

Chapter 4

4 A Global Surveillance Network

4.1 Introduction

The extent of the collaboration between British and American signal intelligence agencies since World War II was long suspected, but it has been incontrovertibly exposed by Edward Snowden. The NSA and GCHQ operate so closely that they resemble a single organisation in many aspects, with an extremely close relationship with the other three members of the Five Eyes pact: Canada, Australia, New Zealand.

Since the end of the Cold War, the network of collaboration around the Five Eyes has grown to the point where we can speak of a global surveillance complex with most countries willing to be part of the club. According to security experts, this is driven by the same network effects that create the Google monopoly.ⁱ

Given that many details of these arrangements remain secret, it is hard to see how parliament and courts in one country can ever hope to rein them in.

This creates practical problems for understanding the extent of intrusiveness of any surveillance, because we do not know who has access to the information. It is possible that US agencies that work closely with the NSA, such as the FBI, have access to more information from GCHQ than British police.

In the other direction, the UK intelligence services are not constrained by any publicly available legislation in obtaining unsolicited intercepted material from other countries, even where the communications in question belong to people within the UK.

But despite these levels of collaboration, the US takes an exceptionalist approach to rights, where citizens from other countries are not given sufficient legal protections from surveillance. This situation may have worked in the past when spying was more restricted and targeted. But the growth of the internet and the central position of the US means that millions of people are now subjected to surveillance without legal recourse.

4.2 The Special Relationship and Friends

The UK has a closer relationship with the US than any other country. There is extensive exchange of information in both directions, with many pooled resources where it is hard to tell who owns the information. This reaction has been widely documented.

The NSA pays GCHQ substantial amounts of money, some £100m in the three years running to 2013.ⁱⁱ This is a fairly small proportion of the overall budget of the NSA, which was \$10.8 billion in 2013.ⁱⁱⁱ The payments have covered infrastructure for raw data gathering - e.g. £15.5m towards redevelopments at GCHQ's site in Bude, Cornwall, which intercepts cable communications - but also support for NATO operations in Afghanistan.

The leaked documents make clear that the money is not negligible and has “protected (GCHQ's core) budget” during several years of cuts. The papers also make clear that this is not a charitable donation, and the NSA expects to get their investment back. But given the strategic importance of the US relationship for the UK, accounting for 60% of refined intelligence,^{iv} GCHQ could be forgiven for prioritising support for the NSA, even without direct compensation. One possible additional explanation for the payments could be that besides protecting GCHQ's core capabilities and the interests of the NSA they also provide some form of legal and information ownership structure for certain joint activities.

Both countries are part of the so-called Five Eyes alliance. The intelligence sharing pact - formally called the UKUSA agreement - covers the US, the UK and ^v Canada, Australia and New Zealand - called Second Parties. The pact was started after the Second World War, but only officially acknowledged in 2010.^{vi} The agreement was so secret that not even some prime ministers were aware of its existence.^{vii} Many of the NSA documents leaked by Edward Snowden are marked FVEY, meaning they can be shared within the alliance.

These countries share raw data from bulk collection, hacking technology and tools for analysis. But the Snowden leaks give a firm impression that the UK is the partner in the alliance that works more closely with the US. The NSA and GCHQ have many joint programmes, including a programme for joint experiments to break encryption.^{viii} As we discuss elsewhere, hundreds of NSA analysts are working within GCHQ on TEMPORA/XKEYSCORE.

NATO countries like Germany and Sweden and other close US allies, such as Israel, have traditionally formed part of a wider intelligence sharing network. But this has now expanded hugely to over 35 countries.^{ix}



4.3 Integrated Systems of Mass Surveillance

Leaked documents paint a picture not just of comprehensive sharing of raw data from bulk collection between the US and the UK, but of completely integrated systems. NSA documents refer to TEMPORA as the world's largest XKEYSCORE, giving instructions for US agents to get an access account, including an induction on the UK legal system.

US analysts celebrated having full access in 2012.^x Analysts that have completed training in the UK legal requirements - and have achieved a certain level of proficiency in using XKEYSCORE - are automatically given TEMPORA access. TEMPORA appears as another database in the analysts' "XKS Central". Cross searches are meant to be compliant with the legal requirement of both jurisdictions.

It has been revealed that 250 NSA operatives have direct access to manipulate Tempora^{xi} and a further 850,000 US personnel have access to the data it generates. According to The Guardian, Americans were given some guidelines on accessing Tempora, but were told by GCHQ that when it came to carrying out their own searches they were responsible for assessing the human rights balance of necessity and proportionality: "it's your call".^{xii}

GCHQ contributes several nodes to the network and have their own XKEYSCORE manual in their internal wiki.^{xiii} The other Five Eyes countries also have access to the system. But it is unclear precisely what access they have to US data.

