SURVEILLANCE AFTER SNOWDEN

Effective Espionage in an Age of Transparency

Robin Simcox

THE HENRY JACKSON SOCIETY
DEMOCRACY · FREEDOM · HUMAN RIGHTS

Published in 2015 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London
SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520
www.henryjacksonsociety.org

Title: Surveillance after Snowden: Effective Espionage in an Age of Transparency
By: Robin Simcox
ISBN 978-1-909035-18-8

£10.00 where sold

Front Cover Image: Laura Poitras/Praxis Films (© wikimedia.org).
www.istockphoto.com

SURVEILLANCE AFTER SNOWDEN

Effective Espionage in an Age of Transparency

Robin Simcox

www.henryjacksonsociety.org

Acknowledgments

Many of those who agreed to speak to me in the course of this project cannot be named. They all have my thanks, as does Elliot Soward for his research assistance. Additional thanks to Richard Black, Samantha Feuer, Mark Finegold, Oscar Isham, Livinia Mouries, Jeevan Vipinachandran, Chris Underwood and Quentin Wight.

About the Author

Robin Simcox is a Research Fellow at The Henry Jackson Society, where he works on terrorism and security issues.

He has written for the likes of *Foreign Affairs, Washington Post, Wall Street Journal, Los Angeles Times, The Guardian, New Republic and The Atlantic*; and comments in the media for the likes of the BBC, CNN, Sky News, al-Jazeera and Fox News. Simcox has spoken on a variety of platforms, including the UK Parliament and United States Southern Command. He has testified in the US Congress on multiple occasions.

Simcox has an MSc in U.S. Foreign Policy from the Institute for the Study of Americas, University of London, and a BA in History (International) from the University of Leeds, which included a year at the University of Newcastle, Australia.

About The Henry Jackson Society

The Henry Jackson Society is a think tank and policy-shaping force that fights for the principles and alliances which keep societies free – working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world.

Acronyms

CSP: Communication Service Provider

DoJ: Department of Justice

DIA: Defense Intelligence Agency

DNI: Director of National Intelligence

FBI: Federal Bureau of Investigation

FISA: Foreign Intelligence Surveillance Act

GC&CS: Government Code and Cypher School

GCHQ: Government Communications Headquarters

IPT: Investigatory Powers Tribunal

ISC: Intelligence and Security Committee of Parliament

OLC: Office of Legal Counsel

NSA: National Security Agency

ODNI: Office of the Director of National Intelligence

PCLOB: Privacy and Civil Liberties Oversight Board

PSP: President's Surveillance Program

RIPA: Regulation of Investigatory Powers Act

SIGINT: Signals Intelligence

SPoC: Single Point of Contact

Contents

EXECUTIVE SUMMARY

In the spring of 2013, former National Security Agency (NSA) contractor Edward Snowden used his government security clearance to steal a large quantity of classified government files. Via select journalists, Snowden alleged that intelligence agencies were tapping into fibre-optic cables containing telephony and internet-traffic data; intercepting and storing webcam images; and carrying out 'warrantless' surveillance. In terms of national security; diplomacy; privacy perceptions; media–state relations; citizens' trust in government; technology company–state relations; and many other ways, his actions have had a profound impact.

Despite the support that Snowden has received from certain sections of society, the expectation that intelligence agencies should stop terrorist attacks and serious crimes remains. Yet, at the same time, there are calls for them to reform and be more transparent in order to rebuild trust. The intelligence agencies are in a particularly unenviable position: asked to be less intrusive; more transparent; and yet, just as effective.

This report – which is informed, in part, by interviews with senior intelligence officers – studies the variety of ways in which Snowden's actions have impacted the US and the UK (particularly in terms of national security) and what lessons may be learned for the future.

UNITED STATES

PATRIOT Act Section 215

The US government carries out bulk collection of telephony metadata, which relates to the date and time of the call; the duration of the call; the calling number; and the number that has been dialled. The metadata is taken from Communication Service Providers (CSPs) and contained in a 'virtual lockbox' operated by the NSA. The agency can query the metadata when there is a 'reasonable, articulable suspicion' that the number is connected to a foreign terrorist group.

Section 215 helps government agencies 'connect the dots' for potential terrorist plots with both a foreign and domestic component. It is best understood as a safety measure designed to be part of the intelligence mosaic concerning attack plans that have a foreign and domestic component.

A Presidential task force assigned to investigate potential reform to government surveillance programmes stated that, with regard to Section 215, 'the use of […] telephony meta-data was not essential to preventing attacks'. However, one analysis noted that this may merely reflect its value in disrupting activities at an early stage; furthermore, thwarting terrorist attacks occurs by integrating various streams of the intelligence community's work, rather than relying on one programme alone.

Foreign Intelligence Surveillance Act Section 702

Section 702 of the Foreign Intelligence Surveillance Act (FISA) governs the interception of communications – for the specific purpose of acquiring foreign intelligence information – of those based outside the US. It is widely considered to be more integral to the NSA's work than that of Section 215.

The Section 702 programme is aimed at foreign nationals; no US citizen or anyone known to be in the US can be intentionally targeted.

Despite this, incidental – or accidental – collection of US citizens' communications occurs as part of the process of acquiring those of a foreign intelligence target, as it is not feasible to separate the two out. This data is retained, though oversight procedures from the Foreign Intelligence Surveillance Court (FISC, or FISA Court); the Executive Branch; and Congress are designed to 'minimize the acquisition, retention and dissemination of incidentally acquired information about US persons.'

There are two distinct types of data acquisition that take place under Section 702 authority: Upstream collection and PRISM collection.

PRISM

PRISM collection can capture the content of e-mails and instant messages. It takes place with the compelled assistance of electronic CSPs. For example, if the NSA discovered that a foreign national, based outside the US, used a US CSP e-mail address to contact his associates about a planned terrorist attack, it would request that the account be queried, as well as request access to the data collected (for example, e-mails sent and received from that address).

Upstream

Upstream collection refers to the NSA tapping into the underwater fibre-optic cable networks (the internet backbone) that carry telephone and internet data going into and out of the US. This type of collection takes place as communications flow between CSPs, and allows for the collection of communications not available via PRISM.

Executive Order 12333

Executive Order (EO) 12333 outlines the goals, direction, duties, responsibilities, and conduct of 17 intelligence agencies in the US. It is considered a foundational authority.

FISA does not apply if communications are being routed through servers or satellites without a US end. As long as it is for a 'valid foreign intelligence purpose', collection in these circumstances takes place under EO 12333. Therefore, EO 12333 is the Executive Branch's primary authority for foreign-intelligence gathering that takes place outside the US and is not governed by FISA.

EO 12333 targets foreign networks; yet, the information from these foreign networks may contain packets of data containing US citizens' communications. EO 12333 allows for the retention of these US citizens' communications, including content, as part of a foreign-intelligence investigation. As this collection occurs outside the US, the oversight that is applicable to Section 702 does not exist. Instead, oversight is provided by Attorney General-approved procedures; a variety of Inspectors general; oversight boards; general counsels; compliance officers; and privacy officers.

UNITED KINGDOM

Regulation of Investigatory Powers Act (RIPA)

The Regulation of Investigatory Powers Act (RIPA) provides the statutory framework for the government's use of covert techniques, including the interception of communications, in order to ensure their proportionality and the necessity of their use.

Section 8(4) of RIPA

Section 8(4) of RIPA is a vital piece of legislation that underpins the Government Communications Headquarters' (GCHQ's) work. Under Section 8(4), the UK intercepts communications by tapping fibre-optic communication cables carrying both external (i.e. communications sent or received outside the UK) and internal communications (i.e. communications sent and received inside the UK, where the sender and recipient are both based in the UK).

Section 8(4) warrants, which apply to external communications, have proved controversial because of the volume of communications being swept up and because communications are being intercepted using a general warrant from the relevant Secretary of State, which does not require a specific named subject to be on it. This type of collection also scoops up internal communications, as even they may be transmitted via internet-service providers in foreign nations (and the two cannot feasibly be separated out during the initial collection).

Sir Iain Lobban – when speaking as head of GCHQ, in November 2013 – explained the need for such data to be collected in bulk: '[i]f you think of the internet as an enormous hay field, what we are trying to do is to collect hay from those parts of the field that we can get access to […] containing the needles or the fragments of the needles that we might be interested in'.

Section 16 of RIPA

Under provisions in Sections 16 of RIPA, the communications of somebody in the UK which have been collected under Section 8(4) can be looked at; listened to; or read, but in limited circumstances.

Section 16(3) allows for their examination if they are 'referable to an individual' currently in the British Islands and the Secretary of State has certified that examination is being carried out for a national-security or serious-crime purpose. Sections 16(4) and (5) allow for their examination if the individual was believed, 'on reasonable grounds', to be abroad at time of interception, or if there has been 'a relevant change of circumstances'. For example, collection under Section 16 can continue for a very limited period if the individual visits the UK.

The exceptions that exist under Section 16 have also been deemed controversial, with privacy and civil-liberty groups raising concerns over the ambiguity of its wording.

Reform of RIPA

There has been significant discussion around the use of RIPA and its modern-day applicability to the new types of data being generated (for example, from social media). There have been calls for reform or for redrafting the legislation entirely.

Yet, RIPA is about oversight and preventing intrusions into civil liberties, not technology. It was drafted to be technologically neutral, which has helped to ensure its continued applicability. Even new RIPA legislation would still need to be technologically neutral. Referencing specific technology and communication methods would mean that the legislation becomes quickly outdated and would need constantly revising; it could also overly restrict the state's ability to gather certain types of intelligence. Yet there is also the possibility that critics of RIPA and intelligence agencies' supposed intrusiveness would discover that reform of the legislation would end up strengthening the agencies' powers, rather than diminishing them.

DAMAGE DONE BY SNOWDEN

Changes in target behaviour and communication methods

Snowden's disclosures about the NSA and GCHQ have led to changes in suspects' behaviour, as terrorists and criminals better understand the scope and scale of Western intelligence capacity. For example:

- At least three al-Qaeda affiliates are known to have altered their communication methods.
- Online jihadist platforms released new encryption tools, and at a quicker pace, following the Snowden leaks. According to one analysis, three significant encryption tools were released 'within a three to five month time frame of the leaks'. For example, the *Global Islamic Media Front* released a new mobile-encryption program in September 2013, while the *al-Fajr Technical Committee* has released multiple versions of an encryption program for e-mails; text messages; and instant messages.
- In January 2015, a video was released onto a jihadist platform, outlining what jihadists had learned from the Snowden disclosures. It provided advice that included tips on how to avoid detection and listed software packages that protect against surveillance, as well as where this software could be acquired.
- The Section 702 program was particularly impacted, as foreign terror suspects now not only realised that their communications potentially passed through the US (even if the individuals themselves were not based there); but also which CSPs were allowing the NSA to access these communications. Terror suspects subsequently stopped using these CSPs to send emails or even stopped using electronic communications entirely.

Intelligence sources have attempted to provide an insight into the day-to-day impact that Snowden has had on their work:

- In June 2014, one British intelligence source said that GCHQ's ability to track domestic and foreign crime gangs – including those relating to people trafficking and drugs – had been reduced by approximately 25%.
- In October 2014, a top GCHQ spy tasked with cracking the communications of high-value national-security targets stated that it can take him three times as long to do so now (taking six weeks instead of two).
- By revealing information concerning intelligence-gathering techniques, Snowden has polluted ongoing operations. As they can no longer be run safely, due to fear of discovery and/or attribution, such intelligence gathering has had to stop.
- There is also a fear that hostile states will read and adapt the methodologies that are displayed in the Snowden files: China and Russia, for example, deploying GCHQ's or the NSA's own cyber strategies against them.

Damaging military capabilities

Snowden created digital keys which allowed him to access a wealth of classified data. Considering the contact that he has had with the Russian security service, the FSB, this is an obvious cause of concern. The US government fears that the cyber capabilities of Russian and Chinese intelligence agencies are such that they could have accessed Snowden's files even without his knowledge.

These files are not limited to material relating to communications interception, either; Snowden created digital keys which allowed him into a variety of intelligence and military systems.

- According to the Director of National Intelligence (DNI), of the information that Snowden accessed, approximately 'less than 10 percent has to do with domestic surveillance.'
- General Martin Dempsey, the chairman of the Joint Chiefs of Staff, has also testified that the 'vast majority' of what Snowden accessed was about 'military capabilities, operations, tactics, techniques and procedures.'
- Mike Rogers, former Chairman of the US House of Representatives Permanent Select Committee on Intelligence, has said that 'Snowden's actions are likely to have lethal consequences for our troops in the field.'

Examples of non-domestic surveillance revealed by Snowden:

- The NSA had received permission to spy on groups such as the Muslim Brotherhood.
- The Norwegian Intelligence Service assisted the NSA in collecting intelligence regarding Russian energy policy and military activities.
- The Swedish Defence Radio Establishment works with the NSA, to gain intelligence on Russia.
- The NSA was considering forming an intelligence-sharing partnership with Vietnam.
- GCHQ intended to target Turkish and South African diplomats.
- The location of NSA offices, bases, and analysts across the world.
- US attempts to spy on China and Hong Kong.
- The NSA's interception of then-Russian President Dmitry Medvedev's communications.
- President Obama had asked for a list of potential foreign targets for US cyber attacks.

Damaging relations between Communication Service Providers and the state

Following the Snowden disclosures, a significant divide has emerged between the government and the CSPs, who were outraged at the intelligence agencies' ability to access their data. Furthermore, this created a perception that they had collaborated with the state in allowing them access to their customers' data. According to Brad Smith, the Executive Vice President and General Counsel at *Microsoft*, 'government snooping potentially now constitutes an "advanced persistent threat," alongside sophisticated malware and cyber attacks.'

The backlash in response has been significant. For example, US-based CSPs are now claiming that the UK has no jurisdiction over them and that they are bound by US law. Therefore, if the UK government wants to access content data (for example, e-mails), then it must use the Mutual Legal Assistance Treaty (MLAT) process. This is an unsuitable tool, as it is primarily used in cases where a crime has already been committed, whereas agencies such as the NSA and GCHQ aim to be pre-emptive – disrupting possible criminal activity in the planning stages.

Intelligence officials view the CSP's stance as being unreasonable, as other foreign companies wishing to deliver a service in the UK are obliged to comply with UK law. This was partially why the Data Retention and Investigatory Powers Act (DRIPA) 2014 was introduced, in order to

clarify that CSPs were required to provide data if served with a UK warrant. One senior British intelligence official said that the public would be 'shocked' if it was aware of how little the state could do because of the actions of major technology companies, while GCHQ Director Robert Hannigan has said that some of the CSPs were 'in denial' about the problem.

CSPs' use of ubiquitous encryption has also increased exponentially since Snowden's leaks, meaning that companies are automatically providing encryption for users, rather than the user having to encrypt the data themselves. Hannigan has explained that '[t]echniques for encrypting messages […] which were once the preserve of the most sophisticated criminals or nation states now come as standard'.

Escalation is inevitable, as the NSA and GCHQ step up their efforts to break into these networks. As General Keith Alexander, former NSA Director, has said, '[w]hen the government asks [the] NSA to collect intelligence on terrorist X, and he uses publicly available tools to encode his messages, it is not acceptable for a foreign intelligence agency like [the] NSA to respond, "Sorry we cannot understand what he is saying".'

SELECT CONCLUSIONS

There is no evidence that mass surveillance is taking place

That mass surveillance is occurring is central to Edward Snowden's accusations; yet, it is untrue. US and UK intelligence agencies are not spying on the phone calls of ordinary citizens or brazenly looking at their e-mails; they are legally intercepting communications in order to prevent attacks from terrorists, cyber criminals, and a host of other state and non-state actors. That mass surveillance and bulk collection of communications have become virtually synonyms is regrettable.

State access to data may actually be insufficient, rather than excessive

There is an ongoing problem regarding the UK government's ability to access communications data (the context, i.e. the 'who, when, where and how' of a communication).

Whereas telephone communications and access to the internet traditionally took place via a fixed landline, they now increasingly take place through mobile networks and broadband. This has been accompanied by a flourishing in communications methods: SMS messages, video messaging, instant messaging, Skype, and social-network platforms.

Furthermore, a single telephone line with a single service provider previously needed to monitor who was called; for what duration; and the geographic location, for billing purposes. Yet, increasing numbers of people pay a fixed-price monthly direct debit or, alternatively, a pay-as-you-go fee to their provider. A consequence of this has been that CSPs no longer retain – or, sometimes, even generate – communications data.

This is a concern. Communications data is an invaluable weapon in safeguarding national security and fighting crime – this includes the prevention of child abuse and exploitation (including the prosecution of its perpetrators); identifying and locating suicide risks; identifying rapists, kidnappers, or threatening callers; and murder investigations.

Judicial oversight over every data application is neither the norm nor necessarily effective

The US has a level of judicial oversight in its communications-interception regime, via the FISA Court. The fact that, in the UK, warrants are issued by a Secretary of State rather than a judge has been used to criticise its interception authorisation regime.

However, the extent to which judges and magistrates are better qualified to, for example, approve or reject warrants is highly contentious. Providing judicial oversight is only potentially a positive when there are enough well-trained, high quality magistrates and judges who understand the legislation; so far, this has not been proved to be the case.

Furthermore, applications for warrants may be legally sound – and, therefore, approvable – but politically unwise. Ministers can also assess the political context and wider public interest in a way that judges cannot.

Ultimately, a non-judicial system in which there is accountability and a rigorous approval process is worth more than ill-trained magistrates or judges carrying out the task. This is reflected in the fact that comparable democracies (Canada; Australia; and France, for example) also have relatively minimal judicial involvement in its interception authorisation regime.

Incidental collection of our everyday communications is a new reality

There must be a greater societal acceptance of the risk of incidental collection of everyday communications during the NSA's and GCHQ's intelligence work.

It was previously the case that the infrastructure used for foreign communications was distinct from that used for domestic; however, data streams have now become entangled. Even internal communications may travel via foreign servers and there is no reasonable way for the state to separate what are internal, rather than external, communications when initially scooping this data up. As a result, intelligence agencies on the lookout for foreign communications inevitably end up capturing some belonging to their own citizens.

Sir Iain Lobban, when speaking as GCHQ Director, has commented that '[y]ou can't pick and choose the components of a global interception system that you like (catching terrorists and paedophiles), and those you don't (incidental collection of data at scale): it's one integrated system.' A similar point was made by General Keith Alexander: 'if all the […] bad guys […] would go to one sector of the network, call it badguys.com, then all we would have to do is monitor that area and everybody else's communications would flow freely. But the reality is, they use the same devices we do'.

As long as the correct oversight is in place to ensure that access to this data is not abused – and, so far, there is very little to suggest that it is being – this should not be the cause for concern that some have attempted to portray it as.

Public concern should not be about capacity, but oversight and culture

The NSA's and GCHQ's intelligence-gathering capacities – which are massive – should not be confused with their legal authorities, which are also strong (even in comparison to other Western democracies).

Western citizens are generally happy for the state to have an army with sophisticated weaponry because they know that it will not be misused; there is faith in the culture of the system and that

the checks and balances are sufficient to ensure public safety. This same principle should apply to the weaponry given to our spy agencies.

With this being the case, the questions for the future should not necessarily revolve around the capacity of intelligence agencies. These debates should, instead, be about the people; the culture of the institution; and the systems in place to safeguard privacy.

Intelligence agencies must aspire for translucency, not transparency

States need secrets, for intelligence and military purposes; for criminal investigations; and for a host of other reasons. Yet, they also need public consent, in order to operate with credibility.

The intelligence agencies may have been overly secretive, and some within these agencies do accept the need to be more open with regard to their work. However, even those officials who are receptive to the idea of more transparency warn of an 'irreducible core' of methods that cannot be revealed; that could be quite broad; and which will be defended, by them, to the hilt.

The concept of 'translucency, not transparency' has been suggested by Mike Leiter, the former head of the National Counterterrorism Center. With this, 'you can see through the thick glass. You get the broad outline of the shapes. You get the broad patterns of movements. But you don't get the fine print.' This is a realistic and workable concept by which to balance security and privacy concerns for the future.

This means agencies opening up further than they have in the past and providing greater translucency. Yet, it also means civil society accepting that unalloyed transparency is not always a positive and that there are good reasons for some state secrets.

It's not just a US problem. The UK has a huge dog in this fight. [GCHQ] are worse than the US.

Edward Snowden, June 2013

The conduct of intelligence is premised on the notion that we can do it secretly, and we don't count on it being revealed in the newspaper.

Director of National Intelligence, James Clapper, October 2013

We do not spend our time listening to the telephone calls or reading the e-mail […] of the vast majority. That would not be proportionate, it would not be legal. We do not do it.

Former GCHQ Director, Sir Iain Lobban, November 2013

INTRODUCTION

In the spring of 2013, former National Security Agency (NSA) contractor and Central Intelligence Agency (CIA) employee Edward Snowden used his government security clearance to steal a huge quantity of classified government files. While the exact amount taken is unknown – and, according to recently retired Director of the NSA, General Keith Alexander, unknowable – anywhere between 50,000 and 200,000 of the files are thought to have been passed to journalists.[1]

For Director of National Intelligence (DNI) James Clapper, it was "potentially the most massive and most damaging theft of intelligence information in [US] history",[2] while General Michael Hayden, the former head of both the NSA and the CIA, called it the "most serious haemorrhaging of American secrets in the history of American espionage".[3] For the UK, at least 58,000 documents relating to its Government Communications Headquarters (GCHQ) were stolen.[4]

Stories emerged, in the press, of intelligence agencies tapping fibre-optic cables containing telephone and internet traffic;[5] carrying out alleged "warrantless" surveillance;[6] monitoring phone calls made by foreign leaders;[7] and intercepting, then storing, webcam images.[8] In terms of national security; diplomacy; privacy perceptions; media–state relations; citizens' trust in government; technology company–state relations; and many other ways, Snowden's actions have had a profound impact. This impact continues to unfold today, in a variety of ways that are, arguably, still yet to be fully understood. As Sir John Sawers, the former head of MI6, said in January 2015, "Snowden threw a massive rock in the pool and the ripples haven't stopped yet".[9]

Snowden claimed that he stole the files because he wanted to "inform the public as to that which is done in their name and that which is done against them";[10] he generated support from sections of the public, the political class, the media, the arts, and from NGOs by doing so. He also succeeded in gaining enormous amounts of media coverage: 26 million blogs and news articles mentioned him in the year after he stole the documents.[11]

1. 'The Snowden Saga: A Shadowland of Secrets and Light', *Vanity Fair*, May 2014, available at: http://www.vanityfair.com/politics/2014/05/edward-snowden-politics-interview, last visited: 16 March 2015.

2. 'Remarks as Delivered by James R. Clapper, Director of National Intelligence', Office of the Director of National Intelligence Public Affairs Office (2014), available at: http://www.dni.gov/files/documents/WWTA%20Opening%20Remarks%20as%20Delivered%20to%20SASC_11_Feb_2014.pdf, last visited: 16 March 2015.

