

'Prism': A massive internet spying scheme by U.S. government is revealed

Files prove existence of undercover operation codenamed Prism

Sunday 9 June 2013, by [ACKERMAN Spencer](#), [FREEDLAND Jonathan](#), [GREENWALD Glenn](#), [MacASKILL Ewen](#), [ROBERTS Dan](#) (Date first published: 8 June 2013).

Revealed: how U.S. secretly collects private data from AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, Yahoo and YouTube.

Contents

- [NSA Prism program taps in \(...\)](#)
- [Obama hits back at 'leaks \(...\)](#)
- [How America's National Security](#)
- [Pressure on UK government \(...\)](#)
- [U.S. draws up list of foreign](#)
- [Glen Greenwald: They have \(...\)](#)
- [Obama is like Google: a \(...\)](#)

Enclosed below is a dossier of articles and commentaries from the UK *Guardian*. It and the *Washington Post* have published the story of Prism, the top secret internet spying-by-internet program of the U.S. government. See also below another *Guardian* article: 'Obama orders US to draw up overseas target list for cyber-attacks.'

Roger Annis

NSA Prism program taps in to user data of Apple, Google and others

- *Top-secret Prism program claims direct access to servers of firms including Google, Apple and Facebook*
- Companies deny any knowledge of program in operation since 2007

The U.S. National Security Agency has obtained direct access to the systems of Google, Facebook, Apple and other US internet giants, according to a top secret document obtained by the *Guardian*. The NSA access is part of a previously undisclosed program called Prism, which allows officials to collect material including search history, the content of emails, file transfers and live chats, the document says.

The *Guardian* has verified the authenticity of the document, a 41-slide PowerPoint presentation – classified as top secret with no distribution to foreign allies – which was apparently used to train intelligence operatives on the capabilities of the program. The document claims “collection directly from the servers” of major US service providers.

Leaked Prism program is top secret; such a top-level leak is unheard of. Although the presentation claims the program is run with the assistance of the companies, all those who responded to a *Guardian* request for comment on Thursday denied knowledge of any such program.

In a statement, Google said: “Google cares deeply about the security of our users’ data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government ‘back door’ into our systems, but Google does not have a back door for the government to access private user data.”

Several senior tech executives insisted that they had no knowledge of Prism or of any similar scheme. They said they would never have been involved in such a program. “If they are doing this, they are doing it without our knowledge,” one said.

An Apple spokesman said it had “never heard” of Prism.

The NSA access was enabled by changes to US surveillance law introduced under President Bush and renewed under Obama in December 2012.

The program facilitates extensive, in-depth surveillance on live communications and stored information. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.

It also opens the possibility of communications made entirely within the US being collected without warrants.

Disclosure of the Prism program follows a leak to the *Guardian* on Wednesday of a top-secret court order compelling telecoms provider Verizon to turn over the telephone records of millions of US customers.

The participation of the internet companies in Prism will add to the debate, ignited by the Verizon revelation, about the scale of surveillance by the intelligence services. Unlike the collection of those call records, this surveillance can include the content of communications and not just the metadata.

Some of the world’s largest internet brands are claimed to be part of the information-sharing program since its introduction in 2007. Microsoft – which is currently running an advertising campaign with the slogan “Your privacy is our priority” – was the first, with collection beginning in December 2007.

It was followed by Yahoo in 2008; Google, Facebook and PalTalk in 2009; YouTube in 2010; Skype and AOL in 2011; and finally Apple, which joined the program in 2012. The program is continuing to expand, with other providers due to come online.

Collectively, the companies cover the vast majority of online email, search, video and communications networks.

Companies are legally obliged to comply with requests for users’ communications under US law, but the Prism program allows the intelligence services direct access to the companies’ servers. The NSA

document notes the operations have “assistance of communications providers in the US”.

The revelation also supports concerns raised by several US senators during the renewal of the Fisa Amendments Act in December 2012, who warned about the scale of surveillance the law might enable, and shortcomings in the safeguards it introduces.

When the FAA was first enacted, defenders of the statute argued that a significant check on abuse would be the NSA’s inability to obtain electronic communications without the consent of the telecom and internet companies that control the data. But the Prism program renders that consent unnecessary, as it allows the agency to directly and unilaterally seize the communications off the companies’ servers.

The Prism program allows the NSA, the world’s largest surveillance organisation, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.

With this program, the NSA is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on targeted users.

The presentation claims Prism was introduced to overcome what the NSA regarded as shortcomings of Fisa warrants in tracking suspected foreign terrorists. It noted that the US has a “home-field advantage” due to housing much of the internet’s architecture. But the presentation claimed “Fisa constraints restricted our home-field advantage” because Fisa required individual warrants and confirmations that both the sender and receiver of a communication were outside the US.