The tools for mass surveillance are shared more widely. Under the codes Special Source Access and Foreign Partner Access, leaked NSA documents describe the global system for accessing communications networks.^{xiv} The US spent around \$192 million between 2011 and 2013 supporting these particular collaborations.

There are two separate programmes. WINDSTOP involves the Five Eyes countries, but primarily a partnership with the UK, “to develop a well-integrated over-arching architecture”^{xv} to utilize unprecedented access to communications into and out of Europe and the Middle East”.

RAMPART-A integrates a broader group of third party countries in the network of high speed access to the internet backbone by providing them with the TURMOIL technology we discussed above. This provides a lower level of access to the data in cables than XKEYSCORE.

But in some cases the NSA also share access to XKEYSCORE system, for example with Germany's^{xvi} BND and Sweden's FRA.^{xvii} It is unclear what is the role of the UK in these arrangements and what exact access these agencies have to British data.

At least some of the information collected by the NSA through cable intercepts in partnership with third parties is shared with the Five Eyes through the TICKETWINDOW programme.^{xviii}

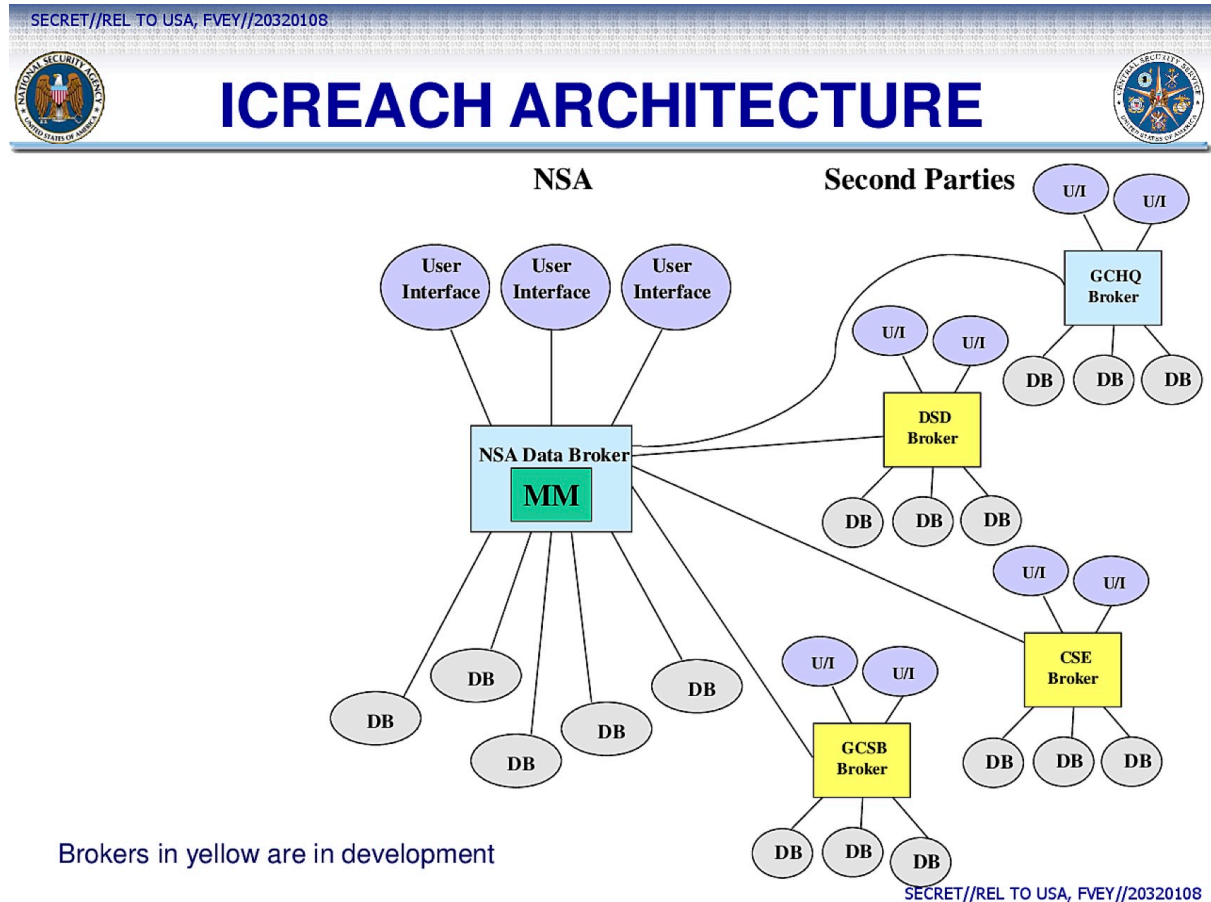
TICKETWINDOW data is obtained by the US under Executive Order 12333, for external data, which means that it has very limited privacy safeguards. In 2011, the type of full take collection of Internet data from cables practiced by GCHQ had been ruled illegal in the US^{xix} under the Foreign Intelligence Surveillance Act (FISA 1978). Despite denials, the NSA appears to bypass these restrictions by getting GCHQ to collect the data and send it to the US. They are then free to search and process under the general capabilities provided by the US Executive Order 12333,^{xx} which is less restrictive as it is intended to cover activities abroad.