3. 'Former NSA Director: Snowden a "Traitor" Engaged in "Treason"', *National Review*, 29 December 2013, available at: http://www.nationalreview.com/corner/367154/former-nsa-director-snowden-traitor-engaged-treason-andrew-stiles, last visited: 16 March 2015.

4. 'GCHQ leaks have "gifted" terrorists ability to attack "at will", warns spy chief', *The Telegraph*, 9 October 2013, available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10365026/GCHQ-leaks-have-gifted-terrorists-ability-to-attack-at-will-warns-spy-chief.html, last visited: 16 March 2015.

5. 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013, available at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, last visited: 16 March 2015.

6. 'NSA loophole allows warrantless search for US citizens' emails and phone calls', *The Guardian*, 9 August 2013, available at: http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls, last visited: 16 March 2015.

7. 'NSA monitored calls of 35 world leaders after US official handed over contacts', *The Guardian*, 25 October 2013, available at: http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls, last visited: 16 March 2015.

8. 'Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ', *The Guardian*, 28 February 2014, available at: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo, last visited: 16 March 2015.

9. 'Ex-MI6 chief: Government and tech firms must agree spy pact', *BBC News*, 20 January 2015, available at: http://www.bbc.co.uk/news/uk-30898859, last visited: 28 April 2015.

10. 'Edward Snowden: the whistleblower behind the NSA surveillance revelations', *The Guardian*, 11 June 2013, available at: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, last visited: 16 March 2015.

11. 'The National Security Agency Debate: The International Implications – Panel One', *The Brookings Institution*, 4 June 2014, available at: http://www.brookings.edu/events/2014/06/04-international-implications-nsa-leaks#/full-event/, last visited: 16 March 2015.

Despite the support that Snowden received from certain sections of society, the expectation remains that intelligence agencies should stop terrorist attacks and serious crimes.[12] Yet, at the same time, there are calls for them to reform and be more transparent in order to rebuild trust. The intelligence agencies are in a particularly unenviable position: asked to be less intrusive; more transparent; and yet, just as effective.

This report explores this and related questions. It studies the programmes used by the NSA and GCHQ that caused such controversy; the laws that govern them; the adequacy of their oversight; the impact that their existence being revealed has had, particularly with regard to national security; the lessons that could be learned; and the issues which we must consider for the future.

12. For example, see some of the fallout to either the Boston-marathon bombings in April 2013, or extremists stabbing a soldier to death in London in May 2013: 'The Boston Bombing Intelligence Failure', *The Daily Beast*, 16 April 2013, available at: http://www.thedailybeast.com/articles/2013/04/16/the-boston-bombing-intelligence-failure.html; see also: 'Boston bombing investigation reveals intelligence failures', *The Washington Times*, 23 April 2013, available at: http://www.washingtontimes.com/news/2013/apr/23/boston-bombing-investigation-reveals-intelligence-/?page=all; see also: 'Woolwich attack: why was suspect Michael Adebolajo free to kill?', *The Telegraph*, 23 May 2013, available at: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10077439/Woolwich-attack-why-was-suspect-Michael-Adebolajo-free-to-kill.html; see also: 'Could MI5 have stopped Lee Rigby's murder?', *The Guardian*, 19 December 2013, available at: http://www.theguardian.com/uk-news/2013/dec/19/mi5-lee-rigby-murder-adebolajo-adebowale, last visited: 16 March 2015.

1. UNITED STATES

1.1 FISA SECTION 702

Section 702 of the Foreign Intelligence Surveillance Act (FISA) governs the interception of communications of foreign nationals based outside the US, for the specific purpose of acquiring foreign intelligence information relating to national security; foreign affairs; and national defence. This includes a focus on terrorism, espionage, and the proliferation of weapons of mass destruction.[13]

Under Section 702, the government provides Communication Service Providers (CSPs) – such as *Google*, *Yahoo!*, *Microsoft*, and *Facebook* –[14] with "selectors" (for example, telephone numbers or e-mail addresses) and compels them to acquire communications on its behalf.[15]

The NSA has stated that collection which occurs under Section 702 "is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the US and around the world."[16]

1.1.1 ORIGINS

Section 702's origins lie in the Terrorist Surveillance Program (TSP), formulated after al-Qaeda's attacks against the US on 11 September 2001. The TSP enabled the NSA to intercept foreign nationals' communications, if they were of suspected intelligence value and the nationals were located abroad (or "reasonably" suspected of being abroad at the point that their communication was intercepted).[17]

Under a Presidential authorisation which stated that an extraordinary emergency existed due to the ongoing terrorist threat, the TSP also permitted this electronic surveillance to be carried out without a warrant or court order, for a "limited" number of days, within the US – as long as there was a counterterrorism purpose.[18]

President George W. Bush renewed the authorisation for these activities (with certain modifications) approximately every one to two months, until 2007. After this, the government

13. Wolf, C., 'A Transnational Perspective on Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), available at: http://justsecurity.org/wp-content/uploads/2014/03/WOLF_PLCOB_MARCH_19_2014.pdf, last visited: 15 April 2015, p. 4.

14. In this report, CSPs are defined as companies that provide a service enabling information to be transported electronically. This is a definition based upon the UK government's understanding, as outlined in: 'Report on the intelligence relating to the murder of Fusilier Lee Rigby', Intelligence and Security Committee of Parliament (2014), available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20141125_ISC_Woolwich_Report%28website%29.pdf?attachauth=ANoY7coPsmsYBsohDx6GEBHVPN14pxhz-7zh7WpAwl3EI5G_2YktHoSEjGxeNYt7NFnj-J05rHzx2yv89yLxPx3btgYIGCWO8QMlg9skpT4RejnBolN1y3_R96m-ciPujOWMHztAzLy2KnnP9nK4766gbdNqEfIcKmt8-hIz4I6R3ewe4CdY7m77U5G73-SG7nkqNw9VneDpGbW77-pTY9Md7vyPcE67soajvbTyW4fQ3fI786Xd-QdR3d_schZGVNeKVwU_5BHF&attredirects=0, last visited: 16 March 2015, p. 139.

15. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), available at: http://www.wired.com/wp-content/uploads/2014/07/PCLOB-Section-702-Report-PRE-RELEASE.pdf, last visited: 16 March 2015, p. 7.

16. 'The National Security Agency: Missions, Authorities, Oversight and Partnerships', National Security Agency (2013), available at: https://www.nsa.gov/PUBLIC_INFO/_FILES/SPEECHES_TESTIMONIES/2013_08_09_THE_NSA_STORY.PDF, last visited: 16 March 2015, p. 4.

17. 'Title VII, Section 702 of the Foreign Intelligence Surveillance Act (FISA), "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons" (50 U.S.C. sec. 1881a)', available at: https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf; see also: 'Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Director of National Intelligence (2013), available at: http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf, last visited: 16 March 2015.

18. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 16.

sought authorisation from the Foreign Intelligence Surveillance Court (FISC, or FISA Court), a secret intelligence court which consists of 11 federal judges.[19] In January 2007, FISC authorised electronic surveillance of telephone and internet communications, provided that the government had, for example, "probable cause" regarding the activities of one of the communicants and the telephone numbers and e-mail addresses involved were reasonably suspected of being used by someone located outside the US.[20] [21] This was altered in May 2007, when another FISC judge ruled that the 'probable cause' determination needed to take place in court, rather than be decided by the government (although it could still add new e-mail addresses and telephone numbers of interest, without requiring a court order).[22]

The government was also using FISA to obtain court orders compelling private companies to acquire the communications of foreign terror suspects using US CSPs.[23] These court orders were predicated on probable cause; however, difficulties in meeting this probable-cause standard led to a degradation in acquiring foreign intelligence communications.[24] Following concerns in the Bush administration over this, it was proposed, in spring 2007, that FISA be modified. Therefore, in August of that year, Congress enacted the Protect America Act of 2007.[25] Among the measures that this introduced was the removal of the need for the government to seek individual court orders showing probable cause. The Protect America Act was eventually replaced with the Congress-approved FISA Amendments Act of 2008, which placed the programme on a longer-term statutory footing. Section 702 was among the provisions enacted in the amendments.

The Attorney General and DNI approve yearly certifications which give authorisation to target foreign intelligence information without specifying to the FISA Court a specific, named individual to be targeted.[26] Instead of having to show probable cause, Section 702 certifications must collect intelligence regarding certain issues: such as international terrorism and the acquisition of weapons of mass destruction.[27]

A reform introduced in 2015 states that the NSA must now produce a written statement showing that a query is "reasonably likely" to produce foreign intelligence.[28]

1.1.2 ACQUISITION

There are two separate types of data acquisition that take place under Section 702 authority: PRISM collection and Upstream collection.

PRISM

PRISM collection takes place with the compelled assistance of CSPs, from whom it can capture

19. Ibid., p. 16.

20. Defined as probable cause that the target of the surveillance is a foreign power or an agent of a foreign power (including international terrorist groups such as al-Qaeda), and that "minimization" procedures – i.e. that these queries are "reasonably likely to return foreign intelligence information" – are met (Ibid., pp. 8 & 24).

21. Ibid., p. 17.

22. Ibid., pp. 17-18.

23. Ibid., p. 18.

24. Ibid.

25. Ibid., p. 19.

26. Ibid., p. 6.

27. Ibid.

28. 'New Privacy Protections for Information Collected under Section 702', *Office of the Director of National Intelligence*, 2015, available at: http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#section-702, last visited: 16 March 2015.

the content of e-mails and instant messages.[29] This collection is carried out when the NSA sends a 'selector' (for example, an e-mail address) to a CSP. This CSP is required to provide communications sent to or from this 'selector' back to the NSA. Parts can also be disseminated to the CIA and Federal Bureau of Investigation (FBI);[30] the UK government has also confirmed that GCHQ has received intelligence via PRISM.[31]

The data and content collected under Section 702, via PRISM, can be stored for up to five years.[32]

How PRISM can work in practice

The NSA discovers that a foreign national based outside the US uses a US CSP e-mail address (for example, a *Google Mail* account) to contact his associates about a planned terrorist attack. The NSA would request that this e-mail address be queried, under Section 702 authority. The FBI would then contact *Google* and compel it to provide all communications from this *Google Mail* account. The NSA would receive all data collected via PRISM, and a copy of the raw data could be sent to the CIA and/or FBI.[33]

Upstream

Upstream collection refers to the NSA tapping into the underwater fibre-optic cable networks (also referred to as "the Internet backbone")[34] that carry telephone and internet data into and out of the US.[35] This type of collection is done under FISA and takes place as communications flow between CSPs.[36]

Raw upstream collection cannot be shared with the CIA or FBI and is retained by the NSA;[37] the data can be stored for up to two years.[38] Approximately 9% of the e-mails that the NSA obtains occur via upstream collection.[39] According to Rajesh De, former General Counsel at the NSA, "upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection."[40]

How Upstream collection can work in practice

With telephony collection, the NSA discovers that a foreign national, reasonably thought to be based outside the US, is using a certain telephone line to contact his associates about a planned

29. 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', *The Washington Post*, 7 June 2013, available at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, last visited: 16 March 2015.

30. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 7.

31. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), available at: https://www.privacyinternational.org/sites/default/files/Witness%20st%20of%20Charles%20Blandford%20Farr_0.pdf, last visited: 16 March 2015, p. 13.

32. 'NSA's Implementation of Foreign Intelligence Surveillance Act Section 702', NSA Director of Civil Liberties and Privacy Office (2014), available at: http://fas.org/irp/nsa/clpo-702.pdf, last visited: 16 March 2015, p. 8.

33. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), pp. 33-34.

34. Ibid., p. 37.

35. Ibid., p. 35.

36. Ibid.; see also: 'NSA collected 56,000 emails by Americans a year: documents', *Reuters*, 22 August 2013, available at: http://uk.reuters.com/article/2013/08/22/us-usa-security-nsa-idUSBRE97K14Y20130822, last visited: 16 March 2015.

37. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 7.

38. 'NSA's Implementation of Foreign Intelligence Surveillance Act Section 702', NSA Director of Civil Liberties and Privacy Office (2014), p. 8.

39. 'NSA collected 56,000 emails by Americans a year: documents', *Reuters*, 22 August 2013.

40. 'Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), available at: http://www.pclob.gov/library/20140319-Transcript.pdf, last visited: 16 March 2015, p. 26.

terrorism attack. The NSA sends – under a Section 702 certification – this phone number to a US CSP, which is compelled to provide telephone communications from or to that particular number.[41]

With Internet collection, the NSA targets foreign nationals by tasking specific 'selectors' (i.e. e-mail addresses) and compels CSPs to intercept communications transiting through internet fibre-optic cable networks.

Upstream collection acquires information concerning the 'to' and 'from' communications (i.e. as the sender or recipient will have been targeted under Section 702, this potentially means all e-mails sent from a specific account and all the e-mails that it has received). However, it can also concern the 'about', which means capturing a communication in which the 'selector' is referenced but is not a participant in either end of the communication (for example, a targeted e-mail address referred to in the body of an intercepted e-mail message).[42]

1.1.3 WHO IS TARGETED?

The Section 702 programme is aimed at foreign nationals; no US citizen or anyone known to be in the US can be intentionally targeted.[43] The NSA is also not allowed to 'reverse target': namely, target a foreign national based outside the US in order to gather intelligence on an individual known to be based in the US.[44]

However, incidental collection of US citizens' communications occurs as part of the process of acquiring actual targeted communications, as it is not feasible to initially separate out the two. It is possible that a US citizens' communications will be swept up while carrying out legitimate collection on a foreign intelligence target: for example, if an al-Qaeda leader in Pakistan was contacting a US citizen.[45] (There are, though, "extensive procedures, specifically approved by the [FISA] court", in place, to "minimize the acquisition, retention and dissemination of incidentally acquired information about US persons."[46])

If evidence of a possible crime is discovered, the NSA is able to disseminate this information to federal law enforcement.[47] The NSA may also inform the FBI if a target enters the US – enabling it (the FBI) to carry out electronic surveillance, for example.[48] A reform introduced in 2015 stated that evidence acquired this way could not be introduced as evidence in court unless it had approval from the Attorney General or was related to a serious crime or national-security issue.[49]

Section 702 collection does not occur in bulk. The Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the Executive Branch, concluded that the Section 702 programme "consists entirely of targeting specific persons" – the definition of which the PCLOB accepts is as broad as "corporations, associations, and entities as well as individuals" – and that

41. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 36.

42. Ibid., p. 37.

43. 'Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Director of National Intelligence (2013).

44. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 23.

45. 'Section 702 of the Foreign Intelligence Surveillance Act', *Office of the Director of National Intelligence*, available at: http://icontherecord.tumblr.com/topics/section-702, last visited: 26 April 2015.

46. Ibid.

47. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 63.

48. Ibid., p. 50.

49. 'New Privacy Protections for Information Collected under Section 702', *Office of the Director of National Intelligence*, 2015.

the government "acquires only those communications involving [a] particular selector", such as a telephone number or e-mail address.[50]

A NOTE ON TERRORISM AND THE INTERNET

In November 2013, Sir Iain Lobban, former Director of GCHQ, commented that the internet had facilitated "a myriad of ways to communicate covertly. It gives [terrorists] a platform, to fund-raise, to radicalise, to spread propaganda. It gives them the means to plan, to command and control, to spread lethal ideas, to exhort violence."[51] The scale of tracking this type of threat is enormous. In a single year, 2.4 trillion e-mails are sent (with more sent in four days than letters are delivered in a whole year), as are 160 billion instant messages; 145 billion text messages; and 1 billion 'tweets'. A further 70 billion *Facebook* views and 23 billion *Google* searches take place,[52] and over 100 hours of video are uploaded to *YouTube* every minute.[53]

Many of its early users hoped that the internet would be a space free from government control; yet, as Sir Iain Lobban has said, "[f]rom what we know of ungoverned spaces in the real world, do we really believe that the world would be a better place if the internet becomes an ungoverned space where anybody can act freely with impunity?"[54]

1.1.4 SECTION 702 CONTROVERSIES

The controversy that existed around Section 702 and the type of collection that occurs under its authority revolved around the facts that:

(a) US citizens' communications incidentally picked up while intercepting foreign communications could be stored. One former official, speaking to *The New York Times* stated, 'This is really a sea change […] It's almost a mainstay of this country that the N.S.A. only does foreign searches."[55]

(b) Collection took place without obtaining a FISA Court warrant against a specific individual; rather, it occurred under a broader warrant enabling collection to take place regarding certain foreign-intelligence topics.

It had been speculated that the lack of a warrant against a specific individual during Section 702 collection would make the programme unconstitutional;[56] however, the PCLOB came to a "unanimous bottom-line conclusion that the core Section 702 program is clearly authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective

50. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 111.

51. 'Uncorrected Transcript of Evidence Given by Sir Iain Lobban, Director, Government Communication Headquarters; Mr Andrew Parker, Director General, Security Service; Sir John Sawers, Chief, Secret Intelligence Service', Intelligence and Security Committee of Parliament (2013), available at: www.globalsecurity.org/intell/library/reports/2013/20131107_isc_uncorrected_transcript.pdf, last visited: 16 March 2015.

52. Clegg, N., 'Security and privacy in the internet age', *UK Government*, 4 March 2014, available at: https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age, last visited: 16 March 2015.

53. 'Report on the intelligence relating to the murder of Fusilier Lee Rigby', Intelligence and Security Committee of Parliament (2014), p. 144.

54. Lobban, I., 'Sir Iain Lobban's valedictory speech - as delivered', *Government Communications Headquarters*, 21 October 2014, available at: http://www.gchq.gov.uk/press_and_media/speeches/Pages/Iain-Lobban-valedictory-speech-as-delivered.aspx, last visited: 16 March 2015.

55. 'Bush Lets U.S. Spy on Callers Without Courts', *The New York Times*, 28 December 2005, available at: http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all, last visited: 16 March 2015.

56. 'Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs', Brennan Center for Justice at New York University School of Law (2013), available at: http://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, last visited: 16 March 2015.

intelligence tool."[57] Similarly, PRISM collection was described as "clearly authorized" under Section 702.[58]

General Hayden has cast doubt on the impact of PRISM on the public debate; he said that the use of PRISM was "softball" and did not "incur much of a ripple in the United States at all."[59]

1.1.5 WHO PROVIDES OVERSIGHT?

The Executive

The Executive's independent inspectors general provide oversight for the Section 702 legislation.[60] In addition, every 60 days (at minimum), the Department of Justice (DoJ) and the Office of the Director of National Intelligence (ODNI) perform on-site reviews of the NSA's "targeting, minimization, and dissemination" procedures.[61]

The Legislature

The DNI and the Attorney General provide Congress with reports on the programme and with FISA Court opinions twice a year. The reports include directives issued under Section 702 (and details of the judicial review of these) and a description of any incidents of non-compliance. The Senate's and House of Representatives' Committees on Intelligence and on the Judiciary are also given briefings on the programme.[62]

The Judiciary

Section 702 collection is carried out with FISA Court approval. The targeting procedures are subject to judicial review by the Court, though individual targeting decisions are not (instead being covered by the DoJ and ODNI reviews).[63]

The FISA Court has been criticised for "rubber stamping" government requests to carry out electronic surveillance.[64] For example, in 2013, the government made 1,588 such applications for authority; all were approved, with only 34 of them being subjected to modifications to the original application. It had similar success in previous years.[65] However, this accusation has been rejected by some officials. Carrie Cordero, a former DoJ official, has said:

> The FISC is not at all the rubber stamp it has been periodically purported to be. The judges, after all, are sitting federal court judges, and any prosecutor or defense attorney will

57. 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 15.

58. Ibid., p. 9.

59. 'Getting Counterterrorism Right: A Transatlantic Conversation', *The Henry Jackson Society*, 30 September 2013, available at: http://henryjacksonsociety.org/2013/09/30/getting-counterterrorism-right-a-transatlantic-conversation/, last visited: 16 March 2015.

60. 'Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Director of National Intelligence (2013).

61. 'Title VII, Section 702 of the Foreign Intelligence Surveillance Act (FISA), "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons" (50 U.S.C. sec. 1881a)'.

62. 'An Act to amend the Foreign Intelligence Surveillance Act of 1978 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes', *The Senate of the United States*, 20 June 2008, available at: http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304pcs/html/BILLS-110hr6304pcs.htm, last visited: 16 March 2015; see also: 'Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Director of National Intelligence (2013).

63. 'Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Director of National Intelligence (2013); see also: 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), pp. 41-42.

64. 'The US Surveillance Court Hasn't Turned Down an NSA Request This Decade', *Motherboard*, 1 May 2014, available at: http://motherboard.vice.com/en_uk/read/the-us-surveillance-court-hasnt-turned-down-an-nsa-request-this-decade.

65. Ibid.

> tell you that federal district court judges do not hesitate to demand information, accuracy and explanation when needed. FISC judges do not abandon their judicial sensibilities and responsibilities when they sit on the FISC. They bring all of their attention, consideration, and exacting requirements to their meaningful role on the Court.[66]

General Alexander has described them in a similar way:

> I'm on the other end of that table with federal judges […] They want to make sure that what we're doing comports with the Constitution and the law. And they are dead serious on it. […] These are tremendous judges […] I've been in front of that court a number of times. I can tell you from the wirebrushings that I received, they are not a rubber stamp.[67]

The success that the government has had in obtaining approval from the FISA Court is likely down to familiarity with the process and what it is possible to achieve approval for, rather than court subservience. This is certainly the case in the UK, where a Secretary of State would not be asked to even consider an application until government lawyers are satisfied that it has met legal requirements.[68]

NSA VIOLATIONS

The NSA violated privacy rules 2,776 times during its surveillance activities between April 2011 and March 2012.[69] These violations included mistyping (for example, of a phone number or e-mail address) and capturing communications of a foreign national who had physically moved his or her location (for example, being temporarily based in the US and therefore protected by the Fourth Amendment – prohibition of unreasonable search and seizure – for that period).[70] When these violations were flagged up, the collection was stopped. Any data gained during the period in which the violation took place was deleted,[71] and none of the violations were known to be deliberate.[72]

There are concerns that such an issue arose in the first place, and that noticing it relied on the goodwill of the agency that was carrying out the wrongdoing. Yet, as Benjamin Wittes, a senior fellow at the *Brookings Institution* has said, "when nobody was watching, the NSA caught big mistakes, reported them and had a significant dialogue with the FISA […] Court on fixing them. The process is not perfect, but it has integrity".[73]

66. 'Carrie Cordero on FISA Court Lessons for a "Drone Court"', *Lawfare*, 18 February 2013, available at: http://www.lawfareblog.com/2013/02/carrie-cordero-on-fisa-court-lessons-for-a-drone-court/, last visited: 16 March 2015.

