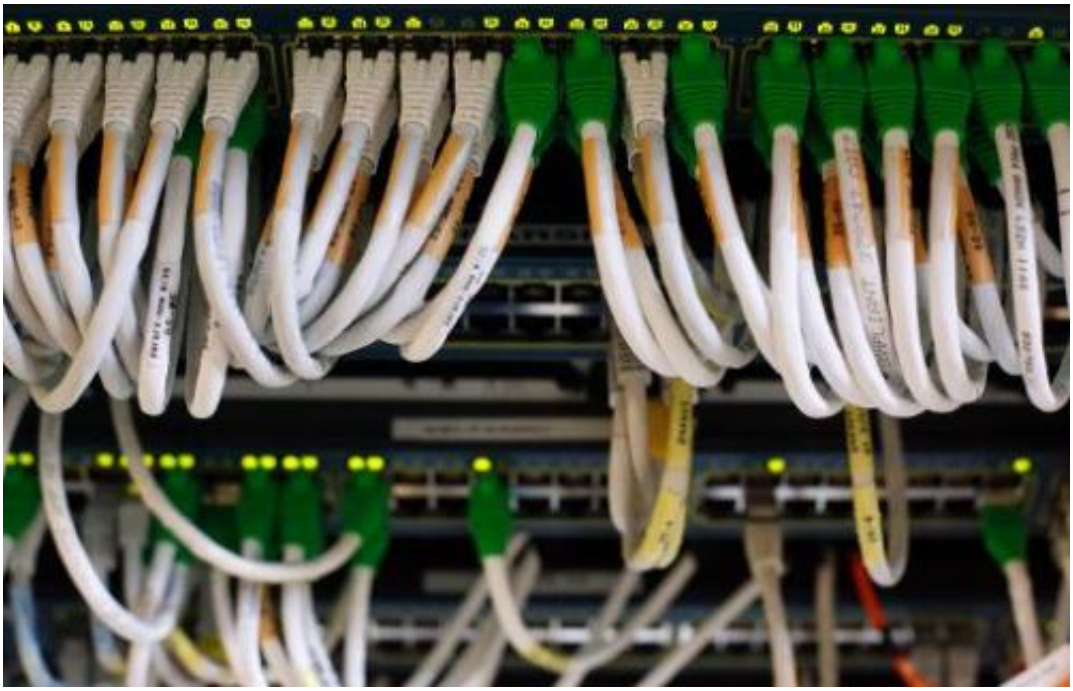
The NSA and foreign intelligence services are "setting fire to the future of the Internet," Snowden said via video from Russia. "You guys are the firefighters and we need you to help fix things."

Recent data security scandals underscore the new vulnerabilities as organizations process unprecedented amounts of data that are analyzed, shipped, stored in "the cloud"—offsite commercial servers—and accessed remotely by mobile technology.

It's a far cry from the days when security focused on safeguarding a stolen laptop.

"It's on every corporation's and every government's mind how they protect their data and their intellectual property," said William Bowmer, a technology stock specialist at Barclays.

Wall Street appears ready to commit more money to security companies as well. Shares of FireEye, which reportedly alerted Target to breaches in its security network even though the company did not take action, have more than tripled from the September 2013 IPO price of $20.



The need for better encryption vaulted to the top of the tech industry's agenda earlier this month by fugitive intelligence contractor Edward Snowden, who last year exposed the massive spying capabilities of the US National Security Agency

Industry insiders see some encryption firms as possibilities for entering the market: Voltage Security, SafeNet, Protegrity and Vormetric Data Security.

Voltage chief executive Sathvik Krishnamurthy described the market for encryption as "thriving and growing" and said the perception of government opposition to encryption is outdated.

Encryption can be integrated into policies that incorporate the lessons of the Snowden revelations with the need to protect national security, Krishnamurthy said.

Spying by authorities "has been going on forever," he said.

"In any society where you think you've had privacy, you've been grossly mistaken. It's just a question of the degree to which you were clueless about Big Brother actually looking at everything you were doing."

He called the NSA's sweep of data "really over the top."

"Did we have to spy on Angel Merkel's emails? No."

But the biggest problem with the NSA program was the lack of disclosure, Krishnamurthy said.

Disclosure by the government of its program "will normalize the line over which we would no longer cross," he said. "If you have to answer for your actions, then you are more likely to be reasonable in your actions."

© 2014 AFP

Citation: Encryption companies rise as anxiety over data mounts (2014, March 29) retrieved 19 April 2024 from https://phys.org/news/2014-03-encryption-companies-anxiety-mounts.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.