US civil liberties groups have criticised^{xxi} the lack of safeguards in EO 12333. The NSA did not deny the existence of the operation but stated^{xxii} that they only focused on foreign targets and applied “Attorney General-approved processes to protect the privacy of U.S. persons - minimizing the likelihood of their information in our targeting, collection, processing, exploitation, retention, and dissemination”.

This system raises similar questions to other forms of data sharing, but its flexibility and live access bring added complications in terms of oversight and accountability.

In addition, leaked documents show that the NSA is sharing data from the Five Eyes with the wider US intelligence community, and in 2007 were building a search tool called ICREACH


that other agencies can use to trawl through large amounts of communications metadata amounting at the time to some 850 billion records about phone calls, emails, cellphone locations, and internet chats.^{xxiii}



We would expect Parliament to ask what exact mechanisms are available for the overseeing of access to data by US security services in the many available channels. For example, security sources have stated that when UK systems identify sensitive data of interest for further investigation, this is noted and passed on to the intercept commissioner. Is this also the case with US operatives?

4.3.1 Muscular

The leaked documents about the MUSCULAR programme of access to cables from Google and other internet companies are marked for access only by the US and the UK, and not the other 5 eye partners.



TOP SECRET//COMINT//REL-USA,GBR

MUSCULAR (DS-200B)

- Operational July 2009
- (S//REL USA,GBR) Large international access located in United Kingdom
- Four TURMOIL T16s at 2.5Gb each - total ingest 10Gb
- LPTs installed May 2010 increase ingest to 20Gb
- Tasking worked cooperatively with GCHQ counterparts
- Partner to assume total control/responsibility for systems
- IP Subnet promotion in place, VoIP in the works

TOP SECRET//COMINT//REL-USA,GBR

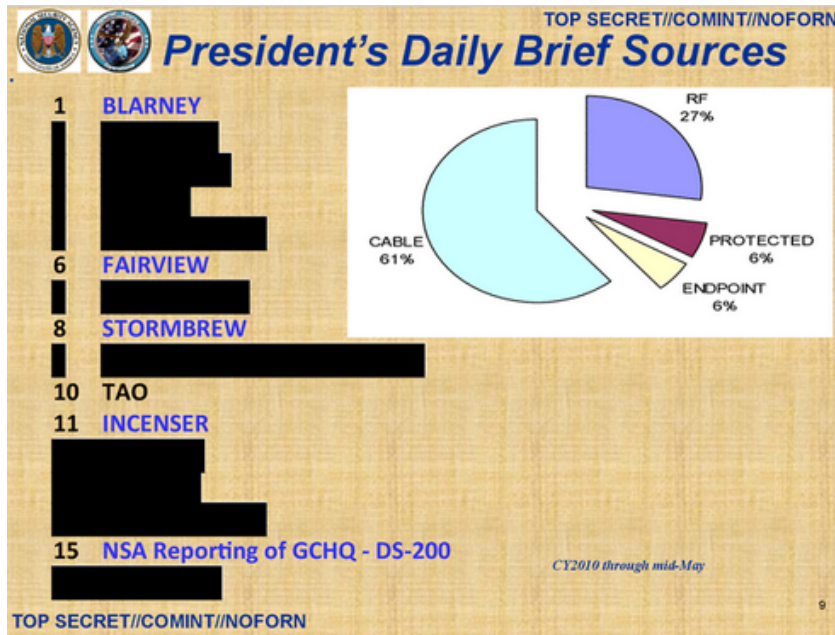
22

The exact legal basis and jurisdiction of the operation - including any safeguards to protect British citizens - are unclear. From the evidence presented by the government at the Investigatory Powers Tribunal in a case brought by Privacy International (see Chapter Six for more details), we can assume this operation is covered by a RIPA section 8(4) warrant for the interception of external communications, maybe the same one authorising Tempora. But in this case the jurisdiction is less clear. The leaked slides clearly show that the programme sends millions of records to their headquarters in Fort Meade, USA. It is unclear how the information of British citizens is protected during processing by the NSA.

4.3.2 Incenser

The sharing of bulk data from the UK to the US under WINDSTOP has been documented in detail by security researchers^{xxiv} following the leaked documents regarding the INCENSER programme described in the previous section.

