

Web's Reach Binds N.S.A. and Silicon Valley Leaders

By James Risen and Nick Wingfield

June 19, 2013

WASHINGTON — When Max Kelly, the chief security officer for Facebook, left the social media company in 2010, he did not go to Google, Twitter or a similar Silicon Valley concern. Instead the man who was responsible for protecting the personal information of Facebook's more than one billion users from outside attacks went to work for another giant institution that manages and analyzes large pools of data: the National Security Agency.

Mr. Kelly's move to the spy agency, which has not previously been reported, underscores the increasingly deep connections between Silicon Valley and the agency and the degree to which they are now in the same business. Both hunt for ways to collect, analyze and exploit large pools of data about millions of Americans.

The only difference is that the N.S.A. does it for intelligence, and Silicon Valley does it to make money.

The disclosure of the spy agency's program called Prism, which is said to collect the e-mails and other Web activity of foreigners using major Internet companies like Google, Yahoo and Facebook, has prompted the companies to deny that the agency has direct access to their computers, even as they acknowledge complying with secret N.S.A. court orders for specific data.

Yet technology experts and former intelligence officials say the convergence between Silicon Valley and the N.S.A. and the rise of data mining — both as an industry and as a crucial intelligence tool — have created a more complex reality.

Silicon Valley has what the spy agency wants: vast amounts of private data and the most sophisticated software available to analyze it. The agency in turn is one of Silicon Valley's largest customers for what is known as data analytics, one of the valley's fastest-growing markets. To get their hands on the latest software technology to manipulate and take advantage of large volumes of data, United States intelligence agencies invest in Silicon Valley start-ups, award classified contracts and recruit technology experts like Mr. Kelly.

“We are all in these Big Data business models,” said Ray Wang, a technology analyst and chief executive of Constellation Research, based in San Francisco. “There are a lot of connections now because the data scientists and the folks who are building these systems have a lot of common interests.”

Although Silicon Valley has sold equipment to the N.S.A. and other intelligence agencies for a generation, the interests of the two began to converge in new ways in the last few years as advances in computer storage technology drastically reduced the costs of storing enormous amounts of data — at the same time that the value of the data for use in consumer marketing began to rise. “These worlds overlap,” said Philipp S. Krüger, chief executive of Explorist, an Internet start-up in New York.

The sums the N.S.A. spends in Silicon Valley are classified, as is the agency’s total budget, which independent analysts say is \$8 billion to \$10 billion a year.

Despite the companies’ assertions that they cooperate with the agency only when legally compelled, current and former industry officials say the companies sometimes secretly put together teams of in-house experts to find ways to cooperate more completely with the N.S.A. and to make their customers’ information more accessible to the agency. The companies do so, the officials say, because they want to control the process themselves. They are also under subtle but powerful pressure from the N.S.A. to make access easier.

Skype, the Internet-based calling service, began its own secret program, Project Chess, to explore the legal and technical issues in making Skype calls readily available to intelligence agencies and law enforcement officials, according to people briefed on the program who asked not to be named to avoid trouble with the intelligence agencies.



Spy agencies invest in Silicon Valley start-ups, award classified contracts and recruit technology experts like Max Kelly. C-Span

Project Chess, which has never been previously disclosed, was small, limited to fewer than a dozen people inside Skype, and was developed as the company had sometimes contentious talks with the government over legal issues, said one of the people briefed on the project. The project began about five years ago, before most of the company was sold by its parent, eBay, to outside investors in 2009. Microsoft acquired Skype in an \$8.5 billion deal that was completed in October 2011.

A Skype executive denied last year in a blog post that recent changes in the way Skype operated were made at the behest of Microsoft to make snooping easier for law enforcement. It appears, however, that Skype figured out how to cooperate with the intelligence community before Microsoft took over the company, according to documents leaked by Edward J. Snowden, a former contractor for the N.S.A. One of the documents about the Prism program made public by Mr. Snowden says Skype joined Prism on Feb. 6, 2011.

Microsoft executives are no longer willing to affirm statements, made by Skype several years ago, that Skype calls could not be wiretapped. Frank X. Shaw, a Microsoft spokesman, declined to comment.

In its recruiting in Silicon Valley, the N.S.A. sends some of its most senior officials to lure the best of the best. No less than Gen. Keith B. Alexander, the agency's director and the chief of the Pentagon's Cyber Command, showed up at one of the world's largest hacker conferences in Las Vegas last

summer, looking stiff in an uncharacteristic T-shirt and jeans, to give the keynote speech. His main purpose at Defcon, the conference, was to recruit hackers for his spy agency.

N.S.A. badges are often seen on the lapels of officials at other technology and information security conferences. "They're very open about their interest in recruiting from the hacker community," said Jennifer Granick, the director of civil liberties at Stanford Law School's Center for Internet and Society.

But perhaps no one embodies the tightening relationship between the N.S.A. and the valley more than Kenneth A. Minihan.

A career Air Force intelligence officer, Mr. Minihan was the director of the N.S.A. during the Clinton administration until his retirement in the late 1990s, and then he ran the agency's outside professional networking organization. Today he is managing director of Paladin Capital Group, a venture capital firm based in Washington that in part specializes in financing start-ups that offer high-tech solutions for the N.S.A. and other intelligence agencies. In effect, Mr. Minihan is an advanced scout for the N.S.A. as it tries to capitalize on the latest technology to analyze and exploit the vast amounts of data flowing around the world and inside the United States.

The members of Paladin's strategic advisory board include Richard C. Schaeffer Jr., a former N.S.A. executive. While Paladin is a private firm, the American intelligence community has its own in-house venture capital company, In-Q-Tel, financed by the Central Intelligence Agency to invest in high-tech start-ups.

Many software technology firms involved in data analytics are open about their connections to intelligence agencies. Gary King, a co-founder and chief scientist at Crimson Hexagon, a start-up in Boston, said in an interview that he had given talks at C.I.A. headquarters in Langley, Va., about his company's social media analytics tools.

The future holds the prospect of ever greater cooperation between Silicon Valley and the N.S.A. because data storage is expected to increase at an annual compound rate of 53 percent through 2016, according to the International Data Corporation.

"We reached a tipping point, where the value of having user data rose beyond the cost of storing it," said Dan Auerbach, a technology analyst with the Electronic Frontier Foundation, an electronic privacy group in San Francisco. "Now we have an incentive to keep it forever."

Social media sites in the meantime are growing as voluntary data mining operations on a scale that rivals or exceeds anything the government could attempt on its own. "You willingly hand over data to Facebook that you would never give voluntarily to the government," said Bruce Schneier, a technologist and an author.