“Fisa was broken because it provided privacy protections to people who were not entitled to them,” the presentation claimed. “It took a Fisa court order to collect on foreigners overseas who were communicating with other foreigners overseas simply because the government was collecting off a wire in the United States. There were too many email accounts to be practical to seek Fisas for all.”

The new measures introduced in the FAA redefines “electronic surveillance” to exclude anyone “reasonably believed” to be outside the USA – a technical change which reduces the bar to initiating surveillance.

The act also gives the director of national intelligence and the attorney general power to permit obtaining intelligence information, and indemnifies internet companies against any actions arising as a result of co-operating with authorities’ requests.

In short, where previously the NSA needed individual authorisations, and confirmation that all parties were outside the USA, they now need only reasonable suspicion that one of the parties was outside the country at the time of the records were collected by the NSA.

The document also shows the FBI acts as an intermediary between other agencies and the tech companies, and stresses its reliance on the participation of US internet firms, claiming “access is 100% dependent on ISP provisioning”.

In the document, the NSA hails the Prism program as “one of the most valuable, unique and productive accesses for NSA”.

It boasts of what it calls “strong growth” in its use of the Prism program to obtain communications. The document highlights the number of obtained communications increased in 2012 by 248% for Skype – leading the notes to remark there was “exponential growth in Skype reporting; looks like the word is getting out about our capability against Skype”. There was also a 131% increase in requests

for Facebook data, and 63% for Google.

The NSA document indicates that it is planning to add Dropbox as a PRISM provider. The agency also seeks, in its words, to “expand collection services from existing providers”.

The revelations echo fears raised on the Senate floor last year during the expedited debate on the renewal of the FAA powers which underpin the PRISM program, which occurred just days before the act expired.

Senator Christopher Coons of Delaware specifically warned that the secrecy surrounding the various surveillance programs meant there was no way to know if safeguards within the act were working.

“The problem is: we here in the Senate and the citizens we represent don’t know how well any of these safeguards actually work,” he said.

“The law doesn’t forbid purely domestic information from being collected. We know that at least one Fisa court has ruled that the surveillance program violated the law. Why? Those who know can’t say and average Americans can’t know.”

Other senators also raised concerns. Senator Ron Wyden of Oregon attempted, without success, to find out any information on how many phone calls or emails had been intercepted under the program.

When the law was enacted, defenders of the FAA argued that a significant check on abuse would be the NSA’s inability to obtain electronic communications without the consent of the telecom and internet companies that control the data. But the Prism program renders that consent unnecessary, as it allows the agency to directly and unilaterally seize the communications off the companies’ servers.

When the NSA reviews a communication it believes merits further investigation, it issues what it calls a “report”. According to the NSA, “over 2,000 Prism-based reports” are now issued every month. There were 24,005 in 2012, a 27% increase on the previous year.

In total, more than 77,000 intelligence reports have cited the PRISM program.

Jameel Jaffer, director of the ACLU’s Center for Democracy, that it was astonishing the NSA would even ask technology companies to grant direct access to user data.

“It’s shocking enough just that the NSA is asking companies to do this,” he said. “The NSA is part of the military. The military has been granted unprecedented access to civilian communications.

“This is unprecedented militarisation of domestic communications infrastructure. That’s profoundly troubling to anyone who is concerned about that separation.”

A senior administration official said in a statement: “The Guardian and Washington Post articles refer to collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act. This law does not allow the targeting of any US citizen or of any person located within the United States.

“The program is subject to oversight by the Foreign Intelligence Surveillance Court, the Executive Branch, and Congress. It involves extensive procedures, specifically approved by the court, to ensure that only non-US persons outside the US are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about US persons.

"This program was recently reauthorized by Congress after extensive hearings and debate.

"Information collected under this program is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats.

"The Government may only use Section 702 to acquire foreign intelligence information, which is specifically, and narrowly, defined in the Foreign Intelligence Surveillance Act. This requirement applies across the board, regardless of the nationality of the target."

Glenn Greenwald and Ewen MacAskill, *The Guardian*, Friday 7 June 2013

Additional reporting by James Ball and Dominic Rushe

* <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>

Obama hits back at 'leaks and media hype' over surveillance

President is defiant as he welcomes public debate about secret system

Washington-Barack Obama struck a defiant stance yesterday in the face of revelations of widespread surveillance of US phone records and overseas internet traffic, arguing he had full congressional approval – then went on to criticise "leaks" and "hype" in the media.

Xi Jinping, China's premier, will attend the presidential summit in California

As the issue threatened to overshadow the president's summit with the Chinese premier Xi Jinping in California, Obama insisted that the operations had full congressional oversight and struck an appropriate balance between privacy and national security.

"If people don't trust Congress and the judiciary then I think we are going to have some problems here," he said.

Obama was speaking on his way to the summit with Xi, where he had been expected to raise the issue of Chinese cyberhacking. Instead, he was forced to deal with a growing row over the extent of the surveillance state in the US.