INCENSER traffic is labeled TICKETWINDOW for sharing with Five Eyes countries with the label DS-300, and it is considered the NSA's fourth-largest cable tapping program in volume which is collected. Information from INCENSER - and other GCHQ sources - is used to write presidential briefings.



The programme provides large amounts of data, being the fourth largest in the NSA network. According to leaked documents between December 10, 2012 and January 8, 2013 the WINDSTOP programme collected more than 14 billion metadata records, of these DS-300 (INCENSER) contributed 14100 million and DS-200B (MUSCULAR): 181 million.

4.4 PRISM and the UK

4.4.1 What is PRISM

The PRISM programme gives the US government access to the internal systems of the largest US Internet companies (including Google, Facebook, Apple, Yahoo and Microsoft) to collect data related to specific users, keywords, etc. The programme operates via the FBI, which acts as intermediary between the NSA and the companies. This raises additional questions about the potential access by US domestic law enforcement agencies to data on UK citizens.

4.4.2 The legal basis for PRISM

The Section 702 of FISA Amendments Act^{xxv} (shortened here to FISA 702) provides the legal basis for PRISM. FISA 702 legalised warrantless wiretapping with some restrictions to safeguard the interests of Americans under the US constitution, but no protection for non-US persons. It is one of the most important elements in modern US surveillance legislation.

This law has brought a huge increase in the amount of data collected by removing the need for probable cause and individual prior warrants for communications data and content held at US soil, but involving foreigners abroad - technically called NON-US-PERSONS – in at least one end. NSA operatives are required to have a 51% confidence that they are not targeting US citizens or residents. Any US Internet business and cloud provider may have to make bulk data on their foreign customers available under FISA 702.

The implications of the FISA reforms that enabled PRISM were slow to sink in before the Snowden leaks. A report for the European Parliament on the security of cloud computing raised concerns that this law, "for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US". Importantly, the reforms also extended surveillance from "communications" as in data in transit, to data stored in cloud computers in the US.^{xxvi} A study from the Netherlands raised additional concerns about the repurposing of private sector data for state surveillance in the context of FISA Amendments 2008.^{xxvii}

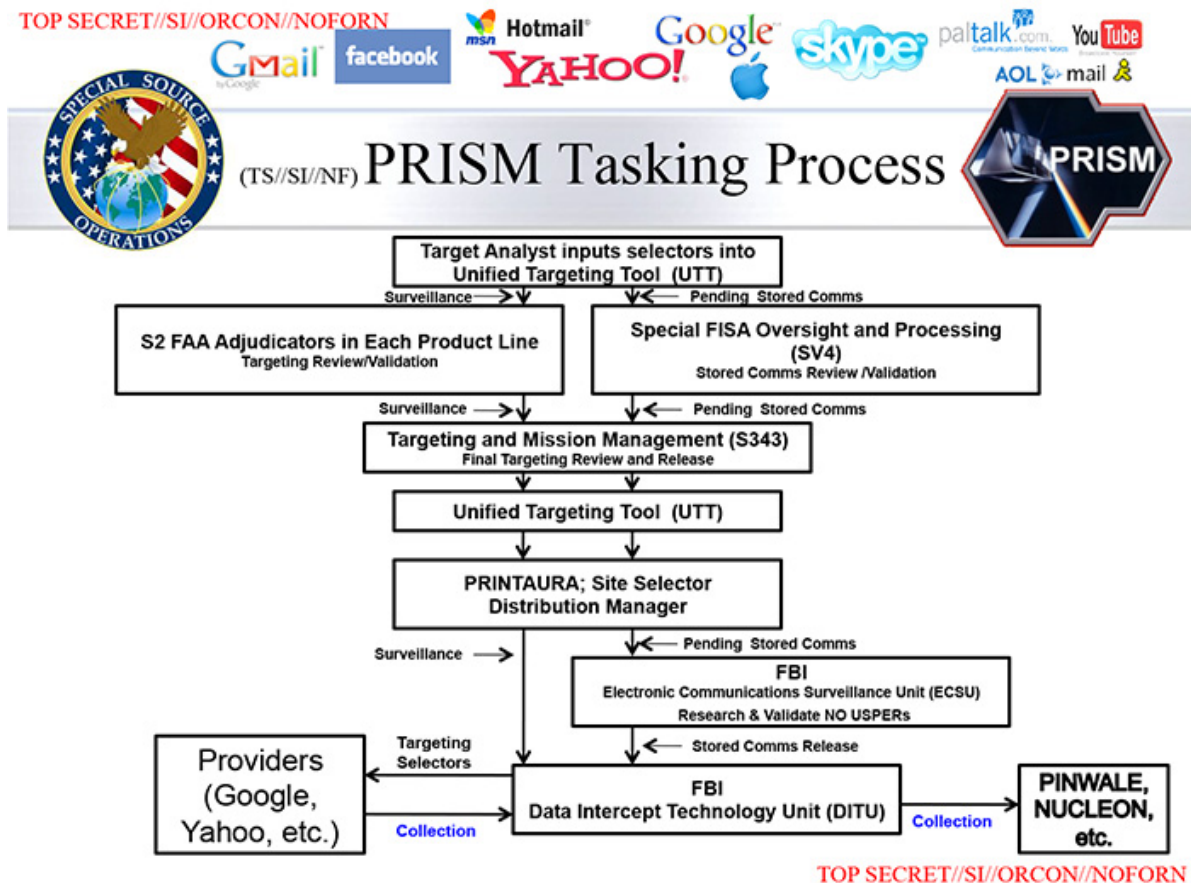
After 9/11 the US passed the infamous Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), which has been heavily criticised by civil liberties groups for giving too much power to the security services. It has a very broad reach, ranging from financial controls to immigration. But it also contains strong powers on surveillance.

