國際觀專欄(116) 美國國家安全局的工作

李家同

最近媒體上常常報導美國和很多其它國家對某通訊公司的設備不放心，怕這家公司的設備有後門，而且是和政府有聯絡的，這樣很多資料會被那個國家的政府拿走，我最近又在電視上看到一部有關Snowden的電影，裡面提到美國的國家安全局(National Security Agency，簡稱NSA)，我曾經在美國的首都華盛頓住了很多年，從華盛頓到北部的公路上就會看到NSA的牌子，我從來沒有進去過，可是我在美國常常參加學術會議，當然都要掛名牌，顯示你是在哪一個機構工作的，有一些人的名牌上註明機構是US Government，他們以為如此就可以保密了，其實誰都知道，他們都是NSA的職員。當年偷取美國政府數以億計資料的Snowden就是在NSA工作的。

在2013年，西方媒體忽然報導NSA偷聽資料的事，請看以下英國衛報的報導，衛報是世界上有名的報紙。

**Guardian 7 June**

**NSA scandal: what data is being monitored and how does it work?**

Everything you need to know about data gathering from internet companies by the US National Security Agency   
  
Fri 7 Jun 2013 16.21 BST First published on Fri 7 Jun 2013 16.21 BST

**What is the scandal?**

The US's National Security Agency (NSA), its wiretapping agency, has been monitoring communications between the US and foreign nationals over the internet for a number of years, under a project called Prism. Some of the biggest internet companies, from Apple to Google to Yahoo, are involved. The US government confirmed the existence of the scheme and its application on Thursday night.

**Which companies are in the scheme?**

Microsoft was the first to be included, in September 2007. Yahoo followed in March 2008, Google in January 2009, Facebook in June 2009, Paltalk, a Windows- and mobile-based chat program, in December 2009, YouTube in September 2010, Skype in February 2011 (before its acquisition by Microsoft), AOL in March 2011 and finally Apple in October 2012.

**How long has it been going on?**

The NSA has allegedly had means of monitoring internet communications as far back as Microsoft's Windows 95, the first version of Windows with built-in internet connectivity, in 1995. This specific project appears to have begun with monitoring in September 2007 of user data going to and from Microsoft.

**What data is being monitored?**

Potentially, everything. The PowerPoint slide about Prism says it can collect "email, chat (video, voice), videos, photos, stored data, VoIP [internet phone calls], file transfers, video conferencing, notifications of target activity – logins etc, online social networking details" and another category called "special requests".

**How much does it cost to monitor so much traffic?**

The budget given in the presentation is comparatively tiny – just $20m per year. That has puzzled experts because it's so low.

**How effective has it been?**

Nobody knows. The US government has said that the monitoring schemes it runs are necessary to defend against terrorist threats. But it hasn't cited any threats that were thwarted – unsurprising, given that the scheme has only just become public.

**Isn't it illegal?**

The NSA – and so the US government – has been careful to avoid any suggestion that the monitoring is being carried out indiscriminately on US citizens, because that would potentially breach the fourth amendment of the constitution against "unreasonable search".

But people overseas get no such protections. The question then is whether UK and EU governments knew of the scheme and were compliant – and whether they could stop it even if they wanted to.

**What about "safe harbour" rules for EU data?**

US companies that want to process private data from EU citizens have to promise a "safe harbour" – but crucially the documents do not mention tapping by US law enforcement. And if disputes arise, the rules say: "Claims brought by EU citizens against US organizations will be heard, subject to limited exceptions, in the US." That would probably mean the NSA's licence to spy would trump EU complaints.

**How does it work?**

The NSA isn't saying. Sources in the data-processing business point to a couple of methods. First, lots of data bound for those companies passes over what are called "content delivery networks" (CDNs), which are in effect the backbone of the internet. Companies such as Cisco provide "routers" which direct that traffic. And those can be tapped directly, explains Paolo Vecchi of Omnis Systems, based in Falmer, near Brighton.

"The Communications Assistance for Law Enforcement Act (Calea) passed in 1994 forces all US manufacturers to produce equipment compliant with that law," says Vecchi. "And guess what: Cisco is one of the companies that developed and maintains that architecture." Cisco's own documents explain its Calea compliance.

Second, it would be possible to tap into the routers at US national boundaries (to capture inbound international traffic) and just search for desired traffic there.