The director of national intelligence, James Clapper, confirmed revelations by the Guardian and the Washington Post that the National Security Agency uses companies such as Google, Facebook and Apple to obtain information that includes the content of emails and online files.

Coupled with the acknowledgement that authorities had undertaken a seven-year programme to monitor the telephone calls of potentially millions of people in the US, it became clear that the Obama administration has embraced and expanded the surveillance regime begun under President Bush.

The Department of Justice declined to say whether it had launched a formal leak inquiry after the revelations. "I have no comment," said Andrew Ames, a spokesman for the department.

Obama claimed that the disclosures had been damaging and said oversight should be left to Congress and the US courts. "I don't welcome leaks, because there's a reason why these programmes are classified," he said. "If every attempt to stop a terrorist act is on the front page of the newspaper or on television ... then the people who are trying to do us harm are going to take preventative measures."

Nonetheless, he said it was good to have a public debate about balancing security with civil liberties, without explaining how that was possible in the case of classified activities. "I think it's healthy for this democracy," said Obama. "I think it's a sign of maturity."

The US has admitted using a secret system to mine the biggest technology companies to spy on millions of people's online activity. Clapper insisted that the internet surveillance programme, known as Prism and disclosed by the Guardian and the Washington Post on Thursday, only covered communications with foreigners and did not target US citizens. "Information collected under this programme is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats," Clapper said.

He acknowledged that Section 702 of the Foreign Intelligence Surveillance Act was being used to "facilitate the acquisition of foreign intelligence information".

A secret 41-slide PowerPoint presentation obtained by the Guardian says the information can be collected "directly from the servers" through the Prism system. The technology companies denied direct access to servers was possible in this way, but they admitted complying with legal orders to turn over information.

Clapper attacked the disclosure as "reprehensible" for risking "important protections for the security of Americans".

More immediately, the admission places the US in an embarrassing position when it confronts Chinese leaders over their alleged use of cyber-espionage during a long-awaited summit that was due to begin in California yesterday.

Experts on US relations in Beijing said the revelations were bound to "weaken the US government's moral position" although they drew distinctions between the two approaches and expected the issue would still be raised. "Obviously the news breaking on the eve of the Sunnylands summit puts Obama in a much weaker position," added Linda Jakobson, east Asia programme director at the Lowy Institute.

To push back against the growing scandal, Clapper also declassified aspects of a highly secretive acquisition of all Verizon's phone records first disclosed by the Guardian. Clapper took the extraordinary step late on Thursday night to argue that the programme operates "within the constraints of law" and "appropriately protect[s] privacy and civil liberties".

"The collection is broad in scope because more narrow collection would limit our ability to screen for and identify terrorism-related communications," Clapper said. Yet he defended the broad, ongoing intelligence collection effort by saying that "only a small fraction" of the phone records - such as phone numbers and call - are ever scrutinized by intelligence analysts for connections to terrorism.

Such scrutiny occurs according to "strict restrictions" overseen by the Justice Department and the special, secretive US surveillance court, he continued.

Clapper reiterated that the content of phone calls is off-limits under the National Security Agency "metadata" collection program - while avoiding reference to the Prism system that sweeps up such

content from nine participating internet companies. Clapper also repeatedly pointed out that some, but not all, members of Congress “have been fully and repeatedly briefed” on the programme.

The secret document obtained by the Guardian shows that the Prism system facilitates extensive, in-depth surveillance on live communications and stored information.

The NSA access was enabled by changes to US surveillance law introduced under President Bush and renewed under Obama in December 2012. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.

Technology companies appeared not to be aware of how the NSA characterises the system. Apple said it had “never heard” of Prism. An Apple spokesman said: “We do not provide any government agency with direct access to our servers and any agency requesting customer data must get a court order.”

A Google spokesman said it did not provide officials with direct access. “Google cares deeply about the security of our users’ data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government ‘back door’ into our systems, but Google does not have a ‘back door’ for the government to access private user data.”

Legislators, particularly those serving on committees that oversee US intelligence, also confirmed the existence of the spy efforts, saying they have been in effect for at least six years.

“These activities have led to the successful detection and disruption of at least one terrorist plot on American soil, possibly saving American lives,” said the leadership of the House intelligence panel, Representatives Mike Rogers, a Republican, and Dutch Ruppersberger, a Democrat, in a joint statement.

But senator Ron Wyden, who for at least two years has warned about secret government interpretations of the Patriot Act authorising much larger surveillance efforts than the Obama administration has described, suggested the spying has not disrupted any such plots.

“Based on several years of oversight, I believe that its value and effectiveness remain unclear,” said Wyden, a Democratic member of the Senate intelligence committee.

Dan Roberts Spencer Ackerman, *The Guardian*, June 8, 2013

How America’s National Security Agency may be watching you

Charles Arthur explains the US government’s huge online surveillance project

What is the scandal?