According the American Civil Liberties Union, Section 215 of the PATRIOT Act "vastly expands the FBI's power to spy on ordinary people living in the United States".^{xxviii} The PATRIOT Act is mainly geared towards domestic surveillance. Snowden documents show that s215 was used to compel Verizon to give the NSA details of all US domestic and international phone calls, and "on an ongoing basis".^{xxix}

But it is worth clarifying that the act does not seem to be directly involved in PRISM.

4.4.3 The workings of PRISM

The exact mechanisms for PRISM's operation are disputed. Technology companies named in the report have denied any knowledge of PRISM (only to be rebuffed by NSA lawyers),^{xxx} and reject the notion that the NSA has full access to their systems. Google for example, claims that they just use a simple secure file transfer server. Full access may not be the case, but a certain level of automated access must be in place to enable the kind of real-time queries and searches described in some documents. It is unclear how much data is extracted into NSA systems for analysis, and how much analysis takes place piggybacking resources from the companies. According to the original leaked documents published by The Guardian, PRISM is very cheap to run, costing some \$20 Million a year. This in principle would point at the use of company resources. The Washington Post has published documents claiming that the agencies have placed equipment inside the companies.^{xxxii}



Analysis of 160,000 actual pieces of surveillance material^{xxxiii} collected under FISA 702 and leaked by Snowden showed that 90% related to innocent people caught in the dragnet, and not the targets. The materials included photographs of children. According to the US Director of National Intelligence Transparency Report around 90,000 people were subjected to FISA 702 searches in 2013,^{xxxiii} some 800,000 innocent people could have been subjected to surveillance

under this programme. The slides published by the Washington Post show that there were 117,675 active surveillance targets in PRISM's counterterrorism database.

4.4.4 PRISM in context

PRISM is not the only source of bulk data obtained by the NSA in US soil, but apparently it has become the most important. As we explained elsewhere, the NSA has collaborated with communication providers - e.g. Verizon, ATT - to obtain internet and telephony data under the programme name UPSTREAM. When this data collection takes place in the US it is also generally authorised by FISA. A declassified 2011 FISA Court ruling^{xxxiv} shows that in a year FISA 702 allowed the NSA to acquire more than 250 million "Internet communications". Of these, around 9% come from UPSTREAM, while PRISM provides 91%. FISA allows materials intercepted to be stored for two years and PRISM data and contents for five.

This gives some idea of the importance of PRISM, but it is not the total of collected communications. The NSA also uses other legal tools for additional Upstream collection abroad and also collects information from satellites. In collaboration with the CIA - via the Special Collections Service^{xxxv} - data is also obtained at clandestine interceptions around the world.

4.4.5 Access to PRISM data by UK intelligence agencies

GCHQ has access to PRISM data, but the exact terms are unclear despite some initial discussions in Parliament in July 2013.^{xxxvi} The agency was reported to have generated at the time almost 200 intelligence reports from this data since 2010.^{xxxvii}

The Intelligence and Security Committee stated, after an investigation,^{xxxviii} that GCHQ did not circumvent any laws when accessing content via PRISM. General access is authorised under the Intelligence Services Act 1994, and when GCHQ sought information from the US, a warrant was already in place under the Regulation of Investigatory Powers Act (RIPA).

The government has explained in court that communications relating to people based in the UK but using US Internet services can be intercepted using RIPA Section 8(4) warrants because those communications are classed as foreign in nature. These RIPA warrants are discussed in more detail in the following sections, but are very broad and don't need to mention named individuals, so it is unclear what exact information has been sought.

These warrants allow for the interception of content and associated metadata, but we do not know if these are treated differently when obtained under PRISM. We don't know if any measures designed to protect excessive intrusion when the data is collected by GCHQ are also in place here.