"The Prism budget – $20m – is too small for total surveillance," one data industry source told the Guardian. Twitter, which is not mentioned in the Prism slides, generates 5 terabytes of data per day, and is far smaller than any of the other services except Apple. That would mean skyrocketing costs if all the data were stored. "Topsy, which indexes the whole of Twitter, has burned through about $20m in three years, or about $6m a year," the source pointed out. "With Facebook much bigger than Twitter, and the need to run analysts etc, you probably couldn't do the whole lot on $20m."

Instead, the source suggests, "they might have search interfaces (at an administrator level) into things like Facebook, and then when they find something of interest can request a data dump. These localised data dumps are much smaller."

**So the NSA would only need to tap the routers?**

Not quite. Much of the traffic going to the target companies would be encrypted, so even when captured it would look like a stream of digital gibberish. Decrypting it would require the "master keys" held by the companies.

**Did the companies know?**

They say not. Those which have been contacted have all denied knowledge of it: Google, for example, said: "Google does not have a 'back door' for the government to access private user data." An Apple spokesman said: "We have never heard of Prism. We do not provide any government agency with direct access to our servers and any agency requesting customer data must get a court order."

The Washington Post retracted part of its story about Prism in which it said that the companies "knowingly" participated. Instead, it quotes a report which says that "collection managers [could send] content tasking instructions directly to equipment installed at company-controlled locations".

It is ambiguous whether "company" refers to the NSA or the internet companies. But the implication seems to be that the NSA has been running a system that can tap into the internet when it wants.

**How could the companies not know if they had provided master decryption keys?**

They might be required to provide them under US law, but would not be allowed to disclose the fact. That would give the NSA all it needed to monitor communications.

**Is there anything I can do to stop it?**

Lots of internet traffic from the west passes through the US because the destination servers are there, or connect there. Encrypting email using PGP is one possibility, though it is not easy to set up. Systems such as Tor, together with a virtual private network (VPN) connection, can cloak your location, though your identity might still be inferred from the sites you connect to.

各位可以看出這件事情是很複雜的，政府要如此大規模地偷聽，並不容易，因為現在的網際網路裡面牽涉到很多設備以及公司，任何懂得現代化通訊技術的人都知道，要偷聽必須要和公司合作，否則不可能，我們也不太能責怪這些肯默默地和美國政府合作，不合作大概也會製造麻煩。

2013年11月21日，法國外交部長Laurent Fabius召見美國駐法大使Charles Rivkin，向他抗議NSA監聽法國公民，大使保證以後不會再犯。

英國也有一個類似NSA的機構，叫做Government Communications Headquarters (GCHQ)，他們的監聽軟體叫做Tempora。

Snowden在NSA工作過，此人在工作時大量下載NSA的秘密檔案，提供給華盛頓郵報和衛報，他使大家知道很多公司都參加了NSA PRISM，在2013年5月20日他出現在香港，6月公布了他所下載的資料，美國政府當然大怒，要求香港遣返Snowden，被香港政府拒絕，6月21日美國宣布他的護照無效，2天以後，他飛到莫斯科，俄羅斯政府拒絕他入境，理由是他的護照已經無效，他在過境室住了一個月，得到政治庇護，普丁總統宣稱俄羅斯不再准許Snowden公布那些秘密資料，其實普丁當然不會公布那些秘密資料，因為俄羅斯政府擁有這些資料了。

我喜歡看間諜小說，所以對於這件事是很有興趣的，各位如果對現在技術有興趣的話，可以看有關PRISM的網站:

<https://en.wikipedia.org/wiki/Prism>

如果你對Snowden有興趣，可以看這個網站:

<https://en.wikipedia.org/wiki/Edward_Snowden>。

各位可以看出大國都在監聽通訊，我可以大膽的說，世界上沒有安全的通訊，唯一的辦法恐怕就是加密，加密也可能被對方破解，但是破解的時間不會太短，所以至少好一點，主要的是不能用大家熟知的語言通訊，絕對不能用的是英文，因為如果加密的英文被破解了，絕大多數的人都會懂英文的，我建議我們國家用我們原住民的語言，比方說用排灣族或者普悠瑪族的語言通訊，恐怕很少人即使解密了，也很難看得懂。

我一直好奇美國的國家安全局如何會讓Snowden大量下載資料，他下載了幾天幾夜，而國家安全局毫不知情，也讓他帶了資料離開美國，這個安全局安全嗎? 我們大學的資訊中心，如果發現有學生大量下載資料，都會表示關心的，那位安全局的局長不知道後來升官沒有? 我如果是美國總統的話，應該立刻將他開除。

最後，對於通訊的安全，國人一定要以這個技術的眼光來看，因此，就必須冷靜，而且要聽專家的話，否則搞不出所以然來。