Photograph: Google Google’s data centre in Iowa. The company says it does not have a ‘back door’ for the US government to access private use data

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 a 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 organisations will be heard, subject to limited exceptions, in the US." That would probably mean the NSA's licence to spy would trump EU complaints. 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 pass 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.

Pressure on UK government over secret intelligence gathering

Ministers were under mounting pressure last night to explain whether they had authorised GCHQ to gather intelligence on Britons from the world's biggest internet companies through a covertly run operation set up by America's top spy agency.

MPs, academics and campaign groups rounded on the government after the Guardian disclosed that GCHQ, the UK's electronic eavesdropping and security headquarters, had been supplied with information from the highly- classified system.

The US-run programme, called Prism, would appear to have allowed GCHQ to circumvent the formal legal process required to seek personal material such as emails, photos and videos from an internet company based outside the UK.

GCHQ, the UK's electronic eavesdropping and security headquarters
According to documents obtained by the Guardian, the agency generated 197 intelligence reports from Prism last year, and has had access to the programme since at least 2010.

Last night senior MPs challenged David Cameron, the foreign secretary William Hague – who oversees the work of GCHQ – and Theresa May, the home secretary, to spell out what they knew of Prism.

David Davis, the former shadow home secretary, told the Guardian: “It is a perfectly reasonable question to put to the foreign secretary: did you or did you not authorise all of these Prism intercepts on British citizens? It is perfectly appropriate for him to answer that. We are not asking him to comment on individual cases. We are saying did you, as a matter of policy, sign off all of them or sign off some of them? If so what was the criteria?”

Yvette Cooper, the shadow home secretary, said parliament's intelligence and security committee (ISC) should launch an immediate inquiry into Prism, the nature of the intelligence being gathered, and the extent of UK oversight by ministers.

“It is important for the UK intelligence community to be able to gather information from abroad including from the United States. However there also have to be legal safeguards in place, including proper protection for British citizens' privacy. That is why the prime minister, home secretary and foreign secretary, and all the intelligence agencies should provide full information to the ISC.” Keith Vaz, the chairman of the home affairs select committee, added: “The most chilling aspect is that ordinary American citizens and potentially British citizens too were apparently unaware that their phone and online interactions could be watched. This seems to be the snooper's charter by the back door.” The Foreign Office and GCHQ have so far refused to be drawn on the issues, saying they will not comment on intelligence matters.

By coincidence, the ISC is due to travel to Washington next week – giving MPs their first opportunity to question US officials about the covert programme.

The details of GCHQ's use of Prism are set out in documents which were obtained by the Guardian. The papers were prepared for senior analysts working at America's National Security Agency, the biggest eavesdropping organisation in the world.

Dated April this year, they describe the remarkable scope of a previously undisclosed "snooping" operation which gave the NSA and the FBI access to the systems of nine of the world's biggest internet companies.

The group includes Google, Facebook, Microsoft, Apple, Yahoo and Skype. The documents, which appear in the form of a 41-page PowerPoint presentation, suggest the firms co-operated with the Prism programme. Technology companies denied knowledge of Prism, with Google insisting it "does not have a back door for the government to access private user data". But the companies acknowledged that they complied with legal orders.

The existence of Prism, though, is not in doubt.

Thanks to changes to US surveillance law introduced under President George Bush and renewed under Barack Obama in December 2012, Prism was established in December 2007 to provide in-depth surveillance on live communications and stored information about foreigners overseas.

The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.

The documents make clear the NSA has been able to obtain unilaterally both stored communications as well as real-time collection of raw data for the last six years, without the knowledge of users, who would assume their correspondence was private.

The NSA describes Prism as "one of the most valuable, unique and productive accesses" of intelligence, and boasts the service has been made available to spy organisations from other countries, including GCHQ.

It says the British agency generated 197 intelligence reports from Prism in the year to May 2012 - marking a 137% increase in the number of reports generated from the year before. Intelligence reports from GCHQ are normally passed to MI5 and MI6. The documents underline that "special programmes for GCHQ exist for focused Prism processing", suggesting the agency has been able to receive material from a bespoke part of the programme to suit British interests.

Unless GCHQ has stopped using Prism, the agency has accessed information from the programme for at least three years. It is not mentioned in the latest report from the Interception of Communications Commissioner Office, which scrutinises the way the UK's three security agencies use the laws covering the interception and retention of data.

Asked to comment on its use of Prism, GCHQ said it "takes its obligations under the law very seriously. Our work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight, including from the secretary of state, the interception and intelligence services commissioners and the intelligence and security committee".

The agency refused to be drawn on how long it had been using Prism, how many intelligence reports it had gleaned from it, or which ministers knew it was being used. A GCHQ spokesperson added: "We do not comment on intelligence matters."

However, campaigners insisted ministers had important questions to answer.

Eric King, head of research at Privacy International – a charity focused on the right to privacy – said: “Keeping the public in the dark about secretive and potentially unlawful programmes must stop, and greater oversight is needed to ensure human rights are not being trampled.”