67. 'Keynote Address by General Keith Alexander, Director, National Security Agency, Black Hat USA 2013', National Security Agency (2013), available at: https://www.nsa.gov/public_info/_files/speeches_testimonies/transcript_of_gen_alexanders_black_hat_speech_31_july_2013.pdf, last visited: 16 March 2015.

68. 'Privacy and Security: A modern and transparent legal framework', Intelligence and Security Committee of Parliament (2015), available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cqWvcEzQ7y1Qdd0x3WSJnUZAXqijMAiAx6selwrLrLm2vi7cvRR6ARNHvcsynQLZyCH2YjSs57zvR_t6CTIj8dr0tXHEPh0lvb9P4N3RlfyCY0SamIMkDfUSrZZlQtUW5255EJszpyn0xA9f-j7ELy_cXHA-FHCoDF94696JgVuWHh4KfNcT0W04rik1k2VwbnmQxRLercxuwwveT-isQ335_xjWKlXcbZvPNTlcj6N6e_KPWz7Ucl9cKz5h8h-2-FHZ4Gk&attredirects=0, last visited: 23 March 2015, p. 74.

69. 'NSA broke privacy rules thousands of times per year, audit finds', *The Washington Post*, 15 August 2013, available at: http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html, last visited: 16 March 2015.

70. Hayden, M., 'Put NSA "violations" in proper context: Opposing view', *USA Today*, 18 August 2013, available at: http://www.usatoday.com/story/opinion/2013/08/18/nsa-privacy-surveillance-editorials-debates/2669479/; see also: Herman A. and John Yoo, 'A Defense of Bulk Surveillance', *National Review*, 7 April 2014, available at: https://www.nationalreview.com/nrd/articles/373789/defense-bulk-surveillance, last visited: 16 March 2015.

71. 'Transcript: NSA Deputy Director John Inglis', *NPR*, 10 January 2014.

72. 'General Keith Alexander Speaks at AFCEA's Conference', National Security Agency (2013), available at: http://www.nsa.gov/public_info/_files/speeches_testimonies/Transcript_of_GEN_Alexanders_AFCEA_Keynote_Speech_27_June_2013.pdf, last visited: 16 March 2015.

73. Cohen, M., 'The real NSA scandal is overseas', *Yahoo! News*, 4 June 2014, available at: http://news.yahoo.com/the-real-nsa-scandal--spying-overseas-210655092.html, last visited: 16 March 2015.

One instance of this occurred in 2011, when the NSA uncovered a technological problem meaning that it was retaining an unnecessary volume of communications – for example, a screenshot of e-mails on a web page, even if only one message was being sought. It subsequently reported this to FISC, leading to the court ruling that its Section 702 collection was "in some respects, deficient on statutory and constitutional grounds."[74] This ruling meant that, between 2008 and 2011, the NSA was not taking sufficient steps to protect the privacy of its incidentally collected domestic communications. The NSA subsequently created a new way of handling the internet traffic that enhanced the protections afforded to American citizens.[75]

1.2 BULK METADATA COLLECTION & SECTION 215

The bulk collection of metadata from telephony and internet communications,[76] authorised under Section 215 of the PATRIOT Act, has its roots in the terrorist attacks of 11 September 2001. The US government now only collects telephony metadata. This relates to the date and time of the call, its duration, the calling number, and the number that has been dialled; it does not include the content of calls, subscriber information, or the geographical location of the caller.[77] The metadata is taken from CSPs and contained in a "virtual lockbox" operated by the NSA.[78] As President Obama acknowledged, this was the programme that caused the most domestic controversy following Snowden's leaks.[79]

1.2.1 ORIGINS

Three days after the 9/11 attacks, the then-NSA Director, General Michael Hayden, approved the targeting of "terrorist-associated" overseas telephone numbers.[80] This collection was pertaining to communication between the US and countries where terrorists were known to operate. Only specific and pre-approved numbers could have their data collected and checked against links originating in the US. By 26 September, this had been broadened so that any Afghan phone number in contact with a US phone number was, from then on, "presumed to be of foreign intelligence value" and could be passed to the FBI.[81]

The NSA undertook these activities under Executive Order (EO) 12333, which concerns foreign-intelligence gathering that is not governed by FISA (for more information, see pages 36-38).[82] This was because targeting e-mail accounts hosted on a US webmail server and belonging to non-US-based foreign nationals required a FISA Court order (the approval process for which could take between four and six weeks or – with an emergency FISA Court order – on average, a day and a half). Along with the volume of terrorist suspects using e-mails, and the regularity with which they

74. 'Memorandum Opinion', United States Foreign Intelligence Surveillance Court, available at: http://fas.org/irp/agency/doj/fisa/fisc0912.pdf, last visited: 16 March 2015, p. 27.

75. 'Secret Court Faulted NSA for Collecting Domestic Data', *The Wall Street Journal*, 21 August 2013, available at: http://online.wsj.com/articles/SB10001424127887323665504579027180087675564, last visited: 16 March 2015.

76. The field of Library and Information Science defines 'metadata' as "data about data" (see: Acker, A., 'Why the definition of "Metadata" matters to the NSA phone record collection', *HASTAC*, 11 June 2013, available at: http://www.hastac.org/blogs/amelia-acker/2013/06/11/why-definition-%E2%80%9Cmetadata%E2%80%9D-matters-nsa-phone-record-collection, last visited: 16 March 2015).

77. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 9 May 2014, available at: http://www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140508-itzhw, last visited: 26 March 2015.

78. 'General Keith Alexander Speaks at AFCEA's Conference', National Security Agency (2013).

79. 'Remarks by the President on Review of Signals Intelligence', *The White House – Office of the Press Secretary*, 17 January 2014, available at: http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence, last visited: 16 March 2015.

80. 'ST-09-0002 Working Draft', Office of the Inspector General (2009), available at: http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection, last visited: 16 March 2015, p. 5.

81. Ibid.

82. Ibid., p. 3.

changed their phone numbers or e-mail addresses, the existing FISA authorisation was seen to be not allowing sufficient flexibility;[83] yet, early efforts to amend it stalled.[84]

Therefore, on 4 October 2001, President Bush issued a Presidential Authorization for "Specified Electronic Surveillance Activities during a Limited Period to Detect and Prevent Acts of Terrorism within the United States".[85] This would become known as the 'President's Surveillance Program' (PSP), and the data collected in it: a security compartment named 'Stellar Wind.[86] The legality of the programme was approved by the Attorney General and the DoJ's Office of Legal Counsel (OLC) – whose Deputy Assistant Attorney General, John Yoo, would write the initial legal memoranda in support of the PSP.[87]

The NSA was now able to acquire, retain, and store content and metadata from telephony and internet communications if there was "probable cause" to believe either that (a) at least one end of the communication came from abroad,[88] or (b) a communicant was "engaged in or preparing for acts of international terrorism."[89] These conditions therefore allowed for the collection of US citizens' data if their communications involved a communicant outside the US, or one not known to be a US citizen.[90]

This was a significant change. Previously, the NSA did not have the legal authority to collect communications if one end was based in the US;[91] it could now do so without a judicial warrant or a court order.[92] The metadata collected, though, could only be queried if there was a "reasonable suspicion" that the individual whose records were being checked was connected to certain foreign terrorist groups.[93]

In October 2001, the PATRIOT Act was passed. Section 215 of the PATRIOT Act amended Title V, Section 501 of FISA ('Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations' (50 U.S.C. § 1861)). Section 215 allowed the government to obtain a FISA Court order which would require third-party companies to provide records relevant to international-terrorism investigations.[94] The use of such a power is not unusual in an array of domestic investigations, with prosecutors usually able to gain business records via a subpoena;[95] yet, prior to the Section 215 amendment, national-security officials were restricted in their abilities to investigate the activities of foreign suspects on US soil. Even if they could get a court order

83. Ibid., pp. 5-6.

84. Ibid., p. 6.

85. Ibid., p. 3.

86. Ibid., pp. 3 & 10.

87. '(U) Unclassified Report on the President's Surveillance Program', Offices of Inspectors General of the Department of Defense; Department of Justice; Central Intelligence Agency; National Security Agency; Office of the Director of National Intelligence (2009), available at: https://www.fas.org/irp/eprint/psp.pdf, last visited: 16 March 2015, pp. 7 & 11.

88. There was initially a provision limiting this collection to Afghanistan; but this was dropped in January 2002, when the Taliban was perceived as having been expelled from power.

89. 'ST-09-0002 Working Draft', Office of the Inspector General (2009), p. 8.

90. Ibid.

91. Ibid., p. 13.

92. 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Privacy and Civil Liberties Oversight Board (2014), available at: http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf, last visited: 16 March 2015, p. 37.

93. 'Section 215 of the USA PATRIOT Act of 2001, which amended Title V, Section 501 of the Foreign Intelligence Surveillance Act (FISA), "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations" (50 U.S.C. sec. 1861)', available at: http://fas.org/irp/news/2013/06/nsa-sect215.pdf, last visited: 16 March 2015.

94. 'Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs', Brennan Center for Justice at New York University School of Law (2013).

95. McNeill, J. and Charles Stimson, 'Letting PATRIOT Act Provisions Expire Would Be Irresponsible', *The Heritage Foundation*, 9 February 2011, available at: http://www.heritage.org/research/reports/2011/02/letting-patriot-act-provisions-expire-would-be-irresponsible, last visited: 16 March 2015.

to do so, they could only access records from businesses registered as a "common carrier, public accommodation facility, physical storage facility or vehicle rental facility".[96] According to Kenneth L. Wainstein, former Homeland Security Advisor to President Bush:

> Section 215 authorized the FISA Court to issue orders for the production of the same kind of records and other tangible things that [domestic] law enforcement officers and prosecutors have historically been authorized to acquire through grand jury subpoenas […Before,] it was easier for prosecutors to secure records in a simple assault prosecution than for national security investigators to obtain records that may help prevent the next 9/11.[97]

In 2003, the OLC began a reassessment of the legal foundations for the PSP. In March 2004, it found that the internet metadata component was prohibited.[98] In July 2004, the FISA Court approved the collection of internet metadata if it travelled through particular communication channels likely to contain messages related to a counterterrorism purpose (the collection was terminated in 2011, with the NSA deciding that it was only of limited value).[99] Gradually, what were previously programmes only operating under the authority of the President were brought into the remit of the FISA Court.[100]

1.2.2 WHY IS TELEPHONY METADATA COLLECTED UNDER SECTION 215 POTENTIALLY USEFUL?

The state's collection of metadata – for example, a telephone number – is a vital component in the fight against terrorism. According to one former intelligence official, "[i]n every major terrorist operation or capture operation, metadata has played a huge role."[101]

Regarding the use of Section 215 specifically, to collect metadata, this is essentially about government agencies being able to "connect the dots" for potential terrorist plots with both a foreign and domestic component.[102] General Keith Alexander has said that "[t]he metadata queries are all about the foreign intelligence nexus. So we're trying to find out if there are terrorists amongst us, and if so, we give that data to the FBI."[103] The US House of Representatives Permanent Select Committee on Intelligence explained that Section 215 helped "connect the dots between foreign terrorists and domestic operatives […] This program is specifically focused on detecting terrorist

96. Wainstein, K., 'Statement of Kenneth L. Wainstein, Partner, O'Melveny & Myers LLP, Before the Subcommittee on the Constitution, Civil Rights and Civil Liberties Committee on the Judiciary, House Of Representatives, Concerning the USA PATRIOT Act Sections 206 and 215 and the "Lone Wolf" Provision of the Intelligence Reform and Terrorism Prevention Act of 2004', Committee on the Judiciary (2009), available at: http://judiciary.house.gov/_files/hearings/pdf/Wainstein090922.pdf, last visited: 16 March 2015, p. 4.

97. Ibid., p. 3.

98. 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Privacy and Civil Liberties Oversight Board (2014), p. 38. This led to a huge amount of infighting within the Bush administration, and almost to the resignation of the head of the Department of Justice's Office of Legal Counsel (OLC); the Director of the FBI; and the Deputy Attorney General. All were prepared to quit, in response to the White House threatening that the President would re-authorise the programme despite the new OLC assessment that the e-mail-metadata part of the programme was legally unsupportable (see: Baker, P., *Days of Fire: Bush and Cheney in the White House* (Anchor, 2014), pp. 315-319).

99. Ibid., p. 40; see also: 'DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001', *Office of the Director of National Intelligence*, 21 December 2013, available at: http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001, last visited: 16 March 2015.

100. '(U) Unclassified Report on the President's Surveillance Program', Offices of Inspectors General of the Department of Defense; Department of Justice; Central Intelligence Agency; National Security Agency; Office of the Director of National Intelligence (2009), p. 30.

101. 'Phones Leave a Telltale Trail', *The Wall Street Journal*, 15 June 2013, available at: http://www.wsj.com/articles/SB10001424127887324049504578545352803220058, last visited: 13 April 2015.

102. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 9 May 2014.

103. Ibid.

plots that cross the seam between foreign terrorist organizations and the US homeland."[104]

The speed with which this can be done under Section 215 is also of relevance, being explained by President Obama in the following way:

> [Section 215] was designed to map the communications of terrorists so we can see who they may be in contact with as quickly as possible […] if a bomb goes off in one of our cities and law enforcement is racing to determine whether a network is poised to conduct additional attacks, time is of the essence.[105]

1.2.3 WHY DOES COLLECTION NEED TO TAKE PLACE IN BULK?

Metadata collection is only effective if done in bulk. The US House of Representatives Permanent Select Committee on Intelligence described it thus:

> [Y]ou are looking for a needle, in this case a number, in a haystack […] You want to make a focused query against a body of data that returns only those numbers that are connected to the one you have reasonable suspicion is connected to a terrorist group. But unless you have […] all the records of who called whom – you cannot answer the question. The confidence you will have in any answers returned by your query is necessarily tied to whether the haystack constitutes a reasonably complete set of records and whether those records look back a reasonable amount of time […] Hence "all" the records are necessary […] even if only an extremely small fraction of them is ever determined to be the match you're looking for.[106]

As Judge William Pauley commented in a US District Court, when considering the metadata programme, "[t]his blunt tool only works because it collects everything."[107]

1.2.4 WHEN CAN THE METADATA BE QUERIED?

The NSA can query metadata when there is a "reasonable, articulable suspicion" that the number that they wish to query is associated with a foreign terrorist group.[108] This query can only be sanctioned by 2 out of 20 line personnel, and then one of two supervisors authorised to do so.[109]

If the NSA discovers terrorism-related communications, it then issues an intelligence report to the FBI or other federal agencies.[110]

1.2.5 HOW SECTION 215 CAN WORK IN PRACTICE

An NSA analyst has a 'reasonable, articulable suspicion' that telephone number 'X' is associated with a foreign terrorist group and wishes to query the number. This is approved by NSA line personnel and a supervisor.

104. 'Media Leaks Facts & Context', U.S. House of Representatives Permanent Select Committee on Intelligence (2013), available at: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/TalkingPointsLong.pdf, last visited: 16 March 2015.

105. 'Remarks by the President on Review of Signals Intelligence', *The White House – Office of the Press Secretary*, 17 January 2014.

106. 'Media Leaks Facts & Context', U.S. House of Representatives Permanent Select Committee on Intelligence (2013).

107. 'American Civil Liberties Union et al. -against- James R. Clapper et al. – Memorandum & Order', United States District Court; Southern District of New York (2013), available at: http://www.theguardian.com/world/interactive/2013/dec/27/nsa-phone-data-collection-legal-full-ruling, last visited: 16 March 2015, p. 2.

108. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 9 May 2014.

109. 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies (2013), available at: http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, last visited: 16 March 2015, pp. 98-99.

110. 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Privacy and Civil Liberties Oversight Board (2014), p. 8.

The 'first hop'

The NSA analyst can now access a breakdown of all the numbers ('list A') that have either called or been called by telephone number 'X' in the past five years. They then attempt to determine whether any of these newly acquired numbers are associated with a foreign terrorist group.

The 'second hop'

The NSA analyst can query their database, in order to obtain every phone number ('list B') that has called or been called by those in 'list A'.

The 'third hop'

Previously, on rare occasions, the NSA analyst could query the database in order to obtain every phone number ('list C') that has called or been called by those in 'list B'.[111]

The level of intrusiveness that exists with the 'third hop' has been criticised.[112] In 2014 President Obama barred all such searches.[113]

1.2.6 HOW OFTEN HAS THIS POWER BEEN USED?

In 2012, the NSA queried 288 'selectors' – meaning a telephone number; e-mail address; or some form of electronic identifier, but not necessarily an individual user – from its metadata collection, leading them to look at a total of approximately 6,000 telephone numbers.[114] In 2013, the NSA queried 423 'selectors'.[115]

1.2.7 WHO PROVIDES OVERSIGHT?

The powers contained in Section 215 have been approved by all branches of the US government. According to General Alexander, Section 215 "probably has the most oversight of any program that [the] NSA utilises."[116]

The Judiciary

The government files a report with the FISA Court, every 30 days, outlining how the programme is being used (for example, providing the number of metadata queries submitted and how often such queries had led to information about US suspects being shared with other departments). The FISA Court must review and re-authorise this programme every 90 days.[117]

The Executive

The basis for the each of the metadata queries is audited by the DoJ. The DoJ is required to meet with the NSA Office of the Inspector General every 90 days (minimum), to ensure that the NSA

111. 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies (2013), pp. 102-103.

112. For example, an article in *The New Yorker* commented that the NSA "can look closely at the communications of anyone who has been in touch with a person who's been in touch with a person whose [sic] been in touch with another person the agency thinks is a suspicious foreigner. That's called not targeting the person you're spying on" (Davidson, A., 'Are the N.S.A. and G.C.H.Q. Trading Webcam Pictures?' *The New Yorker*, 28 February 2014, available at: http://www.newyorker.com/news/amy-davidson/are-the-n-s-a-and-g-c-h-q-trading-webcam-pictures).

113. 'Remarks by the President on Review of Signals Intelligence', *The White House – Office of the Press Secretary*, 17 January 2014.

114. 'NSA Says It Would Welcome Public Advocate At FISA Court', *NPR*, 9 January 2014, available at: http://www.npr.org/templates/transcript/transcript.php?storyId=261079074, last visited: 16 March 2015.

115. '2013 Transparency Report', *Office of the Director of National Intelligence*, 26 June 2014, available at: http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013, last visited: 16 March 2015.

116. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 79 May 2014.

117. 'Section 215 of the USA PATRIOT Act of 2001, which amended Title V, Section 501 of the Foreign Intelligence Surveillance Act (FISA), "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations" (50 U.S.C. sec. 1861)'.

is complying with the courts. Compliance is also assessed, in the same period, during a meeting between representatives from the DoJ; ODNI; and NSA.[118]

The Legislature

Congress must be informed, by the Attorney General, on how Section 215 has been implemented, every six months.[119]

THE 9/11 METADATA DEBATE

According to President Obama, the collection of telephone records in bulk began to occur "out of a desire to address a gap identified after 9/11."[120] One of the hijackers, Khalid al-Mihdhar, had made a call to an al-Qaeda safe house in Yemen, before the attack, which had been seen by the NSA. However, the NSA did not have the authority to check whether al-Mihdhar was actually making the call from within the US itself.[121] (It was not permitted to check records on calls made from the US to an international number.) Yet, under the Section 215 programme, the NSA would have been able to use al-Mihdhar's phone number to map out his other connections, potentially leading them to the other 9/11 hijackers.[122]

However, it has been argued that it was not a dearth of intelligence that led to the attacks on 9/11, but a lack of intelligence sharing between government departments such as the CIA; NSA; and FBI, and an inability to effectively use the authority available to them.[123] For example, from 2000, the CIA was aware that al-Mihdhar was a part of al-Qaeda and had a multi-entry visa to the US; yet, it did not disclose this to the FBI until shortly before 9/11. It also knew that Nawaf al-Hazmi, a known al-Mihdhar associate and a future 9/11 hijacker, was in the US.[124]

Marshall Erwin of the *Hoover Institution* notes that the *9/11 Commission Report* lists "ten operational opportunities related to al-Mihdhar and […] Nawaf al-Hazmi, that could have allowed intelligence and law enforcement officials to disrupt the attack. Problems associated with NSA's collection of al-Mihdhar's communications did not make the list."[125]

1.2.8 CONSTITUTIONAL ISSUES SURROUNDING METADATA COLLECTION

In December 2013, two federal judges reached two different conclusions on the constitutionality of Section 215, within days of each other.

Judge Richard Leon ruled that it violated the Fourth Amendment, with citizens' privacy being "violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-

118. Ibid.

119. 'Section 215 of the Foreign Intelligence Surveillance Act', *Office of the Director of National Intelligence*, available at: http://icontherecord.tumblr.com/topics/section-215, last visited: 16 March 2015.

120. 'Remarks by the President on Review of Signals Intelligence', *The White House – Office of the Press Secretary*, 17 January 2014.

121. Ibid.

122. 'NSA Chief Urges Public Debate of Terrorist Surveillance', *American Forces Press Service*, 13 June 2013, available at: http://www.defense.gov/news/newsarticle.aspx?id=120284, last visited: 16 March 2015.

123. For example, see: German, M., 'No NSA Poster Child: The Real Story of 9/11 Hijacker Khalid al-Mihdhar', *Defense One*, 16 October 2013, available at: http://www.defenseone.com/ideas/2013/10/no-nsa-poster-child-real-story-911-hijacker-khalid-al-mihdhar/72047/; see also: Elliott, J., 'Judge on NSA Case Cites 9/11 Report, But It Doesn't Actually Support His Ruling', *Pro Publica*, 28 December 2013, available at: http://www.propublica.org/article/fact-check-the-nsa-and-sept-11; see also: Bergen, P., 'Would NSA surveillance have stopped 9/11 plot?', *CNN*, 31 December 2013, available at: http://edition.cnn.com/2013/12/30/opinion/bergen-nsa-surveillance-september-11/; see also: Wright, L., 'The Al Qaeda Switchboard', *The New Yorker*, 13 January 2014, available at: http://www.newyorker.com/magazine/2014/01/13/the-al-qaeda-switchboard, last visited: 16 March 2015.

124. Erwin, M., 'Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection', Just Security (2014), available at: http://justsecurity.org/wp-content/uploads/2014/01/Connecting-the-Dots.pdf, last visited: 16 March 2015, p. 5.