It is also unclear what happens to data that has been volunteered without GCHQ asking for it. In some cases maybe it will be urgent information to stop an imminent attack. But given that 60% of refined information comes from the US,^{xxxix} this surely includes a lot of material that is incorporated into ongoing investigations or simply filed.

Since the initial revelations about PRISM, we have learnt that GCHQ had direct access to PRISM during the 2012 London Olympics, with 100 operatives generating some 11,500 extracts in a six day period.^{xl} The role of the FBI in mediating British access is unclear. More recently GCHQ have requested a permanent arrangement for full unsupervised access to PRISM under the above mentioned FISA 702. It is not clear whether this request has been approved, and how it would work in practice.

TOP SECRET//SI//NOFORN



(TS//SI//NF) PRISM Operations Highlight
Olympics Support – GCHQ Using PRISM Access

•Olympic Option Status as of 24 May 2012:

- Trained/approved GCHQ users accessing PRISM data is at 100, expected to remain at that level throughout the Olympic timeframe.
- 256 selectors currently on cover.



- Between 16 May and 22 May 2012, 11,431 cuts of traffic have been forwarded.

-Four reports have been generated since 12 Apr 2012.

- Reports currently tracking suspected terrorist groups or individuals who could potentially target the Olympics.



TOP SECRET//SI//NOFORN

The NSA have stated that they can only share PRISM data with agencies that have minimisation processes to weed out the data of US persons, but do they require any limitations on access to data from nationals of those countries, let alone third parties even from other Five Eyes countries? This could create a situation where different countries spy on each other's citizens, except the US.

The new director of GCHQ has complained extensively that the agency suffers from a lack of access to data from US internet companies. But it appears that the agency has had some access in the past. It is possible that the Snowden leaks have triggered a change in the access to PRISM by GCHQ as US authorities become more stringent. This could well be the largest impact of the leaks for the organisation.

4.5 Access to NSA Databases

The NSA maintains huge amounts of collected data in a complex system of storage and retrieval. Specialised databases keep content and metadata for every type of communication imaginable. For example, the database MARINA^{xli} is used to store Internet metadata of millions of web users for a year, allowing for “pattern of life” analysis. FASCIA^{xlii} collects five billion mobile phone data records from around the world, including location^{xliii} that

allows the tracking of millions of individuals and groups, through the CO-^{xliv}TRAVELER programme.^{xlv} Several systems collect phone calls, videos, VOIP calls, etc.

GCHQ and other Five Eyes partners have some access to MARINA,^{xlvi} but it is unclear what the arrangements are for all the other such databases and associated tools. For example, we don't know what kind of direct access GCHQ has to CO-TRAVELER. Given that the related documents are marked for Five Eyes access, and some of the components were developed by the Australian Signals Directorate, we would expect GCHQ to be able to access and possibly contribute to the system.

But in several cases there is concrete evidence that GCHQ is accessing NSA systems.

DISHFIRE is a text message collection database operated jointly by the NSA and GCHQ since 2012. It collects 200 million text messages from across the world on a daily basis,^{xlvii} in bulk and not limited to intelligence targets. It uses this data to extract a remarkable amount of information: contact-chaining analysis, border crossings (roughly 1.6m a day), names from electronic business cards, financial transactions and geolocation, partly using messages from travel companies.^{xlviii} However, communications from American telephone numbers are minimised or removed.^{xlix} It is unclear whether this is the case with UK numbers.

GCHQ has access to the database. They use the metadata to see to view the contact history of UK numbers,^l but cannot read text contents without a warrant.^{li}

This system is quite unique, according to leaked documents: “In contrast to [most] GCHQ equivalents, DISHFIRE contains a large volume of unselected SMS traffic,” it states (emphasis original). “This makes it particularly useful for the development of new targets, since it is possible to examine the content of messages sent months or even years before the target was known to be of interest.”^{lii}

4.6 Spying on Citizens of Five Eyes Countries

The Snowden documents have raised questions over the extent that the US, UK and the other members of the secret Five Eyes agreement – Canada, Australia, New Zealand – spy on each other's citizens.

Privacy International have lodged a claim at the European Court of Human Rights demanding the agreements are publicly released,^{liii} and have carried out a detailed analysis based on the available information.^{liv} The Five Eyes appears to be the main alliance for intelligence cooperation including joint staffing of facilities and sharing of technology – and a distribution of tasks and geopolitical target areas. However, there is nothing to suggest that there is anything like an absolute no-spy pact and indeed the documents explicitly suggest that this is an option. Despite the lack of an official pact, there appears to be an understanding that citizens of second parties to the agreement should not generally be targeted, but this is possible, although the use of any incidentally collected information should be minimised.