Professor Peter Sommer, a cybersecurity expert, said: “It is one thing for the government to go to the public and say the level of the threat is so great that we need to have this type of surveillance, and quite another for them to do so covertly. The principle of jurisdiction swapping is not new and in some ways the fact the NSA has been helping GCHQ is not surprising. But the consequence of this is that there is far less oversight than people might imagine of GCHQ. One wonders whether ministers would have been told the details of something like Prism, or whether they were told in very general terms about what it involved.”

The existence and use of Prism reflects concern within the intelligence community about access it has to material held by internet service providers.

Many of the web giants are based in the US and are beyond the jurisdiction of British laws. Very often, the UK agencies have to go through a formal legal process to request information from service providers.

Because the UK has a mutual legal assistance treaty with America, GCHQ can make an application through the US department of justice, which will make the approach on its behalf.

Though the process is used extensively – almost 3,000 requests were made to Google alone last year – it is time consuming. Prism would appear to give GCHQ a chance to bypass the procedure.

Nick Pickles, director of privacy and civil liberties campaign group Big Brother Watch, said: “There are legal processes to request information about British citizens using American services and if they are being circumvented by using these NSA spying arrangements then that would be a very serious issue. The wider legal authority of the surveillance that the US government has been undertaking is being disputed by very senior figures and it is essential that questions are asked at the highest levels about whether British citizens have seen their privacy intruded upon without adherence to the proper legal process or any suspicion of wrongdoing.”

In its statement about Prism, Google said it “cares deeply about the security of our users’ data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government ‘back door’ into our systems, but Google does not have a back door for the government to access private user data”.

Several senior tech executives insisted they had no knowledge of Prism or of any similar scheme. They said they would never have been involved in such a programme.

“If they are doing this, they are doing it without our knowledge,” one said. An Apple spokesman said it had “never heard” of Prism.

In a statement confirming the existence of Prism, James Clapper, the director of national intelligence in the US, said: “Information collected under this programme is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats.”

A senior US administration official said: “The programme is subject to oversight by the foreign intelligence surveillance court, the executive branch, and Congress.

“It involves extensive procedures, specifically approved by the court, to ensure that only non-US

persons outside the US are targeted, and that minimise the acquisition, retention and dissemination of incidentally acquired information about US persons.”

Nick Hopkins and Nicholas Watt, *The Guardian*, June 8, 2013

U.S. draws up list of foreign cyber-targets

President is defiant as he welcomes public debate about secret system

Barack Obama has ordered his senior national security and intelligence officials to draw up a list of potential overseas targets for US cyber-attacks, a top secret presidential directive obtained by the Guardian reveals.

The 18- page Presidential Policy Directive 20, issued in October last year but never published, states that what it calls Offensive Cyber Effects Operations (OCEO) “can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging”.

It says the government will “identify potential targets of national importance where OCEO can offer a favourable balance of effectiveness and risk as compared with other instruments of national power”.

The directive also contemplates the possible use of cyber actions inside the US, though it specifies that no such domestic operations can be conducted without the prior order of the president, except in cases of emergency.

The aim of the document was “to put in place tools and a framework to enable government to make decisions” on cyber actions, a senior US administration official told the Guardian.

Obama’s move to establish a potentially aggressive cyber warfare doctrine will heighten fears over the increasing militarisation of the internet.

The directive’s publication came as the president planned to confront his Chinese counterpart Xi Jinping at a summit in California yesterday over alleged Chinese attacks on western targets. It places the US in an embarrassing position when it confronts Chinese leaders over their alleged use of cyber- espionage during a long-awaited summit that was due to begin in California yesterday.

Experts on US relations in Beijing said Barack Obama struck a defiant stance yesterday in the face of revelations of widespread surveillance of US phone records and overseas internet traffic, arguing he had full congressional approval – then went on to criticise “leaks” and “hype” in the media.

As the issue threatened to overshadow the president’s summit with the Chinese premier Xi Jinping in California, Obama insisted that the operations had full congressional oversight and struck an appropriate balance between privacy and national security.

“If people don’t trust Congress and the judiciary then I think we are going to have some problems here,” he said.

Obama was speaking on his way to the summit with Xi, where he had been expected to raise the issue of Chinese cyberhacking. Instead, he was forced to deal with a growing row over the extent of the surveillance state in the US.

The director of national intelligence, James Clapper, confirmed revelations by the Guardian and the Washington Post that the National Security Agency uses companies such as Google, Facebook and Apple to obtain information that includes the content of emails and online files.

Coupled with the acknowledgement that authorities had undertaken a seven-year programme to monitor the telephone calls of potentially millions of people in the US, it became clear that the Obama administration has embraced and expanded the surveillance regime begun under President Bush.

The Department of Justice declined to say whether it had launched a formal leak inquiry after the revelations. "I have no comment," said Andrew Ames, a spokesman for the department.