125. Ibid., p. 6.

tech querying and analysis without any case-by-case judicial approval."[126] The programme was deemed "likely" unconstitutional.[127] Furthermore, Leon pointed out that the government could "not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the government in achieving any objective that was time-sensitive in nature."[128] The PCLOB also raised concerns on the constitutional soundness of this metadata gathering.[129]

However, Judge William Pauley disagreed, concluding that the programme did not violate the Fourth Amendment and was lawful. Pauley commented that "[t]he right to be free from searches and seizures is fundamental, but not absolute […] Whether the Fourth Amendment protects bulk telephony metadata is ultimately a question of reasonableness."[130] A Supreme Court precedent (Smith v. Maryland, 1979) ruled that citizens cannot have a "legitimate expectation of privacy" when making phone calls,[131] as it is known that service providers store customer information for legitimate business purposes – meaning that expectations of privacy are voluntarily being surrendered. Pauley declared that the bulk collection of metadata was "relevant to an authorized investigation" as outlined in Section 215 and that, "without all the data points, the government cannot be certain it connected the pertinent ones […] Armed with all the metadata, NSA can draw connections it might otherwise never be able to find."[132]

Justice Scalia, who sits on the US Supreme Court, has stated that if the action meets the standards of reasonableness when balanced against the risk, then the intrusion is not in violation of the Constitution:

> There are very few freedoms that are absolute […] your person is protected by the Fourth Amendment; but, […] when you board a plane, somebody can pass his hands all over your body – that's a terrible intrusion – but, given the danger that it's guarding against, it's not an unreasonable intrusion. And it can be the same thing with acquiring this data…[133]

Therefore, it could be argued that the government's decision on what is relevant is based on their perception of what is reasonably required to protect national security.

Yet, in May 2015, a federal appeals court ruled that the government's telephony meta-data collection was illegal. Bulk collection of this data was ruled not to be a valid interpretation of the collection of business records relevant to a counterterrorism investigation, which is permitted under Section 215. Clearly, there is no consensus and lots of issues surrounding this program remain contentious.[134]

126. 'Klayman et al. v. Obama et al. – Memorandum Opinion', United States District Court for the District of Columbia (2013), available at: http://www.theguardian.com/world/interactive/2013/dec/16/nsa-collection-phone-metadata-district-court-ruling, last visited: 16 March 2015, p. 56.

127. Ibid., p. 61.

128. Ibid.

129. 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Privacy and Civil Liberties Oversight Board (2014), p. 10.

130. 'Am. Civil Liberties Union v. Clapper', *United States Southern District of New York*, 27 December 2013, available at: https://casetext.com/case/aclu-v-clapper.

131. Ibid.

132. Ibid. This is not an issue that falls on liberal–conservative fault lines: Pauley was a Clinton appointee, and Leon a George W. Bush appointee.

133. 'The Kalb Report - Ruth Bader Ginsberg & Antonin Scalia', *The Kalb Report*, 42:24, 17 April 2014, available at: http://www.youtube.com/watch?v=z0utJAu_iG4&feature=share&t=42m21s, last visited: 16 March 2015.

134. 'N.S.A. Phone Program Is Illegal, Appeals Court Rules', *The New York Times*, 7 May 2015, available at: http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html?_r=0, last visited: 7 May 2015.

1.2.9 DOES SECTION 215 STOP TERRORISM?

As the information that Snowden revealed began to hit the press, the US tried to highlight the role that Sections 215 and 702 played in counterterrorism activities. President Obama stated that "[w]e know of at least 50 threats that have been averted because of this information […] lives have been saved."[135]

One example that has been provided concerns an al-Shabaab network in San Diego, California. In October 2007, the NSA provided the FBI with information gained from metadata which proved a connection between a foreign operative linked to al-Shabaab (al-Qaeda's Somali franchise) and an unknown number based in San Diego.[136] The FBI subsequently began an investigation, which led to the February 2013 convictions of Basaaly Moalin; Issa Doreh; Mohamed Mohamed Mohamud; and Ahmed Nasiri Taalil Mohamud, for conspiring to provide material support to al-Shabaab.[137]

However, a former Deputy Director of the NSA, Chris Inglis, has referred to Section 215 as "an insurance policy" and "not a silver bullet in and of itself".[138] A Presidential task force assigned to investigate potential reform to government surveillance programmes stated that, with regard to Section 215, "telephony meta-data was not essential to preventing attacks".[139] The PCLOB was also sceptical of its worth, concluding that the telephone programme had not provided any warning about attacks that were being planned against the US (such as the al-Qaeda in the Arabian Peninsula 'underwear bomb' plot of Christmas Day 2009, or the attempted Times Square car-bombing of 1 May 2010). It went on to report "little reason to expect that [Section 215] is likely to provide significant value, much less essential value, in safeguarding the nation in the future."[140] Michael Morell, the former deputy director of the CIA, has also stated that Section 702 is a "much more important program" than the telephony metadata collection.[141]

However, the lack of evidence of telephony metadata collection under Section 215 specifically stopping attacks is not necessarily as significant as it sounds. Professor Matthew Waxman, co-chair of the Roger Hertog Program on Law and National Security at Columbia Law School, has suggested that:

> a low number might reflect a program's value, too, in helping to disrupt or interdict terrorist groups' […] activities in their early stages. […Given that the] intelligence community is supposed to be bringing together multiple tools and information streams in support of each other […] it would be remarkable if the government could point to many plots that were foiled singlehandedly by the NSA, let alone a particular NSA program.[142]

Therefore, Section 215 is best understood as a safety measure designed to be part of the intelligence mosaic concerning terrorist activity with a foreign and domestic component. Considering the

135. 'Remarks by President Obama and German Chancellor Merkel in Joint Press Conference', *The White House – Office of the Press Secretary*, 19 June 2013, available at: http://www.whitehouse.gov/the-press-office/2013/06/19/remarks-president-obama-and-german-chancellor-merkel-joint-press-confere, last visited: 16 March 2015.

136. '54 Attacks in 20 Countries Thwarted By NSA Collection', U.S. House of Representatives Permanent Select Committee on Intelligence, available at: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/50attacks.pdf, last visited: 16 March 2015.

137. 'San Diego Jury Convicts Four Somali Immigrants of Providing Support to Foreign Terrorists', *Federal Bureau of Investigation*, 22 February 2013, available at: http://www.fbi.gov/sandiego/press-releases/2013/san-diego-jury-convicts-four-somali-immigrants-of-providing-support-to-foreign-terrorists, last visited: 16 March 2015.

138. 'Transcript: NSA Deputy Director John Inglis', *NPR*, 10 January 2014.

139. 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies (2013), p. 106.

140. 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court', Privacy and Civil Liberties Oversight Board (2014), p. 155.

141. 'CIA's Ex-No. 2 Says ISIS "Learned From Snowden"', *The Daily Beast*, 6 May 2015, available at: http://www.thedailybeast.com/articles/2015/05/06/cia-s-ex-no-2-says-isis-learned-from-snowden.html, last visited: 7 May 2015.

142. Waxman, M., 'How to Measure the Value of NSA Programs?', *Lawfare*, 12 August 2013, available at: http://www.lawfareblog.com/2013/08/how-to-measure-the-value-of-nsa-programs/, last visited: 16 March 2015.

controversy that Section 215 has caused, some may consider this unsatisfactory. Yet, governments around the world use this type of data for a range of security and serious-crime issues; the US should be no different just because it has an especially advanced capacity to capture these communications.

SECTIONS 215 & 702 WORKING TOGETHER: A CASE STUDY

Under Section 702 authority,[143] the NSA intercepted e-mails on 6 and 7 September 2009.[144] The messages were from an al-Qaeda terrorist in Pakistan to a then-unknown individual in the US, discussing (in code) a recipe for explosives and where to obtain them. This lead was passed to the FBI, which identified the US-based individual as a Colorado resident called Najibullah Zazi. Zazi was planning an imminent, major, terrorist operation to bomb the New York City Subway.[145]

On 9 September, the NSA ran Zazi's number against telephony metadata, issuing a Business Records FISA Metadata report on his foreign and domestic contacts, which was passed to the FBI.[146] This unearthed a previously unknown telephone number for Adis Medunjanin, a US-based extremist known to the FBI, who was also connected to the bombing scheme.[147] Zazi and Medunjanin were eventually convicted of a variety of terrorism charges relating to the plot and their support of al-Qaeda.

Marshall Erwin, though, has called into question the role that the NSA played in disrupting this conspiracy – beyond the initial interception under Section 702. For example, it is thought that the FBI had Zazi under surveillance from 7 September and had been following him, as he travelled across the country, for the two days preceding his phone records being queried. Erwin also argues that travel records and an informant had already linked Zazi to Medunjanin prior to the NSA metadata report.

This led Erwin to speculate that "[a]t the point when NSA utilized its bulk phone records collection program, the FBI was well on its way to disrupting Zazi's plot, appears to have had sufficient information to do so, and had already linked Zazi to Medunjanin."[148]

1.3 EXECUTIVE ORDER 12333

Executive Order (EO) 12333 is the Executive Branch's primary authority for foreign-intelligence gathering that (a) takes place outside the US and (b) is not governed by FISA.[149] It was signed into law by President Ronald Reagan, in December 1981, and updated by President Bush, in 2008. A former legal counsel for the CIA and the Senate's Intelligence Committee has described it as an intelligence agent's "Bible";[150] the NSA has described it as a "foundational authority".[151]

EO 12333 outlines the goals, direction, duties, responsibilities, and conduct of the US's

143. '54 Attacks in 20 Countries Thwarted By NSA Collection', U.S. House of Representatives Permanent Select Committee on Intelligence.

144. Erwin, M., 'Connecting the Dots', Just Security (2014), p. 2.

145. 'Joint Statement for the Record by Michael Leiter, Director, National Counterterrorism Center, and [Redacted], Associate Deputy Director For Counterterrorism, Signals Intelligence Directorate, National Security Agency, before the House Permanent Select Committee on Intelligence – Closed Hearing on PATRIOT Act Reauthorization', U.S. House of Representatives Permanent Select Committee on Intelligence (2009), available at: https://www.eff.org/files/2013/10/28/nsa_joint_report_oct_2009_sealed_final.pdf, last visited: 16 March 2015.

146. Ibid.

147. '54 Attacks in 20 Countries Thwarted By NSA Collection', U.S. House of Representatives Permanent Select Committee on Intelligence.

148. Erwin, M., 'Connecting the Dots', Just Security (2014), pp. 3-4.

149. 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies (2013), p. 69.

150. 'NSA revelations of privacy breaches "the tip of the iceberg" – Senate duo', *The Guardian*, 16 August 2013, available at: http://www.theguardian.com/world/2013/aug/16/nsa-revelations-privacy-breaches-udall-wyden, last visited: 16 March 2015.

151. 'The National Security Agency: Missions, Authorities, Oversight and Partnerships', National Security Agency (2013), p. 2.

17 intelligence agencies.[152] According to the President's Review Group on Intelligence and Communications Technologies, it "specifies the missions and authorities of each element of the Intelligence Community; sets forth the principles designed to strike an appropriate balance between the acquisition of information and the protection of personal privacy; and governs the collection, retention, and dissemination of information about United States Persons".[153]

EO 12333 also outlines what activities the intelligence community is not allowed to engage in domestically – for example, preventing the CIA from carrying out electronic surveillance, or preventing agencies other than the FBI from conducting physical searches.[154]

1.3.1 WHY COLLECTION COULD TAKE PLACE UNDER EO 12333

FISA does not apply if communications targeted by Signals Intelligence (SIGINT) are being routed through servers or satellites without a US end. Therefore, as long as it is for a "valid foreign intelligence purpose", collection in these circumstances would take place under EO 12333.[155]

1.3.2 WHY IS IT CONTROVERSIAL?

It has a US collection component

EO 12333 targets foreign networks. However, the data that is being swept up from these networks, as part of the NSA's bulk collection, may contain fragments and packets of information containing communications from US citizens. EO 12333 allows for the retention of these US citizens' communications, including content, as part of a foreign-intelligence investigation.[156]

Communications from US citizens can be kept for up to five years, unless the NSA Director determines that a national-security imperative means that they must be kept longer (a potentially broad loophole).[157] If an American citizen is deemed, by the Attorney General, to be an agent of a foreign power, or if they are part of a foreign-intelligence investigation, these stored communications can then be searched.[158] However, individuals cannot be targeted without a court order, and inspecting content would still require a warrant.[159]

As the collection does not take place under FISA, there is a different level of oversight

As EO 12333 collection occurs outside the US, the oversight that is applicable to Section 702 does

152. 'Executive Order 12333--United States intelligence activities', *The U.S. National Archives and Records Administration*, 4 December 1981, available at: http://www.archives.gov/federal-register/codification/executive-order/12333.html, last visited: 16 March 2015.

153. 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies (2013), p. 69.

154. Ibid., p. 70.

155. Ibid., p. 268.

156. Tye, J., 'Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans', *The Washington Post*, 18 July 2014, available at: http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html, last visited: 16 March 2015.

157. Richards, R., 'NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333', NSA Director of Civil Liberties and Privacy Office (2014), available at: https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf; see also: Nakashima, E. and Ashkan Soltani, 'Privacy watchdog's next target: the least-known but biggest aspect of NSA surveillance', *The Washington Post*, 23 July 2014, available at: http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/.

158. 'Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil', *The New York Times*, 13 August 2014, available at: http://www.nytimes.com/interactive/2014/08/13/us/two-sets-of-rules-for-surveillance.html; see also: Joel, A., 'The Truth About Executive Order 12333', *Politico*, 18 August 2014, available at: http://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121.html#ixzz3JXQHuTJ, last visited: 17 March 2015.

159. 'Most of NSA's data collection authorized by order Ronald Reagan issued', *McClatchy DC*, 21 November 2013, available at: http://www.mcclatchydc.com/2013/11/21/209167_most-of-nsas-data-collection-authorized.html, last visited: 17 March 2015.

not exist.[160] For example, there is no FISA Court oversight;[161] instead, EO 12333 has Attorney General-approved procedures in place, regarding how the information is collected; retained; or disseminated. Further oversight is provided by a variety of inspectors general; oversight boards; general counsels; compliance officers; and privacy officers, at the various departments to which EO 12333 relates.[162]

160. Ibid.; see also: 'Two Sets of Rules for Surveillance, Within U.S. and on Foreign Soil', *The New York Times*, 13 August 2014.

161. Ibid. (both sources).

162. Joel, A., 'The Truth About Executive Order 12333', *Politico*, 18 August 2014.

2. UNITED KINGDOM

The first piece of media coverage concerning GCHQ's activities followed two days after the initial *Guardian* story revealing the NSA's collection of telephone records. This story focused on the access that GCHQ had to PRISM.[163]

Other allegations followed:

- that GCHQ was able to attach intercept probes to the fibre-optic cables which carry internet and phone traffic, in order to set up internet buffers (this would enable it to store and analyse data (Operation Tempora)), including e-mail content; phone calls; and internet-user history, which was shared with the NSA;[164] and
- that GCHQ was intercepting and storing webcam images (Operation Optic Nerve).[165]

Such stories led to calls for greater transparency and potential reform of the intelligence services – including from then-Deputy Prime Minister and Shadow Home Secretary.[166]

GCHQ: ORIGINS

The UK's first SIGINT efforts date back over 100 years, to the First World War and the interception and subsequent analysis of encrypted German communications.[167] The best known SIGINT success story from this conflict occurred in January 1917, when the UK intercepted a telegram from the German Foreign Minister, Count Zimmermann. In this telegram to Mexico, Zimmermann stated that Germany was about to begin attacks against submarines trading with Britain, including those belonging to the then-neutral US. As this would potentially draw the US into the war, on Britain's side, Zimmermann offered Mexico its former territory in Texas; Arizona; and New Mexico, if it agreed to join the German war effort. The British interception and release of this telegram proved influential in the US' eventual decision to join the fighting.

Following the war, the Government Code and Cypher School (GC&CS) was created. GC&CS moved to Bletchley Park in 1939, where the cracking of the Enigma machine's code allowed it to decipher German military strategy, playing a key part in the Allied powers' victory.

GC&CS was renamed 'GCHQ', in 1946. Its responsibilities and functions are laid out in the 1994 Intelligence Services Act; its work must also adhere to the Human Rights Act 1998 and the Regulation of Investigatory Powers Act (RIPA) 2000.

163. 'UK gathering secret intelligence via covert NSA operation', *The Guardian*, 7 June 2013, available at: http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism, last visited: 17 March 2015.

164. 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013.

165. 'Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ', *The Guardian*, 28 February 2014.

166. 'Labour to overhaul spy agency controls in response to Snowden files', *The Guardian*, 2 March 2014, available at: http://www.theguardian.com/uk-news/2014/mar/02/labour-spy-agency-controls-cooper-snowden-files, last visited: 17 March 2015; see also: Clegg, N., 'Security and privacy in the internet age', *UK Government*, 4 March 2014.

167. 'Beginnings', *Government Communications Headquarters*, available at: http://www.gchq.gov.uk/history/pages/beginnings.aspx, last visited: 17 March 2015.

2.1 RIPA AND ITS INTERPRETATION

The Regulation of Investigatory Powers Act (RIPA) 2000 is a core piece of legislation, due to the powers which it contains and the oversight that it offers. According to the Home Office, RIPA "provides the statutory framework which governs the interception of communications."[168]

Part I of RIPA is split into two chapters. Part I, Chapter 1 relates to the interception of communications content and the obtaining of related communications data. It replaced the Interception of Communications Act 1985,[169] and was intended to regulate the government's use of covert surveillance techniques (in order to ensure the proportionality and necessity of their application).[170] This came into force in 2000.

Part I, Chapter 2 concerns the state's ability to acquire and disclose communications data – though it does not regulate what must be retained.[171] It was designed to replace voluntary communications data disclosure arrangements under the Data Protection Act and came into force in 2004.

Charles Farr, the Director General of the Office for Security and Counter-Terrorism, has stated that "[i]nterception under RIPA provides tactical information […and] real time intelligence on the plans and actions of individual terrorists, criminals and other targets […] and facilitates their arrest by law enforcement agencies."[172] According to Farr, intelligence gathered in this way has "led directly to the prevention of terrorist attacks and serious crime, the success of operations aimed at countering the proliferation of weapons of mass destruction and the saving of lives."[173]

2.1.1 WHAT IS COMMUNICATIONS DATA?

Communications data is about the context of a communication – the "who, when, where, how" (i.e. context).[174] However, it is not about the 'what' (i.e. content).[175]

There are three specific types of communications data that are of particular importance to the government.[176]

Subscriber Data

'Subscriber data' relates to information held by a CSP about the services which it provides to its customers when that relevant data is held by the company. It enables the state to carry out

168. 'Regulation of Investigatory Powers Act 2000: Proposed Amendments Affecting Lawful Interception – A Consultation: A Summary of Responses', UK Home Office (2010) available at: http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157983/ripa-lawful-intercept-responses.pdf, last visited: 17 March 2015.

169. 'Surveillance: Citizens and the State', House of Lords – Select Committee on the Constitution (2009), available at: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf, last visited: 17 March 2015, p. 36.

170. 'Surveillance and counter-terrorism', *UK Home Office*, 26 March 2013, available at: https://www.gov.uk/surveillance-and-counter-terrorism, last visited: 17 March 2015.

171. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), available at: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf, p. 5; see also: May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), available at: http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf, last visited: 17 March 2015, p. 2.

172. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), p. 10.

173. Ibid.

174. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), p. 27.

175. 'Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA): Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance', UK Home Office (2012), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf, last visited: 17 March 2015, p. 6.

176. These definitions are guided by the 'Acquisition and Disclosure of Communications Data: Code of Practice', UK Home Office (2007), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97961/code-of-practice-acquisition.pdf; the 'Draft Communications Data Bill', UK Government (2012), available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf; and the 'Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)', UK Home Office (2012).

reverse look-ups, such as finding out who is the owner of a particular phone number; the account holder of a certain e-mail address; or, potentially, those who can post on a certain website. Other information that could be gained includes billing information or the make, model, and serial number of a device used on the account. This data is held by the provider, not the government.

Service Use Data

'Service-use data' relates to postal and telephony communications, and includes telephone call records; connections to internet services; the duration of calls; and/or connections and information relating to data downloads and uploads. However, this is an area in which intelligence agencies are finding it hard to access: if telephone companies provide their customers with unlimited-call packages, for example, they may not need to generate service-use data for billing purposes. Such companies are not obliged to create communications data that they would not need to use themselves; hence, why the government's access to such data has diminished.

Traffic Data

To the extent to which it is retained or even generated, 'traffic data' enables the state to find out, for example, information relating to the origin or destination of a transmitted communication; the location of a mobile phone when a communication was made or received; the address on a letter that has been sent; and internet-browsing history (up to the first 'slash' - for more details, see pages 43-44).

IS COMMUNICATIONS DATA DIFFERENT FROM METADATA?

In a speech delivered by then-Deputy Prime Minister Nick Clegg, the terms 'communications data' and 'metadata' were used interchangeably.[177]

Yet, there is a specific legal definition used in the UK, regarding 'communications data' – as opposed to a broader US interpretation of 'metadata', which can include data gathered by tools that undertake data mining from the internet and social media.[178] This type of metadata mining is not just carried out by the state, but also by the private sector (which sells on the data, for marketing purposes).

An Intelligence and Security Committee (ISC) report clarified that metadata "has no legal definition in RIPA and therefore no bearing on the UK system of interception. For example, in the UK a record of a website visited […] is treated as [communications data], whereas the full web address […] is treated as content. Both of these, however, might be referred to as 'metadata'."[179]

2.1.2 WHY IS ACCESS TO COMMUNICATIONS DATA IMPORTANT?

Communications data is, according to a Parliamentary Joint Committee, "an invaluable weapon" in safeguarding national security and protecting the UK from crime.[180] Home Secretary Theresa May has stated that it "has played a significant role in every Security Service counter-terrorism operation over the last decade", and that "it has been used as evidence in 95 per cent of all serious organised crime cases handled by the Crown Prosecution Service" (being particularly useful in

177. Clegg, N., 'Security and privacy in the internet age', *UK Government*, 04 March 2014.

178. Omand, D., 'Evidence for the Intelligence and Security Committee of Parliament', Intelligence and Security Committee of Parliament (2014), available at: http://bit.ly/1FiQyzk.

179. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 52.

180. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), p. 8.

reconstructing organised-crime networks, for example).[181]

Indeed, the usefulness of communications data extends beyond even this. Communications data is also relevant in identifying and locating suicide risks; identifying rapists, kidnappers, or threatening callers; and in murder investigations.[182] For example, it was used to implicate Ian Huntley and Maxine Carr during the investigation into the killings of the schoolgirls Holly Wells and Jessica Chapman; the communications data from girls' mobile phones demonstrated that they were in close geographical proximity to Huntley, and that his alibi was likely false.[183]

It is also vital in preventing child abuse and exploitation (including the prosecution of its perpetrators). According to Keith Bristow, Director General of the National Crime Agency, "[c]ommunications data is still overwhelmingly the most powerful tool available to those investigating child sexual exploitation and identifying and safeguarding its victims and potential victims."[184]

Sir Anthony May, the Interception of Communications Commissioner, summarised communication data's use in the following way:

> [Communications data] revealed suspects movements and tied them to crime scenes. It often led to other key evidence being identified or retrieved. Links to previously unidentified offenders and offences were revealed. Dangerous offenders were located and offences were disrupted with the assistance of communications data. Patterns of communication provided evidence of conspiracy between suspects. The data highlighted inconsistencies in accounts given by suspects and corroborated the testimony of victims. The data determined the last known whereabouts of victims and persons they had been in contact with. Similarly, communications data assisted to eliminate key suspects or highlighted inconsistencies in accounts given by victims.[185]

2.1.3 WHY DOES COMMUNICATIONS DATA COLLECTION UNDER PART I, CHAPTER 1 OF RIPA NEED TO TAKE PLACE IN BULK?

British security officials have provided a similar explanation to their American counterparts regarding the need for communications data collection to take place in bulk. Sir Iain Lobban, when speaking, in November 2013, as head of GCHQ, explained it – and the constraints that GCHQ face – in the following terms:

> If you think of the internet as an enormous hay field, what we are trying to do is to collect hay from those parts of the field that we can get access to and which might be lucrative in terms of containing the needles or the fragments of the needles that we might be interested in, that might help our mission.
>
> When we gather that haystack, and remember it is not a haystack from the whole field, it is a haystack from a tiny proportion of that field, we are very, very well aware that within that haystack there is going to be plenty of hay which is innocent communications from

181. May, T., 'Home Secretary's oral statement about the use of communications data and interception', *UK Home Office*, 10 July 2014, available at: www.gov.uk/government/speeches/communications-data-and-interception; see also: 'Oral Evidence Taken Before the Joint Committee on the Draft Communications Data Bill – Donald Toon, Cressida Dick, Gary Beautridge, Trevor Pearce and Peter Davies; Daniel Thornton, Councillor Paul Bettison, Gillian McGregor and Nick Tofiluk – Questions 127 - 220', House of Lords & House of Commons (2012), available at: www.parliament.uk/documents/joint-committees/communications-data/uc120712Ev3HC479iii.pdf, last visited: 17 March 2015.

182. 'Oral Evidence – Donald Toon et al. – Questions 127 - 220', House of Lords & House of Commons (2012); see also: 'Acquisition and Disclosure of Communications Data: Code of Practice', UK Home Office (2007).

183. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), p. 8.

184. 'Factsheet #1 – Communications Data – Data Retention and Investigatory Powers Bill', UK Government, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/330510/Factsheet_Data_Retention.pdf, last visited: 13 April 2015.

185. May, A., 'Report of the Interception of Communications Commissioner: March 2015 (covering the period January to December 2014)', Interception of Communications Commissioner's Office (2015), available at: http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf, p. 61, last visited: 29 April 2015.

> innocent people […] And so we design our queries against that data, to draw out the needles and we do not intrude upon […] the surrounding hay.[186]

Another intelligence source stated that "we have a process that allows us to select a small number of needles in a haystack. We are not looking at every piece of straw. There are certain triggers that allow you to discard or not examine a lot of data so you are just looking at needles."[187]

2.1.4 COMMUNICATIONS DATA v. CONTENT

The access of communications data or content data by a public body needs to be shown to be both necessary and proportionate. Traditionally, it has been thought to be less intrusive to look at the former as opposed to the latter. However, the information that can be gained via communications data has become more comprehensive and, therefore, more potentially intrusive. If the data has been generated and can then be acquired, then reasonably detailed personal information can be gathered; it could be possible to piece together a comprehensive picture of people's lives, from a variety of sources revealing and monitoring their movements; habits; social networks; and interests. As former Information Commissioner Richard Thomas has noted, communication records "can be highly intrusive even if no content is collected."[188] This has led to accusations that what is revealed by communications data is now, in many ways, equal to that of content.[189]

Differing levels of authorisation for various types of communications data (depending on the level of intrusiveness) means that this might be an area that the state examines for potential reform in the future. The ISC has suggested the creation of a 'Communications Data Plus' category for communications data that "has the potential to reveal a great deal about a person's private life – his or her habits, tastes and preferences – and [about which] there are therefore legitimate concerns as to how that material is protected."[190]

When it comes to internet searches, the UK currently defines communications data as everything up to the 'first slash' (e.g. http://www.google.co.uk/); anything past the 'first slash' – e.g. typing in 'chemical weapons' on *Google* (http://www.google.co.uk/#q=chemical+weapons) – then becomes content data.[191] Accessing this content would only be possible with a Secretary of State-signed warrant. Therefore, theoretically, only websites visited would classify as communications data, not what was searched for within (e.g. that someone had shopped at *Amazon*, but not what type of books they had searched for, or that someone had shopped online at *Tesco*, but not what they had bought there).

However, a December 2014 submission to the Investigatory Powers Review from the Interception of Communications Commissioner's office highlighted potential ambiguity over this:

> https://accounts.google.com/ServiceLogin?service=mail&continue=https://mail.google.com/mail/ (which is the log-in webpage to activate access to webmail) goes well beyond the 'first slash' and may, at first appearance, be considered to be content of a communications. However, section 21(6)(b) explains that traffic data […] may include data identifying or selecting or purporting to identify or select, apparatus through which, or by means of which, the communications is or may be transmitted. This then begs the

186. 'Uncorrected transcript of Evidence Given by Sir Iain Lobban, Director, Government Communication Headquarters; Mr Andrew Parker, Director General, Security Service; Sir John Sawers, Chief, Secret Intelligence Service', Intelligence and Security Committee of Parliament (2013), p. 13.

187. 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013.

188. 'Every phone call, email or website visit "to be monitored"', *The Telegraph*, 24 April 2009, available at: http://www.telegraph.co.uk/news/uknews/5215413/Every-phone-call-email-or-website-visit-to-be-monitored.html, last visited: 17 March 2015.

189. These arguments are outlined in: 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), pp. 50-51.

190. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 6.

191. Private conversation.

> question whether the log-in webpage (no matter how many 'slashes' there are within the web addresses) is communications data or the content of a communication.[192]

Therefore, while the Codes of Practice (CoP) state that communications data should only be up to the first slash, there is ambiguity over this in RIPA itself. This ambiguity may allow the police or security services to go beyond the first slash in certain circumstances (such as a log-in webpage).

2.2 RIPA PART I, CHAPTER 1

2.2.1 OPERATION TEMPORA AND SECTION 8(4) OF RIPA

Under Section 8(4) of RIPA, the UK intercepts communications by tapping fibre-optic cables carrying both external (i.e. sent or received outside the UK) and internal (i.e. sent and received inside the UK) communications, though the collection of the latter is incidental. Using internet buffers, this data can allegedly be stored and analysed (for three days, with content, and 30 days, for communications data).[193]

This is known as the alleged 'Tempora' interception operation. Its primary purpose is as an intelligence-gathering tool, and, according to the Investigatory Powers Tribunal (IPT), Section 8(4) powers have played a "pre-eminent role" in identifying "threats to UK national security from abroad".[194]

Despite this, Section 8(4) warrants have proved controversial. This is not only because of the volume of communications being swept up, but also because communications are being intercepted using general warrants from the relevant Secretary of State (and therefore do not require specific named subjects to be on them). This is in contrast to interception warrants issued under Section 8(1) of RIPA – which, while also approved by the relevant Secretary of State, must specify the name or describe the individual who is the subject of interception, or the premises to which the interception relates.[195]

Instead, the 8(4) warrant must be for a specific purpose: in the interests of national security; for the purposes of preventing or detecting serious crime; or for the purposes of safeguarding the economic wellbeing of the United Kingdom.[196] As Charles Farr has explained, there is a reason for the difference:

> Within the British Islands, the government has sufficient control and considerable resources to investigate individuals and organisations, and it is feasible to adopt an interception regime that requires either a particular person, or a set of premises, to be identified before interception can take place. Outside the British Islands, the government does not have the same ability […].[197]

This is vital in attempting to discover overseas terrorist-attack planning, for example. The government is often unaware of the precise geographic location of foreign terrorists or cyber criminals, and is therefore unlikely to have "the same practical ability to identify the apparatus over which these communications [are being] carried; nor the same practical power to obtain

192. 'Evidence for the Investigatory Powers Review', Interception of Communications Commissioner's Office (2015), available at: http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf, last visited: 29 April 2015, pp. 18 – 19.

193. 'GCHQ taps fibre-optic cables for secret access to world's communications', *The Guardian*, 21 June 2013.

194. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), pp. 35 & 37.

195. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 7.

196. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 133. An example of the wording in the warrant, with regard to national security, includes: "Material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising" (see: 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 38).

197. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), p. 43.

messages from that apparatus".[198] This has been expanded upon in a recent ISC report, which commented that:

> Within the UK, the Agencies and police have far greater capacity, capability and coverage, and they are therefore more likely to be able to discover threats in the first place. (For example, MI5 may be provided with leads by the public or law enforcement.) […] However, outside the UK, the Agencies simply do not have the same resources and coverage available to discover the identity and location of individuals and organisations who pose a threat to the UK.[199]

While Section 8(4) targets the interception of external communications, it actually scoops up internal ones as well. For the government to be able to obtain what Farr refers to as "at least a fraction of the type of communication in which it is interested", it must intercept the communications in bulk and then select "a small fraction […] for examination".[200] As a result, internal communications are inevitably also swept up. According to Sir Anthony May, there are "no other reasonable means" for the state to separate, or filter out, what are internal rather than external communications when initially scooping this data up;[201] even internal communications may be transmitted via internet-service providers in foreign nations.[202] To access any of the content of what has been collected, though, GCHQ would still need a warrant.[203]

There have been accusations that the government, by utilising Section 8(4), may be acting "unlawfully or to the outer limits of legality".[204] However, Sir Anthony May concluded that the collection; storage; and access of communications data under Section 8(4) is legal, and that this process did not have "any significant risk of undue invasion of privacy."[205] This is an important conclusion for the Interception of Communications Commissioner to come to because, as one senior intelligence official has said, "Section 8(4) of RIPA underpins GCHQ's work", and those trying to change this risk "undermining everything".[206]

2.2.2 WHEN CAN COMMUNICATIONS BE EXAMINED UNDER SECTION 8(4)?

Communications of somebody in the British Islands and collected under Section 8(4) can be looked at; listened to; or read, in limited circumstances, under provisions in Sections 16 of RIPA.

Section 16(3) allows for their examination if they are "referable to an individual who is known to be […] in the British Islands" (essentially making it the same as a Section 8(1) warrant) and the Secretary of State has certified that the examination is being carried out for a national-security or serious-crime purpose.[207] 'Referable to an individual', in this context, could mean a '+44' phone number or a UK postal address. The communications can be examined over a six-month period, for national-security

198. Ibid., p. 44.

199. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 37.

200. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), pp. 44-45.

201. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 54.

202. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), p. 38.

203. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 39.

204. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 58.

205. Ibid., p. 52.

206. Private conversation.

207. 'Regulation of Investigatory Powers Act 2000: 2000 c. 23, Part I, Chapter I, Restrictions on use of intercepted material etc., Section 16', *UK Government*, available at: http://www.legislation.gov.uk/ukpga/2000/23/section/16, last visited: 17 March 2015; see also: May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 51.

investigations, and for three months for serious-crime and economic-wellbeing investigations.[208]

Sections 16(4) and (5) allow for their examination if the individual was believed, "on reasonable grounds," to be abroad at time of interception, or if there has been "a relevant change of circumstances" (such as, it has just been discovered that the individual has actually just entered the British Islands).[209] If it is for a national-security purpose, these communications can be examined for a period of five working days after this discovery; for a serious-crime or economic-wellbeing purpose, one working day.[210] This then allows coverage to continue – for a short time – over targets who are, for example, visiting the UK. Essentially, the Section 16 provisions primarily relate to external communications with one end in the UK.

These exceptions that exist under Section 16 have also been deemed controversial, with privacy and civil-liberty groups raising concerns over the ambiguity of what 'referable to an individual' actually means. For example:

> What constitutes "a factor referable to an individual"? A person's name, address or date of birth may obviously do so. But would such material […] be suitable for inspection if the 'factor' was slightly broader than by reference to an individual: e.g. people who were interested in a particular book? Or mentioned a specific mosque; or ate at a restaurant?[211]

The ambiguities over this are reflected in the comments of Tom Watson, the Labour Party MP, who has described Section 16 as "probably the single most confusing and complex drafting ever put on the statute book".[212] The Interception of Communications Commissioner has also conceded that "[p]arts of section 16 are in convoluted language and style."[213]

WHY IS THERE CONFUSION OVER EXTERNAL COMMUNICATIONS?

It was previously the case that the infrastructure used for foreign communications was distinct from that used for domestic. Yet, technological advances have led to this distinction becoming more contentious; CSPs have 'mirror' servers holding customer information across the world. Communications – e-mails from a certain account, say – can travel to either a UK server or any of these mirror servers abroad. Data streams have become entangled, with e-mails potentially passing through mirror servers in the US; Europe; or Asia – even if they are being sent to the computer next door.[214]

In the UK, an external communication is currently interpreted as one that has a foreign end. E-mails, including personal e-mail messages sent via social-media platforms such as *Facebook*, are defined as internal communications as long as the sender and recipient are based in the UK. This is the case even if the servers used by webmail services (such as *Hotmail*) are based abroad.[215]

208. 'Regulation of Investigatory Powers Act 2000: 2000 c. 23, Part I, Chapter I, Restrictions on use of intercepted material etc., Section 16', *UK Government*.

209. Ibid.; see also May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 51.

210. 'Regulation of Investigatory Powers Act 2000: 2000 c. 23, Part I, Chapter I, Restrictions on use of intercepted material etc., Section 16', *UK Government*.

211. 'Liberty (The National Council For Civil Liberties) and Others – Claimants – and (1) Government Communications Headquarters (2) The Secret Intelligence Service (3) The Security Service – Respondents – Skeleton Argument', Investigatory Powers Tribunal (2014), available at: https://www.liberty-human-rights.org.uk/sites/default/files/Skeleton%20argument%20of%20Liberty,%20the%20ACLU%20and%20others%2012th%20June%202014.pdf, last visited: 17 March 2015.

212. 'House of Commons Debate – Backbench Business: Intelligence and Security Services', *Hansard*, 31 October 2013, available at: http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm, last visited: 17 March 2015.

213. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 50.

214. Byman, D. and Benjamin Wittes, 'Reforming the NSA: How to Spy after Snowden', *Foreign Affairs*, May/June 2014, available at: http://www.foreignaffairs.com/articles/141215/daniel-byman-and-benjamin-wittes/reforming-the-nsa, last visited: 17 March 2015.

215. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), p. 39.

Yet, *Google* and *YouTube* searches; *Twitter* 'tweets'; and *Facebook* 'posts' are all defined as 'external communications'. The government's argument is that *Google*'s data centres and *Twitter*'s; *YouTube*'s; and *Facebook*'s web servers are based outside the UK (usually in the US), and, as there is not a known recipient of the search or the post, it cannot be shown to be an internal communication.[216] Similarly, accessing a website which has its web server located abroad, or uploading files to a cloud storage system overseas (for example, *Dropbox*) would also be treated as external communications.[217]

If the collection of such communications takes place under the general warrant used with Section 8(4), those based in the British Islands can only have their communications searched under the limited circumstances referred to in Section 16(3), (4), and (5).

This has proven controversial among privacy campaigners. For example, Eric King, deputy director of *Privacy International*, has said that the "distinction drawn by the government between 'internal' and 'external' communications no longer has any practical meaning. The safeguards provided by RIPA pertaining to the interception of 'internal' communications do not in fact result in any meaningful protections […] when applied to the modern communications system."[218]

216. Ibid., pp. 40-41.

217. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 40.

218. 'Social media mass surveillance is permitted by law, says top UK official', *The Guardian*, 17 June 2014, available at: http://www.theguardian.com/world/2014/jun/17/mass-surveillance-social-media-permitted-uk-law-charles-farr, last visited: 17 March 2015.

2.3 RIPA PART I, CHAPTER 2

2.3.1 WHO IS AUTHORISED TO ACQUIRE COMMUNICATIONS DATA, AND FOR WHAT PURPOSE?[219]

	Data Type (RIPA s.21(4))			Statutory Purpose (RIPA s.22(2) & SI 2010/480) (as amended by SI 2011/2085, SI 2012/2007, SI 2013/472, SI 2013/602, SI 2014/549, SI 2015/228)										
Public Authority Group	Traffic	Service Use	Subscriber	(a) national security	(b) prevent detect crime / prevent disorder	(c) economic well being of the UK	(d) – public safety	(e) – public health	(f) tax, duty, levy...	(g) in an emergency preventing death / injury...	Art 2(a) miscarriage of justice	Art 2(b) to identify person who has died or is unable to identify themselves, to identify next of kin or other person	Art 2(c) regulation of financial services and markets	Notes
- Intelligence Services	•	•	•	•	•	•								
- Territorial Police Forces of England, Wales, Northern Ireland & Scotland - British Transport Police	•	•	•	•	•	•	•	•		•		•		(d) & (e) subscriber only
- National Crime Agency	•	•	•		•					•		•		
- The Commissioners for Her Majesty's Revenue and Customs	•	•	•		•				•					(f) subscriber only
- The Home Office (Immigration Enforcement)	•	•	•		•		•					•		(d) subscriber only. Asylum fraud investigations can only acquire service use and subscriber information.
- Ministry of Defence Police - Royal Air Force Police - Royal Military Police - Royal Naval Police	•	•	•	•	•	•				•				
- Civil Nuclear Constabulary	•	•	•	•	•									
- Port of Dover Police - Port of Liverpool Police	•	•	•		•		•	•				•		(d) & (e) subscriber only
- Gambling Commission - Gangmasters Licensing Authority - The Information Commissioner - Office of Communications - Police Ombudsman for Northern Ireland - Royal Mail Group - Serious Fraud Office	•	•	•		•									
- Financial Conduct Authority - Prudential Regulation Authority	•	•	•		•								•	Statutory purpose Art.2(c) was made available from 12/02/15
- Independent Police Complaints Commission - Police Investigations and Review Commissioner	•	•	•		•							•		
- The Ministry of Justice - National Offender Management Service - Northern Ireland Office - Northern Ireland Prison Service	•	•	•		•		•					•		(d) subscriber only
- Criminal Cases Review Commission - Scottish Criminal Cases Review Commission	•	•	•								•			
Department of Transport: - Air Accident Investigation Branch - Marine Accident Investigation Branch - Rail Accident Investigation Branch	•	•	•				•							
- Department for Transport Maritime Coastguard Agency - Fire & Rescue Authorities - Ambulance Services / Trusts	•	•	•		•		•			•				(b) service use & sub - scriber only (d) subscriber only. (g) traffic, service use & subscriber
- Environment Agency - Health & Safety Executive - Department for Health - Medicines & Healthcare Products Regulatory Agency - Scottish Environment Protection Agency		•	•		•		•	•						(d) & (e) subscriber only
- Food Standards Agency		•	•		•			•						(e) subscriber only
- Charity Commission - DWP – Child Maintenance Group - Department of Agriculture & Rural Development (Northern Ireland) - Department for Business Innovation Skills - Department for Environment Food & Rural Affairs - Department of the Environment Northern Ireland - Health & Social Care Business Services Organisation - Central Services Agency (Northern Ireland) - Office of Fair Trading / Competition and Markets Authority - Pensions Regulator - NHS Protect - NHS Scotland Counter Fraud Services - The Department of Enterprise Trade and Investment (Northern Ireland)		•	•		•									
- Local Authorities		•	•		•									

Public authorities in grey had their powers removed on 12/02/15 (SI 2015/228)

219. Taken from: May, A., 'Report of the Interception of Communications Commissioner: March 2015 (covering the period January to December 2014)', Interception of Communications Commissioner's Office (2015), pp. 89-90. (As one intelligence official has stated, "The concern here is not about the number of authorities that have access to communications data, but that the ones who do only have access to the data that they strictly need.")

2.3.2 HOW IS IT ACCESSED?

In order for any public authority to acquire communications data, the following must occur:

- The applicant from the government body has to complete an application.
- A Designated Person (DP) within that same body has to assess whether the request for data is lawful, proportionate, and necessary. Following the revised Code of Practice which came into force in March 2015, DPs must be independent from the investigation or operation that the application is pertaining to.[220]
- The Single Point of Contact (SPoC), a trained and accredited individual who acts as a facilitator between CSPs and the authority making the request, must advise the DP and the applicant whether the request is appropriate and its granting lawful.
- A Senior Responsible Officer within the requesting authority must ensure compliance with Part I, Chapter 2 of RIPA and its Code of Practice, as well as the overall integrity of the procedure.[221]

2.4 OVERSIGHT

2.4.1 SECRETARIES OF STATE

One of the methods to intercept communications in the course of transmission is to apply for an interception warrant. This would allow access to the content of an email, for example. An application for an interception warrant must be governed by RIPA and be made by, or on behalf of one of the following:

- the Director General of the Security Service (MI5);
- the Chief of the Secret Intelligence Service (MI6);
- the Director of the Government Communications Headquarters (GCHQ);
- the Director General of the National Crime Agency;
- the Commissioner of the Metropolitan Police;
- the Chief Constable of the Police Service of Northern Ireland (PSNI);
- the Police Service of Scotland;
- the Commissioners of HM Revenue and Customs (HMRC); and
- the Chief of Defence Intelligence, Ministry of Defence.[222]

The interception warrants have to be issued by a Secretary of State (usually the Foreign Secretary, Home Secretary, Defence Secretary, Secretary of State for Northern Ireland, or the Cabinet Secretary for Justice for Scotland).[223]

Sir Anthony May has concluded that "the Secretaries of State and the agencies that undertake

220. 'Acquisition and Disclosure of Communications Data: DRAFT Code of Practice', Home Office (2015), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409562/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice__web_....pdf, last visited: 29 April 2015, p. 19.

221. Ibid., p. 20.

222. 'What we do: Interception inspections', *Interception of Communications Commissioner's Office*, available at: http://www.iocco-uk.info/sections.asp?sectionID=2&chapter=3&type=top, last visited: 17 March 2015.

223. Ibid.

interception operations under RIPA 2000 Chapter I Part I do so lawfully, conscientiously, effectively and in the national interest",[224] and that they were "entirely conscientious in undertaking their RIPA 2000 Part I Chapter I duties. They do not rubber stamp applications. On the contrary, they sometimes reject applications or require more information."[225] As a 2015 ISC report stated, a "warrant application would not reach the Home Secretary's desk unless it was considered necessary, proportionate and legal",[226] and Sir Malcolm Rifkind has confirmed that:

> These applications are no mere formality. The Agencies must make a detailed case, normally running to several pages. Warrants are subject to retrospective examination by Commissioners, who are, or have been, very senior judges, to check that applications are lawful and that the subsequent use of any warrant was consistent with those applications.[227]

2.4.2 INTELLIGENCE AND SECURITY COMMITTEE

The Intelligence and Security Committee of Parliament (ISC) was created by the Intelligence Services Act 1994. It is the all-party, parliamentary oversight body relating to GCHQ; MI5; and MI6,[228] and the principal way in which the agencies can be scrutinised by Parliament.