This situation has generated mixed messages and confusion. US Secretary of State Hillary Clinton has claimed that blanket no-spy agreements do not exist,^{lv} explicitly mentioning Britain; a claim repeated by President Obama himself.^{lvi} But this has been denied by former intelligence operative, who claimed the Five Eyes countries were off limits.^{lvii}

A draft NSA memo from 2005 explains that in some cases it will be legitimate to secretly target Five Eyes citizens.^{lviii} But given the excellent relationships between the agencies it is unclear to what extent this targeted surveillance without the knowledge of the UK government has been put in practice.

What seems more significant is a document from 2007 outlining changes that enabled the routine analysis by the NSA of raw data of UK citizens caught in the dragnet of mass surveillance^{lix}.

There is less information on how the British agency operates, but in documents seen by The Guardian, UK officials have apparently boasted of their light oversight regime compared to the US.^{lx}

Leaked UK documents give some information on how the NSA handles queries to the US counterpart of TEMPORA, XKEYSCORE.^{lxi} According to these documents, targeting “US/Five Eyes” citizens is a violation, but their information could be used as part of a “defeat list” that is used to automatically reduce the volume of information processed.^{lxii} But it is unclear how these procedures work with direct queries to the British system, if indeed there is a completely separate system instead of procedural distinctions over the same databases.

In 2009 the NSA was slammed by the US Foreign Intelligence and Security Court (FISC) – responsible for authorising certain surveillance operations - for inappropriately storing information in databases accessible to other US agencies.^{lxiii} “NSA has generally failed to adhere to the special dissemination restrictions originally proposed by the government, repeatedly relied upon by the Court in authorizing the collection of the PR/TT metadata, and incorporated into the Court’s orders... as binding on NSA.” It is possible this affected the data of British citizens.

The activities of the other members of the club have received little scrutiny. According to leaked Five Eyes documents,^{lxiv} the Australian Signals Directorate proposed sharing “bulk, unselected, unminimised metadata” with the Five Eyes surveillance alliance, “as long as there is no intent to target an Australian national. Unintentional collection is not viewed as a significant issue.” This raises important questions for Australian citizens, but also for the UK government, if the offer was followed through. It also shows the disregard for privacy that seems to permeate those institutions.

Snowden has claimed that New Zealand has shared XKEYSCORE data on its own citizens with other partners in the alliance.^{lxv}

Third party countries don’t have guarantees that their citizens will not be targeted. For example, there is a RAMPART-A programme^{lxvi} involving access to cables in partnership

with countries such as Germany and Denmark. But according to Snowden any limitations in access to data about nationals in a country are bypassed by the NSA simply collecting the data at the other end of the cable in a different country.

In separate leaked documents the US is shown to be sharing raw intelligence data with Israel while acknowledging that both countries target each other.^{lxvii} In the memorandum of understanding, Israel is expected to extend the measures designed to handle data of US persons to “persons” of Five Eyes countries. But there is little detail and any protections appear to be mediated by the US, with no direct relationship between Israel and the UK. In addition, it is unclear if an obligation to immediately destroy data relating to the US government also applies to the Five Eyes.

In summary, it appears that membership of any club does not offer full immunity from US spying.

4.7 Conclusion

In this chapter, we have seen how inter-agency co-operation has become integration. It is hard to see how UK interests and UK citizens' privacy can be protected given the levels of data sharing and common analytics tools.

This is a very difficult area for politicians. There are different standards of law in different Five Eyes countries and entrenched views of what rights are extended to non-citizens. In the USA's case, their views of the rights of foreign citizens are strikingly low. Yet from the UK's point of view, there is a simple need to ensure protection of the innocent and ensure people's human rights can be protected to the standards we would expect domestically, whatever the legal regime of our allies.

Sometimes views will seem difficult to shift: why should the USA decide to honour foreigners' privacy and sacrifice their ability to spy, for security, political and economic ends? However there is some room for hope. The USA's ability to spy through data acquisition also depends on the position of their IT industry and internet platforms particularly. These companies in turn need our trust as foreigners. The result is that there is political and economic pressure for the USA to clean up their act.

When looking at the vast integration of personal data and spying tools, it is also obvious that there are questions of sovereignty and foreign policy that emerge. At the very least, it becomes hard for the UK to separate its own interests from those of the USA. It also provides potential leverage for the USA if the UK is obstinate about a particular policy. The possibility of collusion in other people's crimes emerges. It is not a given that USA will never engage in human rights abuses such as torture and assassination. We need a frank discussion about the implications; they may be acceptable but they should not be hidden.

The same underlying problems with GCHQ's essential approach resurfaces in this chapter. As the Internet and digital technologies have made communications central to the operation of most of our daily lives, we all become targets and implicated, in this case by international

data sharing and common analytics tools. Is that fair or reasonable: and how do we understand if it is?