Obama claimed that the disclosures had been damaging and said oversight should be left to Congress and the US courts. "I don't welcome leaks, because there's a reason why these programmes are classified," he said. "If every attempt to stop a terrorist act is on the front page of the newspaper or on television ... then the people who are trying to do us harm are going to take preventative measures."

Nonetheless, he said it was good to have a public debate about balancing security with civil liberties, without explaining how that was possible in the case of classified activities. "I think it's healthy for this democracy," said Obama. "I think it's a sign of maturity."

The US has admitted using a secret system to mine the biggest technology companies to spy on millions of people's online activity. Clapper insisted that the internet surveillance programme, known as Prism and disclosed by the Guardian and the Washington Post on Thursday, only covered communications with foreigners and did not target US citizens. "Information collected under this programme is among the most important and valuable intelligence information we collect, and is used to protect our nation from a wide variety of threats," Clapper said.

He acknowledged that Section 702 of the Foreign Intelligence Surveillance Act was being used to "facilitate the acquisition of foreign intelligence information".

A secret 41-slide PowerPoint presentation obtained by the Guardian says the information can be collected "directly from the servers" through the Prism system. The technology companies denied direct access to servers was possible in this way, but they admitted complying with legal orders to turn over information.

Clapper attacked the disclosure as "reprehensible" for risking "important protections for the security of Americans".

More immediately, the admission places the US in an embarrassing position when it confronts Chinese leaders over their alleged use of cyber-espionage during a long-awaited summit that was due to begin in California yesterday.

Experts on US relations in Beijing said the revelations were bound to "weaken the US government's moral position" although they drew distinctions between the two approaches and expected the issue would still be raised. "Obviously the news breaking on the eve of the Sunnylands summit puts Obama in a much weaker position," added Linda Jakobson, east Asia programme director at the Lowy Institute.

To push back against the growing scandal, Clapper also declassified aspects of a highly secretive acquisition of all Verizon's phone records first disclosed by the Guardian. Clapper took the extraordinary step late on Thursday night to argue that the programme operates "within the constraints of law" and "appropriately protect[s] privacy and civil liberties".

"The collection is broad in scope because more narrow collection would limit our ability to screen for and identify terrorism-related communications," Clapper said. Yet he defended the broad, ongoing intelligence collection effort by saying that "only a small fraction" of the phone records – such as phone numbers and call – are ever scrutinized by intelligence analysts for connections to terrorism.

Such scrutiny occurs according to "strict restrictions" overseen by the Justice Department and the special, secretive US surveillance court, he continued.

Clapper reiterated that the content of phone calls is off-limits under the National Security Agency "metadata" collection program – while avoiding reference to the Prism system that sweeps up such content from nine participating internet companies. Clapper also repeatedly pointed out that some, but not all, members of Congress "have been fully and repeatedly briefed" on the programme.

The secret document obtained by the Guardian shows that the Prism system facilitates extensive, in-depth surveillance on live communications and stored information.

The NSA access was enabled by changes to US surveillance law introduced under President Bush and renewed under Obama in December 2012. The law allows for the targeting of any customers of participating firms who live outside the US, or those Americans whose communications include people outside the US.

Technology companies appeared not to be aware of how the NSA characterises the system. Apple said it had "never heard" of Prism. An Apple spokesman said: "We do not provide any government agency with direct access to our servers and any agency requesting customer data must get a court order."

A Google spokesman said it did not provide officials with direct access. "Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'back door' into our systems, but Google does not have a 'back door' for the government to access private user data."

Legislators, particularly those serving on committees that oversee US intelligence, also confirmed the existence of the spy efforts, saying they have been in effect for at least six years.

"These activities have led to the successful detection and disruption of at least one terrorist plot on American soil, possibly saving American lives," said the leadership of the House intelligence panel, Representatives Mike Rogers, a Republican, and Dutch Ruppersberger, a Democrat, in a joint statement.

But senator Ron Wyden, who for at least two years has warned about secret government interpretations of the Patriot Act authorising much larger surveillance efforts than the Obama administration has described, suggested the spying has not disrupted any such plots.

"Based on several years of oversight, I believe that its value and effectiveness remain unclear," said Wyden, a Democratic member of the Senate intelligence committee.

Glenn Greenwald, Ewen MacAskill, Dan Roberts, Spencer Ackerman; *The Guardian*, June 8,

2013

* <http://www.guardian.co.uk/world/2013/jun/07/obama-china-targets-cyber-overseas>

Glen Greenwald: They have gone too far. The fightback has started

Glenn Greenwald, the journalist who broke the surveillance story, says US government persecution of whistleblowers must end

Commentary in *The Guardian*, June 8, 2013

Ever since Richard Nixon's administration broke into Daniel Ellsberg's psychoanalyst's office, the tactic of the US government has been to attack and demonise whistleblowers as a means of distracting attention from their own exposed wrongdoing and destroying the credibility of the messenger so that everyone tunes out the message.