Initially, the ISC existed largely to examine expenditure and other administrative functions of the Agencies over which it had jurisdiction. While it did have access to sensitive material, it only had what a former Chair of the ISC has described as "seriously restricted" powers to act as an effective oversight body.[229]

However, the Justice and Security Act 2013 enhanced the scope of the ISC's investigatory powers – giving it more access to operational activity and correspondence, as opposed to just policy and performance.[230] For example:

- the Chair of the ISC is now appointed by the Committee, rather than by the Prime Minister;
- if the ISC requests information from the intelligence services, these services now have a legal requirement to supply it. The ISC staff can even go into the office of intelligence agencies and, with agency staff, pick the files that they wish to see;[231] before, the ISC could only 'request' such information. Only a Secretary of State can now choose to withhold the information, as opposed to a head of one of the intelligence services;[232]
- there has been a doubling in budget and a rise in staffing; and
- the ISC has statutory responsibility for the oversight of Agency operations. MI5; MI6;

224. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 18.

225. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 11.

226. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 74.

227. Rifkind, M., 'Intelligence Agencies in the Internet Age - Public Servants or Public Threat?', *Wadham Lecture – Wadham College, Oxford*, 8 May 2014, available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20140508_ISC_Wadham_lecture.pdf?attachauth=ANoY7cpueJLbNLJp3o-hCV6E8cIPOJvlpQzgVh28RYHV4hNt2NDWsA6hrJuNCHjbHZ_WMv6ghKslZg3zsPS87V9kzV71Rr-8G2NoJrBSBv2E3-bpEaBfos5v3k3sA4F5y57VYtYlk9YmM5yyU_8p4nE94-aEkYgfRV3xwzAIzgTwQ3276RuD4xcr4JUM2Um-vaut20DOSI_THNfgN1dY-2Yc5f1xh9ry_U-QC4hKluCCIPmmfH2KI1I%3D&attredirects=2, last visited: 17 March 2015.

228. 'The law', *Government Communications Headquarters*, available at: www.gchq.gov.uk/how_we_work/running_the_business/oversight/Pages/the-law.aspx, last visited: 17 March 2015.

229. Rifkind, M., 'Intelligence Agencies in the Internet Age', *Wadham Lecture – Wadham College, Oxford*, 8 May 2014.

230. 'Annual Report 2012–2013', Intelligence and Security Committee of Parliament (2013), available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/211553/31176_HC_547_ISC.PDF, last visited: 17 March 2015.

231. Rifkind, M., 'Intelligence Agencies in the Internet Age', *Wadham Lecture – Wadham College, Oxford*, 8 May 2014.

232. 'Parliamentary Oversight', *Security Service: MI5*, available at: https://www.mi5.gov.uk/home/about-us/how-we-operate/how-mi5-is-governed/oversight/parliamentary-oversight.html, last visited: 17 March 2015.

> and GCHQ now have to provide detailed information on their operations, on a quarterly basis.[233]

One senior intelligence official has commented that the ISC is now "maxed out", in terms of its powers, and is much more interventionist and intrusive than ever before, including on operational details.[234] However, Lord Carlile, the government's former independent reviewer of terrorism legislation, has commented that, while the ISC is "probably fit for purpose, in an ideal world, you would have an ISC that was treated as fully vetted [and] was able to see absolutely anything, and there would be no discretion […] to say, 'Sorry, we are not giving you that'."[235]

2.4.3 INDEPENDENT COMMISSIONERS

The UK has no FISA Court equivalent; however, quasi-judicial oversight is provided by a variety of individuals who have held high judicial office and now serve as Independent Commissioners and report directly to the Prime Minister. Two Independent Commissioners have oversight over GCHQ: the Intelligence Services Commissioner and the Interception of Communications Commissioner.[236]

The Interception of Communications Commissioner reviews the use of RIPA, Part I (concerning interception) and oversees all agencies that are able to apply for interception warrants and communications data requests (including GCHQ).[237] The Commissioner also audits the lawfulness of the interception of content (and related communications data) and the "acquisition and disclosure" of communications data;[238] reviews warrants and certificates issued by the Secretaries of State;[239] and carries out content (and related communications data) audits, approximately twice a year, on the nine interception authorities.[240] It carries out additional inspections on a number of other public authorities in relation to communications data.

Hazel Blears MP, a member of the ISC, has praised the Commissioners' work, particularly regarding the scrutiny that they offer and their ability to meet any public-awareness issues that have arisen since Snowden's disclosures.[241] Yet, there has been some suggestion that their roles may have to be modified in order to help provide a more public voice on the state's part in interception. For example, one official has described the Commissioners as not "select-committee friendly", and has said that their discomfort with operating in the public eye has made the work of British intelligence agencies "vulnerable".[242] Yvette Cooper, speaking as the Shadow Home Secretary, has suggested that the Commissioners are performing inadequately and that what the government may need is one inspector general who has oversight over all intelligence agencies.[243] Others have questioned whether so many commissioners are needed, and feel that the absence of any enforcement powers and financial clout mean that they lack the authority to perform their

233. Rifkind, M., 'Intelligence Agencies in the Internet Age', *Wadham Lecture – Wadham College, Oxford*, 8 May 2014.

234. Private conversation.

235. Interview with Lord Carlile, September 2014.

236. 'The law', *Government Communications Headquarters*.

237. 'Privacy International et al. v. The Government Communications Headquarters et al. – Witness Statement of Charles Blandford Farr on Behalf of the Respondents', Investigatory Powers Tribunal (2014), p. 27.

238. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 3.

239. 'Interception of Communications: Code of Practice', UK Home Office (2007), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf, last visited: 17 March 2015, p. 27.

240. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 9.

241. Telephone interview with Hazel Blears MP, September 2014.

242. Private conversation.

243. 'Labour to overhaul spy agency controls in response to Snowden files', *The Guardian*, 02 March 2014.

oversight tasks adequately.

Julian Huppert, a Liberal Democrat MP who sat on the Joint Committee on the Communications Data Bill, has also voiced concerns about the relationship between the Commissioners and the intelligence agencies, calling it "far, far too cosy".[244] However, Sir Anthony May, the current Interception of Communications Commissioner, has been described, by one official, as "not instinctively pro-establishment".[245] (May was one of the senior judges who ruled against the government when it attempted to redact information regarding MI5 knowledge of the alleged torture of former Guantánamo Bay detainee Binyam Mohamed.[246]) In addition, the Commissioners have no enforcement powers and no direct impact on setting the policy. As Sir Malcolm Rifkind says, their roles are "like an accountant looking at a tax return; he doesn't look to see if tax policy is right or wrong".[247]

2.4.4 INVESTIGATORY POWERS TRIBUNAL

One further level of quasi-judicial oversight is provided by the IPT, a body formed as part of RIPA (in 2000) that consists of judges and lawyers. The IPT is responsible for investigating complaints regarding the use of RIPA (including the collection, storage, and use of data by the intelligence agencies) and for ensuring that the authorities' activities comply with the Human Rights Act.[248] A public authority has acted unlawfully if "it fails to obtain lawful authority or there is no lawful authority possible for infringing your human rights", or "if it breaches your rights by incorrectly balancing them against the public interest."[249] However, at present, these cases can only be appealed to the European Court of Human Rights, in Strasbourg; there is no domestic right of appeal – something that the ISC now recommends be rectified.[250] Furthermore, this mechanism can only be referred to retrospectively, after potential mistakes or wrongdoing by the state have already occurred.

2.4.5 A CULTURE OF SELF-REGULATION?

When speaking as GCHQ Director, Sir Iain Lobban was keen to stress his agency's "strong culture and ethos of personal accountability."[251] He has stated, "I don't employ the type of people who would [delve into innocent e-mails and phone calls]. My people are motivated by saving the lives of British forces on the battlefield. They're motivated by finding terrorists and serious criminals. If they were asked to snoop I wouldn't have the workforce, they'd leave the building".[252] Similarly, former GCHQ Director Sir David Omand has commented that "self-regulation is the most important form of regulation […] You can have all the rules and all the oversight, but when they are out of your sight, you have to rely on the fact that [your staff] have internalised a code of values."[253]

244. Telephone interview with Julian Huppert MP, August 2014.

245. Private conversation.

246. 'Binyam Mohamed torture evidence must be revealed, judges rule', *The Guardian*, 10 February 2010, available at: http://www.theguardian.com/world/2010/feb/10/binyam-mohamed-torture-ruling-evidence, last visited: 17 March 2015.

247. Telephone interview with Sir Malcolm Rifkind MP, August 2014.

248. 'Surveillance: Citizens and the State', House of Lords – Select Committee on the Constitution (2009), p. 62; see also: 'Functions - Key role', *Investigatory Powers Tribunal*, 11 June 2014, available at: http://www.ipt-uk.com/section.aspx?pageid=1, last visited: 17 March 2015.

249. 'Functions - Legislative Basis', *Investigatory Powers Tribunal*, 29 June 2014, available at: http://www.ipt-uk.com/section.aspx?pageid=2, last visited: 17 March 2015.

250. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 80.

251. Lobban, I., 'Sir Iain Lobban's valedictory speech - as delivered', *Government Communications Headquarters*, 21 October 2014.

252. 'Spying leaks "help terrorists and paedophiles," says GCHQ director', *London Evening Standard*, 07 November 2013, available at: http://www.standard.co.uk/news/politics/spying-leaks-help-terrorists-and-paedophiles-says-gchq-director-8927528.html, last visited: 17 March 2015.

253. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 76.

This does not mean, though, that there have not been mistakes or occasional wrongdoing – this in inevitable in such large organisations. For example, there has been a case where GCHQ fired a staff member for inappropriate use of its systems,[254] and MI5 and MI6 have both disciplined or dismissed staff for "inappropriately accessing personal information".[255] Furthermore, administrative errors – officers typing in e-mail addresses and phone numbers incorrectly – can also lead to data being collected on individuals of no relevance to an investigation. In 2014, according to the Interception of Communications Commissioner, there were 998 errors relating to communications data, out of a total of 517, 208 notices and authorisations; and 60 interception errors.[256]

PUBLIC OPINION

Public response to the Snowden leaks has differed in both the US and the UK.

A poll from the *Pew Research Center* and *The Washington Post*, in June 2013, found that 56% of Americans believed that "getting secret court orders to track telephone calls of millions of Americans in an effort to investigate terrorism" was "acceptable".[257] In contrast, 58% of people surveyed in a *CBS News* poll that same month disapproved of the government "collecting phone records of ordinary Americans".[258] A *Gallup* poll – also in June 2013 – saw 44% of respondents approving of Snowden's actions, whereas 42% disapproved.[259]

A more recent *Pew* poll, in November 2014, found that 80% of Americans believed that the public "should be concerned about the government's monitoring of phone calls and internet communications." As Congressman Peter King has said, "Cynicism is spreading, and it's taking away support for the government."[260]

The UK response has also been ambivalent. A June 2013 poll by *YouGov* found that only 27% thought that Snowden was wrong "to give information on how the US government was monitoring telephone calls and emails to the press."[261] Yet, an October 2013 poll by the same company showed that Snowden's disclosures had not led to clamour for reining in the British security services' powers; only 19% believed that the authorities had too many powers, with 42% believing that the balance was about right, and 22% believing that they had insufficient powers. By then, more people also regarded the Snowden leaks as a bad thing (43%) than a good thing (35%).[262] Prime Minister David Cameron has commented that he believes that the public was "unmoved" by the disclosures, and that "the public reaction has not been one of shock horror. It has been much more one of 'intelligence agencies carry out intelligence work, good'."[263]

254. Ibid., p. 46.

255. Ibid., p. 58.

256. May, A., 'Report of the Interception of Communications Commissioner: March 2015 (covering the period January to December 2014)', Interception of Communications Commissioner's Office (2015), p. 39, 70.

257. 'Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic', *Pew Research Center*, 10 June 2013, available at: http://www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/, last visited: 17 March 2015.

258. 'Most disapprove of gov't phone snooping of ordinary Americans', *CBS News*, 12 June 2013, available at: http://www.cbsnews.com/news/most-disapprove-of-govt-phone-snooping-of-ordinary-americans/, last visited: 17 March 2015.

259. 'Americans Disapprove of Government Surveillance Programs', *Gallup*, 12 June 2013, available at: http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx, last visited: 17 March 2015.

260. Interview with Congressman Peter King, July 2014.

261. 'Edward Snowden: Hero?', *YouGov*, 16 June 2013, available at: https://yougov.co.uk/news/2013/06/16/edward-snowden-hero/, last visited: 17 March 2015.

262. 'Little appetite for scaling back surveillance', *YouGov*, 13 October 2013, available at: http://yougov.co.uk/news/2013/10/13/little-appetite-scaling-back-surveillance/, last visited: 17 March 2015.

263. 'Cameron says he failed to make case for mass surveillance after Snowden leaks', *The Guardian*, 30 January 2014, available at: http://www.theguardian.com/politics/2014/jan/30/cameron-failed-mass-surveillance-snowden-communication-laws, last visited: 17 March 2015.

Therefore, while Snowden himself may poll well, the consequence is not a call to rein in the state's powers; there appears to be sympathy for the notion that safeguarding national security is a challenging task and that the police and security services require relatively broad powers in order to do so.

3. IMPACT

3.1 THE CONSEQUENCES OF THE SNOWDEN LEAKS

Government officials from both the US and the UK have stressed the significant national-security impact of Snowden's actions.

Lieutenant General Michael Flynn, the former head of the Defense Intelligence Agency (DIA), has suggested that "Snowden's disclosures have done grave damage to the Department of Defense".[264] James Clapper, the DNI, has said that they have caused "profound damage […] putting the lives of members or assets of the intelligence community at risk, as well as those of our armed forces, diplomats, and our citizens".[265] David Omand, a former Director of GCHQ, has commented that "substantial damage to UK security has been caused by the Snowden revelations",[266] and, in October 2013, the MI5 Director General, Andrew Parker, labelled disclosures about GCHQ's work a "gift" for terrorists.[267]

The precise impact that Snowden's leaks have made is not always easy to quantify. A DIA assessment of his disclosures was that "[t]he scope of the compromised knowledge related to US intelligence capabilities is staggering."[268] However, this was based on the assumption that Snowden's master file contained data from every network he scanned, and that America's adversaries either possess this file or will do so eventually. The DIA is working to a worst-case scenario: the assumption that everything which Snowden touched was stolen;[269] we still do not know if this was the case.

Nevertheless, certain trends have emerged. The following section attempts to summarise the tangible impact that Snowden has had on intelligence agencies' work.

3.1.1 REVEALING CAPACITY

The public airing of certain intelligence-gathering techniques has polluted ongoing operations, due to fear of discovery and/or attribution.[270] As they can no longer be run safely, such intelligence gathering has had to stop.[271] With state actors, there is also a fear that the West's adversaries will read and adapt the methodologies that are displayed in the Snowden files: China and Russia, for example, deploying the NSA's and GCHQ's own cyber strategies against them.[272]

For terror suspects, the disclosures have enabled them to "now understand the scope and scale of

264. 'Intelligence Leaders Detail Global Threats to Senate Panel', *American Forces Press Service*, 11 February 2014, available at: http://www.defense.gov/news/newsarticle.aspx?id=121644, last visited: 18 March 2015.

265. 'Remarks as Delivered by James R. Clapper, Director of National Intelligence', Office of the Director of National Intelligence Public Affairs Office (2014).

266. '"Snowden's leaks scupper surveillance of crime gangs"', *The Sunday Times*, 8 June 2014, available at: http://www.thesundaytimes.co.uk/sto/news/uk_news/Defence/article1420212.ece, last visited: 15 April 2015.

267. 'Director General's Speech at RUSI, 2013', *Security Service: MI5*, 8 October 2013, available at: https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/director-generals-speech-at-rusi-2013.html, last visited: 18 March 2015.

268. 'DoD Information Review Task Force-2: Initial Assessment', Information Review Task Force-2 – Defense Intelligence Agency (2013), available at: http://www.theguardian.com/world/interactive/2014/may/22/pentagon-report-snowden-leaks-damage-report, last visited: 18 March 2015.

269. 'Snowden Keeps Outwitting U.S. Spies', *The Daily Beast*, 6 February 2014, available at: http://www.thedailybeast.com/articles/2014/02/06/snowden-still-outwitting-u-s-spies.html, last visited: 18 March 2015.

270. '"Snowden's leaks scupper surveillance of crime gangs"', *The Sunday Times*, 08 June 2014.

271. Private conversation.

272. Private conversation.

Western collection capabilities".[273] In January 2015, a seven-and-a-half-minute video was released onto a jihadist platform, outlining some of what had been discerned from Snowden's disclosures about spy agencies' activities. For example, the video stated that:

> All mobile phone providers use the same software, your device continuously is in contact with the nearest tower […] As you are moving around your different coordinates are tracked and stored. All your calls, messages and internet history are stored in this same place […] spies have access to these files and can know your daily routine, friends and what you are planning to do tomorrow night at that tall building […] Every Mujahed that does not take the right precautions can be a tool in the hand of the enemy. With his phone, tablet or laptop the enemy can listen/record all conversations and meetings.[274]

The video also stated that governments work with internet companies in order to obtain the information. It then provided advice on how to avoid detection, listing software packages that protect against surveillance and from where they can be acquired.[275]

There are other ways in which Western intelligence agencies' capacities have been revealed. To give former Deputy Director of the NSA Chris Inglis's example, "[i]t might be surprising to someone that a communication that makes its way from, say, some ungoverned space in the north of southwest Asia to a place like Yemen sometimes transits through the United States of America."[276]

According to the former deputy director of the CIA, Michael Morell, the Section 702 program was particularly impacted by this, as foreign terror suspects now not only realised that their electronic communications often passed through the US (even if the individuals themselves were not based there), but also which CSPs were allowing the NSA to access these communications. These suspects subsequently stopped using these CSP's services to send emails, for example, or even stopped using electronic communications entirely.[277]

Morell has gone as far as to state that it was "clear" that Snowden's leaks also "played a role in the rise" of the Islamic State. Morell said the group had "learned from Snowden". However, this is not a consensus view within the intelligence community. Some have suggested that the Islamic State was already aware its communications were being targeted having been the subject of major NSA and military surveillance and hacking campaign during the 2007-08 period of the Iraq war.[278]

273. Nicholas Rasmussen, Director of the National Counterterrorism Center, quoted in 'Snowden Leaks Didn't Make Al Qaeda Change Tactics, Says Report', *NBC News*, 16 September 2014, available at: http://www.nbcnews.com/storyline/nsa-snooping/snowden-leaks-didnt-make-al-qaeda-change-tactics-says-report-n203731, last visited: 18 March 2015.

274. 'Al Qaeda's YouTube guide for jihadists', *Daily Mail*, 20 January 2015, available at: http://www.dailymail.co.uk/news/article-2916475/Al-Qaeda-YouTube-video-shows-jihadists-using-Snowden-leaks-evade-Western-surveillance.html, last visited: 18 March 2015.

275. Ibid.

276. 'Transcript: NSA Deputy Director John Inglis', *NPR*, 10 January 2014.

277. 'CIA's Ex-No. 2 Says ISIS "Learned From Snowden"', *The Daily Beast*, 6 May 2015.

278. Ibid.

THE INTELLIGENCE AGENCY OMNIPOTENCE MYTH

The NSA's capacity is impressive; but it has also been exaggerated. In a 2013 report, the agency stated that "the Internet carries 1,826 Petabytes of information per day […The] NSA touches about 1.6% of that […and,] of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic […] less than one part in a million."[279] The same is true of GCHQ; one intelligence official was particularly withering of the idea that "5,000 people in Cheltenham can process the Internet".[280]

3.1.2 CHANGES IN TARGET BEHAVIOUR AND COMMUNICATION METHODS

Snowden's disclosures have led to changes in the way that suspects communicate. One senior US intelligence official said that, post-Snowden, the shift in communication methods was the "most significant change" that had taken place.[281] Other senior individuals have corroborated that this change in communication methods took place, including Matt Olsen, the former Director of the National Counterterrorism Center;[282] Dutch Ruppersberger, a former Ranking Member on the House of Representatives' intelligence committee;[283] Michael Morell;[284] and Admiral Michael S. Rogers, the head of the NSA.[285] Speaking in November 2013, while still Chair of the House of Representatives Permanent Select Committee on Intelligence, Mike Rogers (not to be confused with Michael S. Rogers) said that Snowden's disclosures had allowed "three different terrorist organizations, affiliates of al Qaeda to change the way they communicate".[286]

This communications shift has impacted the UK as well. In December 2014, a senior UK security official suggested that intelligence agencies "have specific evidence of where key targets have changed their communication behaviour as a direct result of what they have read", adding that "because we only focus on the most serious, the top end networks, then the impact they have in the mean time is multiplied."[287]

It is not easy to prove that security agencies losing track of a certain target, for example, is specifically down to the information that Snowden passed to journalists; yet, intelligence sources have attempted to provide an insight into the day-to-day impact that Snowden has had on their work:

- In June 2014, one British intelligence source said that GCHQ's ability to track domestic and foreign crime gangs – including those relating to people trafficking and drugs – had been reduced by approximately 25%.[288] The same number was cited by intelligence

279. 'The National Security Agency: Missions, Authorities, Oversight and Partnerships', National Security Agency (2013), p. 6.

280. Private conversation.

281. Private conversation.

282. 'Transcript: Senate Intelligence hearing on national security threats', *The Washington Post*, 29 January 2014, available at: http://www.washingtonpost.com/world/national-security/transcript-senate-intelligence-hearing-on-national-security-threats/2014/01/29/b5913184-8912-11e3-833c-33098f9e5267_story.html, last visited: 18 March 2015.

283. 'Snowden's Damage', *The Wall Street Journal*, 10 January 2014, available at: http://online.wsj.com/news/articles/SB10001424052702304347904579310813434692676, last visited: 18 March 2015.

284. 'CIA's Ex-No. 2 Says ISIS "Learned From Snowden"', *The Daily Beast*, 6 May 2015.

285. 'New N.S.A. Chief Calls Damage From Snowden Leaks Manageable', *The New York Times*, 29 June 2014, available at: http://www.nytimes.com/2014/06/30/us/sky-isnt-falling-after-snowden-nsa-chief-says.html?_r=0, last visited: 18 March 2015.

286. Joscelyn, T., 'House Intel Chair: Snowden Leaks Tipped Off Al Qaeda', *The Weekly Standard*, 4 November 2013, available at: http://www.weeklystandard.com/blogs/house-intel-chair-snowden-leaks-tipped-al-qaeda_765838.html, last visited: 18 March 2015.

287. 'GCHQ warns serious criminals have been lost in wake of Edward Snowden leaks', *The Telegraph*, 21 December 2014, available at: http://www.telegraph.co.uk/news/uknews/law-and-order/11300936/GCHQ-warns-serious-criminals-have-been-lost-in-wake-of-Edward-Snowden-leaks.html, last visited: 18 March 2015.