-
- i <http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf>
- ii <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>
- iii <http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/>
- iv <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>
- v This may sound a simplistic stereotype, and some will argue that it is not relevant. But it is difficult to make sense of the Five Eyes other than through the bonds of cultural affinity brought by a shared ethnicity.
- vi <https://www.nationalarchives.gov.uk/ukusa/>
- vii <https://www.privacyinternational.org/reports/eyes-wide-open/understanding-the-five-eyes>
- viii <http://www.spiegel.de/media/media-35509.pdf>
- ix <http://electrospace.blogspot.co.uk/2014/09/nsas-foreign-partnerships.html>
- x <http://www.spiegel.de/media/media-34090.pdf>
- xi <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>
- xii Ibid.
- xiii <http://www.spiegel.de/media/media-34105.pdf>
- xiv <https://s3.amazonaws.com/s3.documentcloud.org/documents/1200866/foreignpartneraccessbudgetfy2013-redacted.pdf>
- xv Ibid.
- xvi <http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html>
- xvii <http://www.svt.se/ug/fra-has-access-to-controversial-surveillance-system>
- xviii <https://nsa.gov1.info/dni/2014/no-place-to-hide/sso/5.jpg>
- xix http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html
- xx <http://www.archives.gov/federal-register/codification/executive-order/12333.html>
- xxi <https://www.accessnow.org/blog/2014/07/22/rightscon-secret-law-and-the-democratic-process>
- xxii http://www.washingtonpost.com/world/national-security/nsa-statement-on-washington-post-report-on-infiltration-of-google-yahoo-data-center-links/2013/10/30/5c135254-41b4-11e3-a624-41d661b0bb78_story.html
- xxiii <https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/>
- xxiv <http://electrospace.blogspot.co.uk/2014/11/incenser-or-how-nsa-and-gchq-are.html>
- xxv <http://apps.washingtonpost.com/g/page/world/fisa-amendments-act-of-2008-section-702-summary-document/1141/>
- xxvi [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET\(2012\)462509_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf)
- xxvii <http://www.ivir.nl/publicaties/download/977>
- xxviii <https://www.aclu.org/free-speech-national-security-technology-and-liberty/reform-patriot-act-section-215>
- xxix http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf
- xxx <http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de>
- xxxi <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>
- xxxii http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html
- xxxiii http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013
- xxxiv https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf
- xxxv https://en.wikipedia.org/wiki/Special_Collection_Service
- xxxvi <https://www.openrightsgroup.org/ourwork/reports/prism-the-nsa-surveillance-and-the-uk-remaining-unanswered-questions-for-parliament>
- xxxvii <http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>
- xxxviii https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf

-
- xxxix <http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>
- xl <https://firstlook.org/theintercept/article/2014/04/30/gchq-prism-nsa-fisa-unsupervised-access-snowden/>
- xli <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>
- xlii <http://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden>
- xliii http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html
- xliv <http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/new-documents-show-how-the-nsa-infers-relationships-based-on-mobile-location-data/?commentID=washingtonpost.com/ECHO/item/1386720327-479-532#whitepaper>
- xlv http://www.washingtonpost.com/world/national-security/nsa-tracking-phone-locations-on-planetary-scale/2013/12/05/dfe21740-5db2-11e3-bc56-c6ca94801fac_story.html
- xlvi <https://www.spiegel.de/images/image-583972-galleryV9-mmeg.jpg>
- xlvii <http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>
- xlviii Ibid.
- xlix Ibid.
- l <http://www.channel4.com/news/intercept-text-messages-spy-nsa-gchq-british-phone>
- li <http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>
- lii Ibid.
- liii <http://www.theguardian.com/world/2014/sep/09/five-eyes-surveillance-pact-appeal-disclosure-human-rights>
- liv <https://www.privacyinternational.org/?q=node/301>
- lv <http://www.spiegel.de/international/world/hillary-clinton-interview-on-german-us-ties-and-presidential-plans-a-979812.html>
- lvi <http://www.nationaljournal.com/tech/obama-we-do-not-have-a-blanket-no-spy-agreement-with-any-country-20140502>
- lvii <http://thelead.blogs.cnn.com/2014/07/08/former-cia-operative-hillary-clinton-is-wrong-on-u-s-no-spy-agreement/>
- lviii <http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data>
- lix <http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data>
- lx <http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world>
- lxi <https://firstlook.org/theintercept/document/2014/02/18/discovery-sigint-targeting-scenarios-compliance/>
- lxii <https://epic.org/foia/doj/pen-reg-trap-trace/EPIC-FISA-PEN-REGISTER-FOIA-RELEASE-08082014-25.pdf>
- lxiii <http://www.lawfareblog.com/2013/11/the-november-nsa-trove-iv-the-internet-metadata-collection-story-develops/>
- lxiv <https://www.privacyinternational.org/?q=node/479>
- lxv Snowden claimed that New Zealand uses it to monitor
- lxvi <https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>
- lxvii <http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>