As these whistleblowing acts become increasingly demonised ("reprehensible", declared the director of national intelligence, James Clapper), please just spend a moment considering the options available to someone who has access to numerous top secret documents.

They could easily enrich themselves by selling those documents for huge sums of money to foreign intelligence services. They could seek to harm the US government by acting at the direction of a foreign adversary and covertly pass those secrets to them. They could gratuitously expose the identity of covert agents.

None of the whistleblowers who have been persecuted by the Obama administration as part of its unprecedented attack on whistleblowers has done any of that: not one of them. Nor have those who are responsible for these current disclosures.

They did not act with any self-interest in mind. In fact the opposite is true: they undertook great personal risk and sacrifice for one overarching reason: to make their fellow citizens aware of what their government is doing in the dark. Their objective is to educate, to democratise, to create accountability for those in power.

The people who do this are heroes. They do it knowing exactly what is likely to be done to them by the planet's most powerful government, but they do it regardless. I don't want to over-simplify this: human beings are complex, and usually act with multiple, mixed motives.

But those who step forward to blow these whistles rarely benefit at all. The ones who benefit from their actions are you. You discover what you should know but what is being hidden from you: namely, the most consequential acts being taken by those with the greatest power, and how those actions are affecting your life, your country and your world.

In 2008, when he was a candidate for the presidency, Barack Obama decreed that "often the best source of information about waste, fraud, and abuse in government is an existing government employee committed to public integrity and willing to speak out," and he hailed whistleblowing as "acts of courage and patriotism, which can sometimes save lives and often save taxpayer dollars,

[and] should be encouraged rather than stifled as they have been during the Bush administration.”

The current, presidential incarnation of Obama prosecutes those same whistleblowers at double the number of all previous presidents combined, and spent the latest campaign season boasting about it.

The 2008 version of Obama was right. As the various attacks are inevitably unleashed on the whistleblowers, they deserve the gratitude and – especially – the support of everyone, including media outlets, for the noble acts that they have undertaken for the good of all of us.

When it comes to what the Surveillance State is building and doing in the dark, we are much more informed today than we were yesterday, and will be much more informed tomorrow than we are today, thanks to them.

Like puppets reading from a script, various Washington officials almost immediately began spouting all sorts of threats about “investigations” they intend to launch about these disclosures.

This has been their playbook for several years now: they want to deter and intimidate anyone and everyone who might shed light on what they’re doing with their abusive, manipulative exploitation of the power of law to punish those who bring about transparency.

That isn’t going to work. It’s beginning completely to backfire on them. It’s precisely because such behaviour reveals their true character, their propensity to abuse power, that more and more people are determined to bring about accountability and transparency for what they do.

The way things are supposed to work is that we’re supposed to know virtually everything about what they do: that’s why they’re called public servants. They’re supposed to know virtually nothing about what we do: that’s why we’re called private individuals.

This dynamic – the hallmark of a healthy and free society – has been radically reversed. Now, they know everything about what we do, and they are constantly building systems to know more. Meanwhile, we know less and less about what they do, as they build walls of secrecy behind which they function. That’s the imbalance that needs to come to an end.

No democracy can be healthy and functional if the most consequential acts of those who wield political power are completely unknown to those to whom they are supposed to be accountable.

The times in American history when political power was constrained were when they went too far and the system backlashed and imposed limits. That’s what happened in the mid-1970s when the excesses of J Edgar Hoover and Nixon became so extreme that the legitimacy of the political system depended upon it imposing restraints on itself.

And that’s what is happening now as the government continues on its orgies of whistleblower prosecutions, trying to criminalise journalism, and building a massive surveillance apparatus that destroys privacy, all in the dark. The more they overreact to measures of accountability and transparency – the more they so flagrantly abuse their power of secrecy and investigations and prosecutions – the more quickly that backlash will arrive.

I’m going to go ahead and take the constitution at its word – that we’re guaranteed the right of a free press. So, obviously, are other people.

And that means that it isn’t the people who are being threatened who deserve and will get the investigations, but those issuing the threats who will get that. That’s why there’s a free press. That’s what adversarial journalism means.

Obama is like Google: a once hip brand tainted by Prism

Commentary by Jonathan Freedland, *The Guardian*, June 8, 2013

Among the guests at the fabled Bilderberg meeting, held this weekend just outside London, are the top brass of Google, Amazon and Microsoft. How appropriate they should be there, alongside luminaries of the US political and military establishment.* For this was the week that seemed to confirm all the old bug-eyed conspiracy theories about governments and corporations colluding to enslave the rest of us.

The Guardian revealed that the US National Security Agency has cracked open our online lives, that it can rifle through your emails, listen to your calls on Skype, watching “your ideas form as you type”, as a US intelligence officer put it – apparently in cahoots with the corporate titans of the web.