288. '"Snowden's leaks scupper surveillance of crime gangs"', *The Sunday Times*, 8 June 2014.

sources, in December 2014.[289]

- In October 2014, a top GCHQ spy tasked with cracking the communications of high-value national-security targets stated that his work sometimes take three times as long now, when compared to before the Snowden disclosures (six weeks instead of two).[290] Another spy, tasked with hacking terrorist activities on the internet, stated that Snowden had made the job "a thousand times more difficult".[291]

- In the same month, Olsen said that, in the US, "people that we were concerned about, we are no longer collecting their communications. We lost insight into what they were doing."[292]

Ultimately, according to Clapper, that "[t]errorists and other adversaries of this country are going to school on […] intelligence sources, methods, and tradecraft. And the insights they're gaining are making our job […] much, much harder."[293]

3.1.3 NEW ENCRYPTION TECHNIQUES

Further significant shifts by terrorist groups have been the development of new encryption technology and even greater caution regarding being detected electronically.[294] This has been confirmed by several serving, as well as former, intelligence officials.[295]

Online jihadist platforms released new encryption tools at a quicker pace following the Snowden revelations. According to one analysis, three significant encryption tools were released "within a three to five month time frame of the leaks."[296] For example, the *Global Islamic Media Front* released a new mobile-encryption program in September 2013.[297] Similarly, the *al-Fajr Technical Committee*, which distributes al-Qaeda propaganda, has released multiple versions of an encryption programs for e-mails; text messages; and instant messages.[298]

There has also been an exponential increase in the use of encryption by CSPs (for further details, see p. 63 – 64).

289. 'GCHQ warns serious criminals have been lost in wake of Edward Snowden leaks', *The Telegraph*, 21 December 2014.

290. 'GCHQ: "This is not Blitz Britain. We sure as hell can't lick terrorism on our own"', *The Telegraph*, 11 October 2014, available at: http://www.telegraph.co.uk/news/uknews/defence/11154322/GCHQ-This-is-not-Blitz-Britain.-We-sure-as-hell-cant-lick-terrorism-on-our-own.html, last visited: 18 March 2015.

291. Ibid.

292. 'Ex-counterterror chief: U.S. lost track of terrorists after Snowden', *CNN*, 21 October 2014, available at: http://thelead.blogs.cnn.com/2014/10/21/ex-counterterror-chief-u-s-lost-track-of-terrorists-after-snowden/, last visited: 30 April 2015.

293. 'Remarks as Delivered by James R. Clapper, Director of National Intelligence', Office of the Director of National Intelligence Public Affairs Office (2014).

294. It is worth noting that previous issues of *Inspire*, al-Qaeda in the Arabian Peninsula's English-language propaganda magazine, had provided a public key to access *Asrar al-Mujahideen*, their encryption-software program, enabling readers to contact the group. Yet, the issue after the Snowden leaks stated that, "due to technical and security reasons," they had stopped using certain e-mail addresses and were not providing an encryption key. See: 'al-Qaeda's Embrace Of Encryption Technology Part III – July 2014-January 2015', *The Cyber & Jihad Lab*, 5 February 2015, available at: http://cjlab.memri.org/analysis-and-special-reports/al-qaedas-embrace-of-encryption-technology-part-iii-july-2014-january-2015-islamic-state-isis-and-other-jihadis-continue-to-develop-their-cyber-and-encryption-capabilities-post-snowden/, last visited: 15 April 2015; see also: *Inspire*, Issue 12 (2014), available at: https://azelin.files.wordpress.com/2014/04/inspire-magazine-issue-12.pdf, last visited: 18 March 2015.

295. This consensus has been challenged by Flashpoint Global Partners. See'Snowden Leaks Didn't Make Al Qaeda Change Tactics, Says Report', *NBC News*, 16 September 2014.

296. 'How Al-Qaeda Uses Encryption Post-Snowden (Part 1)', *Recorded Future*, 8 May 2014, available at: https://www.recordedfuture.com/al-qaeda-encryption-technology-part-1/, last visited: 18 March 2015.

297. Ibid.

298. 'Al-Fajr Technical Committee Releases Android App For Secure Communication, Announces New Website', *The Cyber & Jihad Lab*, 11 June 2014, available at: http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/al-fajr-technical-committee-releases-android-app-for-secure-communication-announces-new-website/, last visited: 18 March 2015.

3.1.4 OPERATIONAL CONSEQUENCES

Snowden created digital keys which allowed him to access various intelligence and military systems. Considering the contact that he has had with the Russian security service, the FSB, this is an obvious cause of concern, particularly given that his access was not limited to material relating to communications interception. US fears are that, such are the cyber capabilities of Russian and Chinese intelligence agencies, they could have accessed this and similar information from Snowden's files, even without his knowledge.[299] Lieutenant General Michael Flynn has called this a prospect "very serious", warning that even "if [the Russians] don't have access, you have to assume that they are going to try to".[300]

Furthermore, James Clapper, has stated that "what [Snowden] did, what he took, what he has exposed, goes way, way, way beyond the so-called domestic surveillance programs."[301] (Congressman Peter King appears to concur, claiming that the "overwhelming percentage of what Snowden took was military and military-countermeasures" information.[302]) According to Clapper, of the files that Snowden had access to – and, therefore, potentially took – approximately "less than 10 percent has to do with domestic surveillance."[303]

Certainly, it is hard to make the civil-liberties case for disclosing:

- that the NSA had received permission to spy on groups such as the Muslim Brotherhood;
- that the Norwegian Intelligence Service assisted the NSA in collecting intelligence regarding Russian energy policy and military activities;
- that the Swedish Defence Radio Establishment works with the NSA to gain intelligence on Russia;
- that the NSA was considering forming an intelligence-sharing partnership with Vietnam;
- that GCHQ intended to target the communications of Turkish and South African diplomats;[304]
- the location of NSA offices, bases, and analysts across the world;[305]
- US attempts to spy on China and Hong Kong;[306]

299. Sanger, D. and Eric Schmitt, 'Congressional Leaders Suggest Earlier Snowden Link to Russia', *The New York Times*, 19 January 2014, available at: http://www.nytimes.com/2014/01/20/us/politics/congressional-leaders-suggest-snowden-was-working-for-russia.html?_r=0, last visited: 27 March 2015.

300. 'Transcript: Interview With Lt. Gen. Michael Flynn', *NPR*, 7 March 2014, available at: http://www.npr.org/2014/03/07/287037148/transcript-interview-with-lt-gen-michael-flynn, last visited: 27 March 2015.

301. 'Spy Chief James Clapper: We Can't Stop Another Snowden', *The Daily Beast*, 23 February 2014, available at: http://www.thedailybeast.com/articles/2014/02/23/spy-chief-we-can-t-stop-another-snowden.html, last visited: 18 March 2015.

302. Interview with Congressman Peter King, July 2014.

303. 'Clapper: Most of data stolen by Snowden not on domestic programs', *The Hill*, 4 February 2014, available at: http://thehill.com/policy/defense/197429-officials-on-snowden-10-percent-of-stolen-data-was-domestic, last visited: 18 March 2015.

304. 'GCHQ intercepted foreign politicians' communications at G20 summits', *The Guardian*, 17 June 2013, available at: http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits, last visited: 18 March 2015.

305. 'Catalog of the Snowden Revelations', *Lawfare*, available at: http://www.lawfareblog.com/catalog-of-the-snowden-revelations/, last visited: 18 March 2015.

306. 'Edward Snowden: US government has been hacking Hong Kong and China for years', *South China Morning Post*, 14 June 2013, available at: http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china, last visited: 18 March 2015.

- the NSA's interception of then Russian President Dmitry Medvedev's communications;[307]
- that President Obama had asked for a list of potential foreign targets for a US cyber attacks;[308] and
- portions of the US-intelligence budget.[309]

Indeed, when General Martin Dempsey (the chairman of the Joint Chiefs of Staff) testified before the House Armed Services Committee, in March 2014, he explained that the "vast majority of the documents that Snowden […] exfiltrated […] were related to our military capabilities, operations, tactics, techniques and procedures."[310]

As a result, it is Flynn's opinion that Snowden "has placed the men and women of our armed services at risk […] and that his disclosures will cost lives on our future battlefields."[311] This was seconded by Mike Rogers, former Chairman of the Permanent Select Committee on Intelligence, who said that "Snowden's actions are likely to have lethal consequences for our troops in the field."[312] Rogers has gone as far as to say that Snowden should be charged with murder as a result.[313]

3.1.5 COMMUNICATION SERVICE PROVIDER BACKLASH

Interception of communications has historically been carried out in liberal democracies, without significant tension arising between the government and communication carriers. The NSA and GCHQ perceive themselves to be carrying out the same kind of long-standing forms of state interception that they always have: for example, intercepting an envelope, which shows an address and a postmark containing a date and geographic location (the equivalent of communications data), and studying the letter inside the envelope (the equivalent of content).

Yet, following the Snowden disclosures, a significant divide has emerged between the government and the CSPs.[314] *Google*'s chief legal officer has stated that the company was "outraged at the lengths to which the government seems to have gone to intercept data from our private fibre networks".[315] In December 2013, the Executive Vice President and General Counsel at *Microsoft*,

307. 'G20 summit: NSA targeted Russian president Medvedev in London', *The Guardian*, 17 June 2013, available at: http://www.theguardian.com/world/2013/jun/16/nsa-dmitry-medvedev-g20-summit. As the *National Review* stated, "[t]his is not a scandal; it is *literally* the NSA's job" ('Is Rand Paul "Part of that Hate-America Crowd"?', *National Review*, 6 January 2014, available at: http://www.nationalreview.com/campaign-spot/367670/rand-paul-part-hate-america-crowd-jim-geraghty, last visited: 18 March 2015).

308. 'Obama orders US to draw up overseas target list for cyber-attacks', *The Guardian*, 7 June 2013, available at: http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas, last visited: 18 March 2015.

309. '"Black budget" summary details U.S. spy network's successes, failures and objectives', *The Washington Post*, 29 August 2013, available at: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html. To CIA Deputy Director Mike Morell, the most damaging disclosure was the way in which the intelligence community's 'black budget' – the amount of money that the US government gives to the agencies which make up its National Intelligence Program – is spent, as those hostile to the US "could focus their counterintelligence efforts on those places where we're being successful. And not have to worry as much about those places where we're not being successful." ('The Deputy Director: Mike Morell', *CBS News*, 30 October 2013, available at: http://www.cbsnews.com/news/the-deputy-director-mike-morell, last visited: 18 March 2015).

310. 'Was Snowden's Heist a Foreign Espionage Operation?', *The Wall Street Journal*, 9 May 2014, available at: http://www.wsj.com/articles/SB10001424052702304831304579542402390653932, last visited: 18 March 2015.

311. 'Intelligence Leaders Detail Global Threats to Senate Panel', *American Forces Press Service*, 11 February 2014.

312. 'HPSCI Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger -- "Snowden's acts of betrayal truly place America's military men and women in greater danger around the world."', *U.S. House of Representatives Permanent Select Committee on Intelligence*, 09 January 2014, available at: http://intelligence.house.gov/press-release/hpsci-chairman-mike-rogers-and-ranking-member-ca-dutch-ruppersberger-%E2%80%9Csnowden%E2%80%99s-acts, last visited: 18 March 2015.

313. 'Event Transcript: "Safeguarding Our Societies in the Internet Age: National Security, Intelligence and Legal Structures"', *The Henry Jackson Society*, 21 October 2014, available at: http://henryjacksonsociety.org/2014/11/20/event-transcript-safeguarding-our-societies-in-the-internet-age-national-security-intelligence-and-legal-structures/, last visited: 18 March 2015.

314. Masnick, M., 'Thank Snowden: Internet Industry Now Considers The Intelligence Community An Adversary, Not A Partner', *Tech Dirt*, 13 February 2015, available at: https://www.techdirt.com/articles/20150213/07100730015/thank-snowden-internet-industry-now-considers-intelligence-community-adversary-not-partner.shtml, last visited: 18 March 2015.

315. 'Snowden leaks: Google "outraged" at alleged NSA hacking', *BBC News*, 31 October 2013, available at: http://www.bbc.co.uk/news/world-us-canada-24751821, last visited: 18 March 2015.

Brad Smith, said that "government snooping potentially now constitutes an 'advanced persistent threat,' alongside sophisticated malware and cyber attacks."[316]

One senior British security official said that the biggest impact of Snowden's actions were that technology companies were now "disengaging from the security apparatus after years of being helpful within the law".[317] Another said that the public would be "shocked" if it was aware of how little the state could do because of the actions of major technology companies,[318] and GCHQ Director Robert Hannigan went as far as to say that some of the companies were "in denial" about the problem.[319]

This CSP backlash has manifested itself in different ways. Admiral Rogers has commented that CSPs are now telling government that "you are going to have to compel us" to provide data, so that they can prove to their customers that this is not a voluntary arrangement.[320] In theory, this is not necessarily a huge shift; the response of one CSP to the first story ever published about so-called 'warrantless surveillance' – in the *New York Times*, in December 2005 –[321] was to ask the government to compel them to provide the information via court order, rather than it be a voluntary arrangement.[322] The difference now is that there is a mood of greater intransigence from CSPs towards governments because Snowden exposed the extent of their interaction. This is a severe problem, because co-operation is needed: the usual way for the government to access the content of communications is by serving an interception warrant against a CSP, which, in turn, provides the information.[323]

Arguments used by one major US-based technology company in refusing to respond to a UK-government request for content data are now said to be as follows:

- that they are a software platform, not a CSP, and should not be legally bound as if they were;
- even if they are a CSP, they are primarily based in the US and are, therefore, bound by US law;
- it would be illegal, under US law, to provide the data, as Title III of the Omnibus Crime Control and Safe Streets Act 1968 (the Wiretap Act) "prohibits the unauthorized, nonconsensual interception of 'wire, oral, or electronic communications' by government agencies as well as private parties";[324] and
- they cannot obey the laws of all other jurisdictions – i.e. Russia – so why should they follow UK law?

To intelligence officials, this is unreasonable: "if financial or pharmaceutical services want to deliver a service, they have to comply with UK law; why not the CSPs?" asked one.[325] A US official

316. 'Protecting customer data from government snooping', *Microsoft*, 4 December 2013, available at: http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/, last visited: 18 March 2015.

317. Private conversation.

318. Private conversation.

319. Hannigan, R., 'The web is a terrorist's command-and-control network of choice', *The Financial Times*, 3 November 2014, available at: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I7Jjs7jf, last visited: 18 March 2015.

320. 'New N.S.A. Chief Calls Damage From Snowden Leaks Manageable', *The New York Times*, 29 June 2014.

321. 'Bush Lets U.S. Spy on Callers Without Courts', *The New York Times*, 28 December 2005.

322. 'ST-09-0002 Working Draft', Office of the Inspector General (2009).

323. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 17.

324. 'Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)', *U.S. Department of Justice, Office of Justice Programs*, 19 September 2013, available at: https://it.ojp.gov/default.aspx?page=1284, last visited: 18 March 2015.

325. Private conversation.

explained that the "trade-off" for a telecommunications company entering a foreign country is that they may be compelled, by that country, to give direct access to call records.[326] Yet, the US companies remain adamant that the UK has no jurisdiction on requests for content in intelligence investigations.[327]

One example of the fault lines that are developing on this emerged in January 2014, when *Microsoft* announced that it would allow foreign customers to have their personal data stored on various servers outside the US;[328] this included a data centre based in Dublin, Republic of Ireland. Storing data on different servers in different countries further obscures jurisdictional lines.[329]

Microsoft challenged a US attempt to access this data; however, a US judge rejected its argument, comparing the request for stored data as analogous to a subpoena – under which information must be provided, regardless of location.[330] The likes of *Apple*, *eBay*, *Verizon*, and *Amazon* have since filed letters in support of *Microsoft*.[331]

Some of the CSPs' concerns on these issues are understandable; they have not only been made to appear as if they cannot protect private data, one report has also argued that they have suffered financially.[332] In 2014, it was suggested that *Verizon* had lost a contract to run telecommunications services in Germany because of the "ties revealed between foreign intelligence agencies" and such companies.[333] After he retired from the NSA, General Alexander said that it could have done "more to set the record straight sooner on companies' commitment to protecting privacy, the lengths to which companies go to do this, the legally compelled nature of these programs, and that these companies comply with the law."[334]

Intelligence officials in both the US and the UK also feel that tech companies in Silicon Valley contain an anti-establishment culture, in which any government interference with the internet must be a negative. Part of this is down to fears about the tech companies' brand in the US, where they perceive themselves to be on the wrong side of public opinion.

While one senior employee at a technology company said that there had not "been a conscious decision in the company to say, 'We're going to push back on more requests with governments', there has been a conscious effort to say, 'We think that government surveillance regimes need reform'."[335] A *Facebook* chief security officer has acknowledged that "[c]ompanies certainly have become more comfortable standing up and showing their commitment to the people who use their services."[336]

326. Private conversation.

327. 'Report on the intelligence relating to the murder of Fusilier Lee Rigby', Intelligence and Security Committee of Parliament (2014), p. 142.

328. 'Microsoft to shield foreign users' data', *The Financial Times*, 22 January 2014, available at: http://www.ft.com/cms/s/0/e14ddf70-8390-11e3-aa65-00144feab7de.html#ixzz3MGRlhIfC, last visited: 18 March 2015.

329. Hill, J., 'Problematic Alternatives: MLAT Reform for the Digital Age', *National Security Journal – Harvard Law School*, 28 January 2015, available at: http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/, last visited: 18 March 2015.

330. 'Microsoft "must release" data held on Dublin server', *BBC News*, 29 April 2014, available at: http://www.bbc.co.uk/news/technology-27191500, last visited: 18 March 2015.

331. 'Tech rivals join Microsoft in fight over US data demand', *BBC News*, 16 December 2014, available at: http://www.bbc.co.uk/news/technology-30494562, last visited: 18 March 2015.

332. Bankston, K., Greene, R., Kehl, D., and Robert Morgus, 'Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity', New America's Open Technology Institute (2014), available at: http://www.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf, last visited: 18 March 2015.

333. 'New N.S.A. Chief Calls Damage From Snowden Leaks Manageable', *The New York Times*, 29 June 2014. For countries such as Germany, this type of move may ultimately be counterproductive, as the NSA is less legally restrained when it comes to tapping into data being stored overseas (see: Byman, D. and Benjamin Wittes, 'Reforming the NSA: How to Spy after Snowden', *Foreign Affairs*, May/June 2014).

334. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 09 May 2014.

335. Private conversation.

336. 'Facebook's security chief on the Snowden effect, the Messenger app backlash and staying optimistic', *The Washington Post*, 12 August 2014, available at: http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/12/facebooks-security-chief-on-the-snowden-effect-the-messenger-app-backlash-and-staying-optimistic/, last visited: 18 March 2015.

One manifestation of this occurred in December 2013, when *Google*; *Apple*; *Facebook*; *Twitter*; *AOL*; *Microsoft*; *LinkedIn*; and *Yahoo!* formed the 'Reform Government Surveillance' coalition.[337] Another, in July 2014, saw seven (albeit very minor) internet-service providers file legal complaints against GCHQ.[338] US telecommunication companies such as *Sprint*, *Verizon*, and *AT&T* have also now begun to push back.[339]

CSP encryption and the government response

Companies' use of ubiquitous encryption has also increased exponentially since Snowden's leaks, meaning that CSPs are automatically providing encryption for users – rather than the users encrypting data themselves.[340] Those to have done this include *Google*, *Microsoft*, *Apple*, *Yahoo!*, and *WhatsApp*;[341] such companies say that this is in response to customers' demand.[342]

This has potential benefits for those in authoritarian regimes. A Chinese citizen typing 'Tiananmen Square' into *Google*, for example, would not necessarily fall foul of their authorities' censorship programme. (However, the Chinese government likely has ways around this: such as using a proxy, so that those who think that they are communicating with *Google* are actually running into China's 'Great Firewall'.) This increase in encryption, a *Google* spokesperson confirmed, has come in response to the Snowden revelations that "underscored our need to strengthen our networks."[343]

This has had a major impact on US and UK security agencies' work. As GCHQ Director Robert Hannigan has said:

> Techniques for encrypting messages or making them anonymous which were once the preserve of the most sophisticated criminals or nation states now come as standard. These are supplemented by freely available programs and apps adding extra layers of security, many of them proudly advertising that they are "Snowden approved".[344]

FBI Director James B. Comey has said that this means, for example, that even the "companies themselves won't be able to unlock phones, laptops, and tablets to reveal photos, documents, e-mail, and recordings stored within."[345] According to a recent ISC report, "[t]he effect of increased privacy controls has been to place some of the communications of [companies'] users beyond the reach of law enforcement and intelligence officers and even, in some cases, beyond the reach of the law courts".[346]

337. 'Global Government Surveillance Reform', *Reform Government Surveillance*, available at: https://www.reformgovernmentsurveillance.com/, last visited: 18 March 2015.

338. 'ISPs take legal action against GCHQ', *BBC News*, 02 July 2014, available at: http://www.bbc.co.uk/news/technology-28106815, last visited: 18 March 2015.

339. 'Telecoms push back on proposed NSA plan', *Associated Press*, 03 March 2014, available at: http://bigstory.ap.org/article/telecoms-push-back-proposed-nsa-plan, last visited: 18 March 2015.

340. Private conversation.

341. 'Apple and Others Encrypt Phones, Fueling Government Standoff', *The Wall Street Journal*, 18 November 2014, available at: http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801, last visited: 18 March 2015; see also: 'The Future of Global Technology, Privacy, and Regulation', The Brookings Institution (2014), available at: http://www.brookings.edu/~/media/events/2014/06/24%20future%20technology/20140624_global_tech_privacy_transcript.pdf, last visited: 18 March 2015.

342. 'Top British Spy Warns of Terrorists' Use of Social Media', *The New York Times*, 4 November 2014, available at: http://www.nytimes.com/2014/11/05/world/europe/GCHQ-director-tech-companies-militants.html?_r=1, last visited: 18 March 2015.

343. 'Google is encrypting search globally. That's bad for the NSA and China's censors.', *The Washington Post*, 12 March 2014, available at: http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/12/google-is-encrypting-search-worldwide-thats-bad-for-the-nsa-and-china/?wpisrc=nl_eve, last visited: 18 March 2015.

344. Hannigan, R., 'The web is a terrorist's command-and-control network of choice', *The Financial Times*, 3 November 2014.

345. Comey, J., 'Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?', *Federal Bureau of Investigation*, 16 October 2014, available at: http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course, last visited: 18 March 2015.

346. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 9.