This disgraces all involved, but it damages the head of the US government most. Barack Obama always had much in common with the Apple and Facebook crowd. Like them, he held out the promise of modernity – a slick, cool contrast to their creaky, throwback rivals. (Obama was rarely without BlackBerry and iPod; McCain and Romney came from the age of the manual typewriter.) But, like those early internet giants, he promised more than just an open-necked, hipper style. He would be better too. Google’s informal motto is Don’t be Evil. Obama’s is Hope.

Perhaps people lost their innocence about Google and Facebook long ago, realising that, just because their founders were kids in jeans, they were no less red-toothed than any other capitalist behemoth. But now the president’s reputation will suffer the same treatment. This Prism will dim the halo that once adorned him.

For he has authorised not merely the continuation of a programme of state surveillance that he once opposed, but has actively expanded it. That officers who serve him could brag in a 41-page presentation – one laced with David Brent-style grandiosity, starting with the naffness of the Prism logo – of their ability to collect data “directly from the servers” of the likes of Microsoft, Apple and Yahoo, will be a lasting stain on his record. In this, he is George W Obama. There is a mirthless chuckle to be had from a president repeatedly slammed as a “liberal” whose legacy will be marred by a series of gravely illiberal acts.

He promised but failed to close the detention camp at Guantánamo Bay, where men have been held for more than a decade without charge (though Congress shares the blame for that). He has made routine the use of drones, assassinating enemies from the sky – repeatedly taking the innocent in the process, as he’s admitted. Last month it emerged that Obama had seized two months of telephone records from Associated Press. Little wonder that the high citadel of US liberalism, the editorial column of the New York Times, this week declared that “The administration has now lost all credibility”, later softening the blow by adding the words, “on this issue”.

It is becoming ever harder for liberals to defend Obama. One forlorn effort I heard this week was that perhaps he did not know what the NSA was up to, even though we’re told Prism is now the prime generator of material for the president’s daily brief. When you’re reduced to saying your hero is not evil, just useless, you know you’re in trouble.

As for the web companies, their role remains unclear. Initially they insisted that the access-all-areas relationship described in Prism's PowerPoint presentation is false and there was no such collaboration. Yet one industry insider tells me that "it's very hard to think the companies did not know" the NSA was collecting their data, since such an intrusion "would show up pretty damn quick". That leaves a third possibility: that the Prism pitch was exaggerated, in order to make it a more attractive sell to its potential customers among the US - and UK - intelligence fraternity.

Whatever the truth, it's unlikely to have a lasting impact on the web giants' success. That's partly because of cynicism: plenty of us assumed these big companies abused our privacy anyway. But it's also because our relationship is one of dependence. When it emerged that Starbucks, Amazon and Google had all been paying negligible tax in the UK, it was obvious Starbucks would feel the consumer heat most, simply because it's easy to get a cup of coffee somewhere else. Amazon is harder to avoid and Google all but impossible. So reliant are we on these companies' services, we simply shrug and move on.

And here lies the heart of the matter, the shift in our lives that has made Prism possible. Back in the Le Carré days of cold war espionage, private information was hard to get. Spies relied on papers stuffed in manila files, or operatives on street corners, forced to gain each bit of knowledge by hand. Back then, people gave up their personal details sparingly and reluctantly.

Now we are liberal with our innermost secrets, spraying them into the public ether with a generosity our forebears could not have imagined. Where we once sent love letters in a sealed envelope, or stuck photographs of our children in a family album, now such private material is despatched to servers and clouds operated by people we don't know and will never meet. Perhaps we assume that our name, address and search preferences will be viewed by some unseen pair of corporate eyes, probably not human, and don't mind that much. We guess the worst that can happen is Google bothering us with an annoying ad or Spotify recommending Taylor Swift.

But if that knowledge goes elsewhere, if governments can get it when they ask for it, or even without asking for it, that means something else entirely. It means the intelligence agencies can watch the entire population, albeit by privatised means, having in effect outsourced spying to the web mega-companies.

That leaves us with a choice. Either we try to stuff this genie back in the bottle and return to the privacy habits of old. Unlikely. Or we demand companies stand firm when pressed by governments to disclose our data. Not easy. Or we demand lawmakers change the rules, restraining the executive branch's limitless appetite for information on us.

It's hard to be optimistic, for technology has made the pickings available too rich, too tempting, for the spies to resist. And, strangest of all, it is us who made this possible - by becoming informants on ourselves.

** Seven members of Canada's economic and political elite are attending the 2013, invitation-only Bildeberg Conference. They are Heather Reisman, Galen Weston, Frank McKenna, Brad Wall, Ed Clark, John Torys and economist Marie-Josée Kravis.-RA*

P.S.

* From A Socialist in Canada:

<http://www.rogerannis.com/prism-a-massive-internet-spying-scheme-by-u-s-government-is-revealed/>