The existence of a 'data cloud', such as that used by *Apple*, is not a solution. Not everyone backs up their phones regularly, or even chooses to upload to the 'cloud', meaning that law-enforcement and intelligence agencies could be unable to access data of relevance. Furthermore, it is *Apple* that has the keys to the 'cloud'; as Comey says: "[e]ncryption isn't just a technical feature; it's a marketing pitch."[347]

Escalation is inevitable with the NSA and GCHQ being forced to step up their efforts to break into these networks. As General Alexander has said:

> [w]hen the government asks NSA to collect intelligence on terrorist X, and he uses publicly available tools to encode his messages, it is not acceptable for a foreign intelligence agency like NSA to respond, "Sorry we cannot understand what he is saying". Our job is to break the codes […].

He continued:

> To ask NSA not to look for weaknesses in the technology that we use, and to not seek to break the codes our adversaries employ to encrypt their messages is, I think, misguided. I would love to have all the terrorists just use that one little sandbox over there so that we could focus on them. But they don't. They use the same technology products and the same web services that we've all got.[348]

The status quo cannot be allowed to continue. As GCHQ Director Robert Hannigan recently stated, "[h]owever much they may dislike it, [technology companies] have become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us."[349] Better co-operation between the government and CSPs is needed urgently.

MUTUAL LEGAL ASSISTANCE TREATIES

The Mutual Legal Assistance Treaty (MLAT) process is a "system of bilateral and multilateral agreements by which nation states commit to assist one another in criminal investigations and prosecutions."[350]

As CSPs place jurisdictional boundaries on data sharing, they tend to favour the use of the MLAT process when it comes to data sharing between nations.[351] One official from a major tech corporation has said that, at present, if UK authorities are attempting to access content from that company's servers, that type of request would be pushed to an MLAT and could not be fulfilled until approval was received from a US court.[352] This is not something that the UK government accepts, as it claims that RIPA has extraterritorial jurisdiction.[353]

In addition, the MLAT process is extremely slow. The same tech official acknowledged that some MLATs can take months or even years;[354] on average, it takes the DoJ 10 months to process

347. Comey, J., 'Going Dark', *Federal Bureau of Investigation*, 16 October 2014.

348. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 9 May 2014.

349. Hannigan, R., 'The web is a terrorist's command-and-control network of choice', *The Financial Times*, 3 November 2014.

350. Hill, J., 'Problematic Alternatives: MLAT Reform for the Digital Age', *National Security Journal – Harvard Law School*, 28 January 2015.

351. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), p. 67.

352. Private conversation.

353. 'Report on the intelligence relating to the murder of Fusilier Lee Rigby', Intelligence and Security Committee of Parliament (2014), p. 141.

354. Private conversation.

an MLAT request.[355] If a terrorist plot is unfolding and data is needed immediately, relying on this system is clearly unrealistic. This is something that even MLAT defenders acknowledge, recognising that the system needs reform and the appointment of more judges. However, that is still not a satisfactory fix because MLATs are essentially focused on data sharing for crimes that have already been committed. Agencies such as the NSA and GCHQ, on the other hand, aim to be pre-emptive; they need to carry out interception in order to disrupt possible criminal activity in its planning stages, not after it has already been performed.

Charles Farr is sceptical about their use, saying, "MLATs have not been designed […] to facilitate ongoing investigations on a day to day basis […] Neither we nor the Department of Justice can easily see how an MLAT can be transformed into an almost real-time tool for the exchange of data."[356] Furthermore, MLATs can cost around £10,000 a case; a law-enforcement agency with a small budget is unlikely to use it if this continues to be the cost. While reform to the MLAT system way be worthwhile on its own merits, it is unlikely to be the answer to the current data-sharing issues.

355. 'Liberty and Security in a Changing World', The President's Review Group on Intelligence and Communications Technologies (2013), p. 227.

356. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), p. 66.

4. FUTURE CONSIDERATIONS

4.1 POLICY ISSUES

4.1.1 State access to data may actually be insufficient, rather than excessive

There is a significant problem regarding governments' diminishing ability to access communications data.

Issue A: An evolution in communication methods

SIGINT, the interception of foreign communications and information systems, has historically occurred via telegram; telephone; fax; or e-mail. Local calls were carried by wire, and international calls by microwave towers which were used to transmit signals via radio; however, most communications today travel through fibre-optic cables. Similarly, telephone communications and access to the internet used to mainly take place via a fixed landline; they now increasingly use broadband and mobile networks. This has been accompanied by a flourishing in communications methods: SMS messages, video messaging, instant messaging (such as *WhatsApp* and *Blackberry Messenger*), *Skype*, and social-network platforms.

Issue B: A decline in the need for companies to generate Communications Data

Service providers previously needed to know who was called; where; and for how long, for billing reasons.[357] However, increasing numbers of people pay a fixed-price monthly direct debit or, alternatively, a pay-as-you-go fee, making these factors increasingly irrelevant to CSPs; communications data does not need to be held in order to ensure that customers are paying their bills. Therefore, businesses' rationale for communications data retention, or even generation, is declining. If it is not generated and then retained, then networks of interest to intelligence agencies cannot be reconstructed.

The UK Government's response

In April 2012, the UK government announced that the Home Secretary was attempting to introduce legislation requiring CSPs to store a small number of additional datasets relating to communications data. However, the bill faced significant political opposition – including from Deputy Prime Minister Nick Clegg – for infringing on civil liberties, and was dubbed a 'Snoopers' Charter'.[358] Upon scrutiny by a Parliamentary joint committee, it was concluded that this draft Communications Data Bill paid "insufficient attention to the duty to respect the right to privacy, and [went] much further than it need[ed] or should for the purpose of providing necessary and justifiable official access to communications data."[359] The ISC also encouraged more work to be done.[360]

After this essentially removed any prospect of the Bill passing, the government was forced to the Data Retention and Investigatory Powers Act (DRIPA) 2014, emergency legislation passed in July

357. 'Oral Evidence Taken Before the Joint Committee on the Draft Communications Data Bill – Richard Alcock, Charles Farr and Peter Hill – Questions 1 - 96', House of Lords & House of Commons (2012), available at: http://www.parliament.uk/documents/joint-committees/communications-data/ucJCDCD100712Ev1.pdf, last visited: 18 March 2015, p. 2.

358. See: 'Nick Clegg pledges open hearings over web surveillance plans', *The Guardian*, 3 April 2012, available at: http://www.theguardian.com/politics/2012/apr/03/nick-clegg-open-hearings-surveillance; see also: 'Nick Clegg tries to head off Lib Dem revolt over email surveillance plans', *The Guardian*, 3 April 2012, available at: www.theguardian.com/uk/2012/apr/03/theresa-may-email-surveillance-plans, last visited: 18 March 2015.

359. 'Draft Communications Data Bill, Session 2012-13', Joint Committee on the Draft Communications Data Bill (2012), p. 3.

360. 'Access to communications data by the intelligence and security Agencies', Intelligence and Security Committee of Parliament (2013), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf, last visited: 18 March 2015.

2014. The EU's Data Retention Directive (DRD) of March 2006 – a directive which the UK government played a large role –[361] required telecommunications and internet-service providers to retain communications data for a minimum of six months and a maximum of 24 (Britain kept its data for 12 months).[362] However, in April 2014, the European Union Court of Justice (ECJ) ruled that the DRD was invalid, as it threatened "the fundamental rights to respect for private life and to the protection of personal data."[363] This not only made the UK's legal position unclear; it meant that while the CSPs could still retain some types of data for their own business purposes, they did not have a clear legal basis for retaining it for the length of time that the UK government wished.[364]

The UK responded by passing DRIPA. The bill removed ambiguity by defining telecommunications services as "the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system."[365] DRIPA made clear that even those CSPs which hold data abroad and are based abroad were subject to UK law if there was a warrant or notice served on them compelling them to intercept communications or disclose data (although there is also an important provision in DRIPA outlining that "regard is to be had […] to any requirements or restrictions under the law of that country or territory" in doing so).[366]

DRIPA also required CSPs to retain communication data for up to 12 months.[367] As this ensured the data's retention, this latter requirement was essentially about keeping existing powers, rather than extending them.

Then, in November 2014, the government introduced the Counter-Terrorism and Security Bill, which, among other measures, contained provisions requiring CSPs to retain data used to help identify which Internet Protocol (IP) address belonged to a certain individual.[368] This received Royal Assent in February 2015.

However, there is still more that needs to be done legislatively. For example, there is still no legislation which requires the creation of communications data if the CSPs are not doing so for their own purposes; internet browsing, for example, is not always available retrospectively. This will need to be addressed in the future.

Further data challenges

Additional problems that shifts in technology have presented for law-enforcement agencies have been outlined in a recent speech by James B. Comey. He said that he faced two specific, overlapping, challenges: one concerned "real-time court-ordered interception of […] phone calls, e-mail, and live chat sessions"; the other, "court-ordered access to data stored on our devices, such

361. Private conversation.

362. 'Transposition of the European Data Retention Directive', *Internet Service Providers' Association*, 18 February 2009, available at: http://www.ispa.org.uk/transposition-of-the-europan-data-retention-directive/, last visited: 16 April 2015.

363. 'The Court of Justice declares the Data Retention Directive to be invalid', Court of Justice of the European Union (2014), available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, last visited: 18 March 2015.

364. Private conversation.

365. 'Data Retention and Investigatory Powers Act 2014 – Chapter 27', UK Government (2014), available at: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf, last visited: 30 April 2015, p. 6.

366. Ibid., p. 5.

367. Ibid., p. 2.

368. 'Counter-Terrorism and Security Bill', UK Government (2014), available at: http://www.publications.parliament.uk/pa/bills/cbill/2014-2015/0127/15127.pdf, p. 11.

as e-mail, text messages, photos, and videos."[369] The fact that this data was increasingly encrypted was only exacerbating these problems.

Previously, a target against whom the FBI was carrying out surveillance would have had a phone with a single carrier. Now, however, as Comey said, there are "countless providers, countless networks, and countless means of communicating";[370] these include mobile phones, tablets, and laptops, which use a variety of networks and contain numerous different apps. A suspect switching from using their mobile coverage to Wi-Fi – or from a voice service to a messaging app, or from one app to another – could mean that law enforcement loses coverage of their target's communications, giving all manner of national-security threats and criminals a potential edge.[371]

From a US perspective, while telecommunication and internet-service providers are required, by law, to install interception capabilities into their networks (under the Communications Assistance for Law Enforcement Act 1994 (CALEA)), new means of communication are not always covered and some companies do not comply with a court order because they do not have the interception capabilities required (even if they want to help, these capabilities take time – and money – to be constructed). Furthermore, some companies which provide some form of communications service are not necessarily covered by CALEA – an issue which the US government may look to address.[372]

4.1.2 RIPA's Codes of Practice should continue to be tweaked in the short-term; but any wholesale reform of the legislation must be considered carefully

There has been significant discussion about reform of RIPA, its modern-day applicability, and the concerns that it is being used incorrectly and disproportionately.[373] For example:

- In 2004, an Association of Chief Police Officers (ACPO) review of RIPA concluded that "the legislation had several ambiguities and deficiencies and had been implemented poorly";[374]
- Shadow Home Secretary Yvette Cooper has stated that a "full review of RIPA" is needed;[375]
- a Home Affairs Select Committee review into RIPA declared it "not fit for purpose";[376]
- Deputy Chief Constable Jon Boutcher has commented that RIPA "isn't fit for the way we now live our lives and the communications challenges that we have";[377] and
- a 2015 ISC report concluded that "serious reforms" to RIPA were required.[378]

One particularly common criticism is that levelled by Lord Macdonald, the former Director of Public Prosecutions, who has argued that, as social media did not exist when RIPA was enacted,

369. Comey, J., 'Going Dark', *Federal Bureau of Investigation*, 16 October 2014.

370. Ibid.

371. Ibid.

372. Ibid.

373. For example, see: Moore, M., 'RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework', *The Political Quarterly* 85.2 (2014), available at: http://www.academia.edu/7895161/RIP_RIPA_Snowden_Surveillance_and_the_Inadequacies_of_our_Existing_Legal_Framework, last visited: 18 March 2015.

374. 'Surveillance: Citizens and the State', House of Lords – Select Committee on the Constitution (2009), p. 37.

375. Cooper, Y., 'The challenges of a Digital World to our Security and Liberty', *Labour Press*, 3 March 2014, available at: http://press.labour.org.uk/post/78448368189/the-challenges-of-a-digital-world-to-our-security-and, last visited: 18 March 2015.

376. 'Regulation of Investigatory Powers Act 2000: Eighth Report of Session 2014–15', House of Commons – Home Affairs Committee (2014), available at: http://www.publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/711.pdf, last visited: 18 March 2015, p. 11.

377. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 101.

378. Ibid., p. 102.

by default, it must be incapable of dealing with modern communication-interception issues.[379]

Yet, RIPA is not about technology; it is about oversight and preventing intrusions into civil liberties. It was drafted to be technologically neutral (because, according to Sir David Omand, the Home Office "did not want to have to keep coming back to Parliament every time somebody developed a new app"),[380] something which has ensured its continued applicability. Even if RIPA legislation was to be redrafted, it would still need to be technologically neutral; referencing specific technology and communication methods would mean that the legislation not only becomes quickly outdated and invites constant revision, but could overly restrict the state's ability to gather certain types of intelligence.

Therefore, RIPA's age is not necessarily relevant. As Sir Malcolm Rifkind has said, "the fact it's a few years old is not automatically a problem: see the US constitution."[381] Home Secretary Theresa May has also said that she continues to regard RIPA as "good legislation that is still working well".[382]

Root-and-branch reform of RIPA is a high-risk strategy that would likely see demands for changes to sections of the legislation which are fundamental to the work of intelligence agencies and law-enforcement agencies, and could be contrary to the public interest. There is also the possibility that critics of RIPA and intelligence agencies' supposed intrusiveness would discover that reform of the legislation would end up strengthening the agencies' powers, rather than diminishing them; as one intelligence official commented, "this is one of the ironies of Snowden".[383] This is something that David Omand, former head of GCHQ, has also hinted at.[384]

Certain concerns about RIPA's modern day applicability can be resolved by focusing on its CoP. As Omand has said, these codes:

> could […] give Parliamentarians, the media, and the interested public a much clearer view of the purposes for which interception is authorised […] more could have been done over the last few years of rapid technological change to explain these matters to the public, and the Codes of Practice could provide an authoritative vehicle for filling this gap.[385]

Progress has been made on this front already. A revised communications data CoP came into force in March 2015, while a revised interception CoP has also gone out for public consultation, but has not yet been enacted.

4.1.3 Judicial oversight over every data application is neither the norm nor necessarily effective

The fact that, in the UK, warrants are issued by a Secretary of State, rather than a judge, is often used to criticise its interception authorisation regime. Human rights organisations have lamented the lack of formal judicial oversight for surveillance and have criticised the power that rests with

379. 'Social media mass surveillance is permitted by law, says top UK official', *The Guardian*, 17 June 2014.

380. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 101.

381. Telephone interview with Sir Malcolm Rifkind MP, August 2014.

382. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 102.

383. Private conversation.

384. Bartlett, J., *The Dark Net: Inside the Digital Underworld* (William Heinemann, 2014), p. 103.

385. Omand, D., 'Evidence for the Intelligence and Security Committee of Parliament', Intelligence and Security Committee of Parliament (2014), p. 6.

the Secretaries of State.[386] There are those who believe that an individual judge examining each warrant is required.

However, the extent to which judges and magistrates are better qualified to, for example, approve or reject warrants is highly contentious. In the latest Chief Surveillance Commissioner report, Sir Christopher Rose comments:

> What has become clear is that the knowledge and understanding of RIPA among magistrates and their staff varies widely. Adequate training of magistrates is a matter for others, but I highlight the need. The public is not well served if, through lack of experience or training, magistrates are not equipped effectively to exercise the oversight responsibility which the legislation requires. I am aware, for example, of one magistrate having granted an approval for activity retrospectively, and another having signed a formal notice despite it having been erroneously completed by the applicant with details of a different case altogether.[387]

Therefore, simply providing more judicial approval is not necessarily an unalloyed good without having well-trained, high-quality judges.

There is another reason why legal bodies are not necessarily best placed to make these decisions: politics. Applications for warrants may be legally sound – and, therefore, approvable – but, at the same time, politically unwise. As a recent ISC report pointed out:

> Ministers can […] apply an additional test in terms of the diplomatic and political context and the wider public interest. This additional test would be lost if responsibility were transferred to judges and might result in more warrant applications being authorised. Furthermore, judges are not held accountable, or asked to justify their decisions to Parliament and the public, as Minsters are.[388]

In the US, judicial oversight is carried out by federal judges appointed to the FISA Court. However, the two countries' systems cannot be easily compared, as there is not the same political connect between the elected civilian leadership and the security agencies. The NSA operates within the Secretary of Defense's broad remit, but is also answerable to the DNI – neither of whom are politicians/affiliated with the governing political party; GCHQ operates directly under a Foreign Secretary who is part of an elected political party (and who will be held to account for any warrants that they choose to sign).

Not even all members of the Supreme Court believe that judges are best placed to rule on issues such as domestic surveillance. In March 2014, Justice Antonin Scalia commented that "[t]he Supreme Court does not know diddly about the nature and the extent of the threat. It's truly stupid that my court is going to be the last word on it."[389] In a UK context, the ISC has agreed, saying that ministers are "well informed about the current nature of the threat and are therefore best placed to assess national security considerations."[390]

386. For example, see: 'Freedom from Suspicion: Surveillance Reform for a Digital Age', JUSTICE (2011), available at: http://2bquk8cdew6192tsu41lay8t.wpengine.netdna-cdn.com/wp-content/uploads/2015/01/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf, last visited: 18 March 2015, p. 42.

387. 'Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014', Office of Surveillance Commissioners (2014), available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/350857/Annual-Report-of-the-Chief-Surveillance-Commissioner-for-2013-2014-laid-4-September-2014.pdf, last visited: 18 March 2015, p. 6.

388. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 7.

389. 'The Kalb Report - Ruth Bader Ginsberg & Antonin Scalia', *The Kalb Report*, 36:18, 17 April 2014, available at: http://www.youtube.com/watch?v=z0utJAu_iG4&feature=share&t=36m18s, last visited: 16 March 2015.

390. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 75.

Ultimately, a non-judicial system in which there is accountability and a rigorous approval process is worth more than ill-trained magistrates or judges carrying out the task.

This situation is, by no means, unique to the UK; comparable democracies also have a lack of strong judicial approval. For example, the Australian Security Intelligence Organisation (ASIO) Act 1979 grants access to target computers if a government minister is "satisfied there are reasonable grounds" for ASIO to believe that the data on a certain computer will "substantially assist the collection of intelligence" in a security matter.[391] Similarly, the Telecommunications Act 1997 compels carriers to disclose "specified information or specified documents" if an ASIO officer is "satisfied that the disclosure would be in connection with the performance by [ASIO] of its functions".[392]

In Canada, the Communications Security Establishment (CSE) – "Canada's national cryptologic agency" –[393] can intercept foreign-intelligence communications without judicial approval, also only requiring ministerial approval.[394]

In Germany, intelligence agencies are permitted to carry out searches on electronic communications made online, without a prior court order – with permission being given by the Federal Ministry or Federal State Authority.[395]

In France, government bulk collection can take place in "defense of national interests" and without oversight.[396] Once this collection has identified a potential threat, authorisation for targeted interception is approved by the Prime Minister's office, which also gives permission for the government to obtain any "information or documents that are necessary for the implementation or use of the interceptions authorized by law."[397] There is no judicial oversight, but, instead, a three-man security commission which evaluates the warrant's necessity and reports back to the Prime Minister. In addition, CSPs are obliged to retain user-identification information, including e-mail addresses; passwords; payment details; geolocation data; and traffic logs. A December 2013 law also now allows metadata collection in real time, without a court order. Furthermore, interception is allowed in order to protect France's "economic and scientific potential", not just security concerns.[398]

4.2 PRIVACY AND LIBERTY

4.2.1 Neither GCHQ nor the NSA are carrying out mass – potentially illegal – surveillance on ordinary citizens

The allegation that mass surveillance is occurring is central to Edward Snowden's accusations, yet is untrue.

With regard to the NSA, there are procedural constraints in place, internally, to prevent rule-breaking, and no evidence suggests that such a culture exists. As has been previously noted, the fact that inspectors general and all branches of the US government have some form of review

391. Wolf, C., 'A Transnational Perspective on Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), p. 8.

392. Ibid., pp. 8-9.

393. 'About us', *Communications Security Establishment*, 23 April 2015, available at: https://www.cse-cst.gc.ca/en/about-apropos, last visited: 23 April 2015.

394. Bailey, J., 'Systematic government access to private-sector data in Canada', *International Data Privacy Law* 2.4 (2012), available at: http://idpl.oxfordjournals.org/content/2/4/207.full.pdf+html, last visited: 18 March 2015.

395. Wolf, C., 'A Transnational Perspective on Section 702 of the Foreign Intelligence Surveillance Act', Privacy and Civil Liberties Oversight Board (2014), pp. 11-12.

396. Ibid., p. 10.

397. Ibid., p. 11.

398. Ibid.

means that there would need to be a concerted; co-ordinated; government-wide conspiracy to be able to carry out any kind of sustained, illegal breach of citizens' privacy.[399]

There have also been attempts to argue that GCHQ's surveillance programmes are unethical, or even illegal. Representatives from the government and independent oversight mechanisms – even those critical of overextending the government's powers on communications data and surveillance, such as Deputy Prime Minister Nick Clegg –[400] have refuted such accusations:

- In July 2013, the ISC issued a statement saying that GCHQ conformed to its statutory duties and did not break the law in regard to its interception of communications.[401]
- In his 2013 report, Interception of Communications Commissioner Sir Anthony May said that "[u]nlawful and unwarranted intercept intrusion of any kind, let alone 'massive unwarranted surveillance', is not and, in my judgment could not be carried out institutionally within the interception agencies themselves."[402]
- In March 2014, Sir Mark Waller, the Intelligence Services Commissioner, commented that GCHQ "know perfectly well that they have to make out their case and the legality of their cases and so on and I have absolutely, clearly, accepted that [they do]".[403]
- In October 2014, then-GCHQ Director Sir Iain Lobban stated that, "of all the communications out there globally – the e-mails, the texts, the images – only a small percentage are within reach of our sensors. Of that, we only intercept a small percentage. Of that, we store a minuscule percentage for a limited period of time. Of that, only a small percentage is ever viewed or listened to, as permitted by our legal framework, and self-evidently, constrained by resource."[404]

It is also important to consider that the UK and the US do not have an historical culture of suppression. That does not mean that there can be complacency about such things in the future; but it is still significant. The state may never have had such an extensive technological capacity to be able to breach the civil liberties of its citizens as it does now; but that does not mean that it is doing so.

Furthermore, the NSA's and GCHQ's intelligence-gathering capacities – which are massive – should not be confused with their legal authorities, which are also strong (even in comparison to other Western democracies). We are generally happy for the state to have an army with sophisticated weaponry because there is faith in the system and that the checks and balances are sufficient. With this being the case, the questions for the future should not necessarily revolve around the capacity of intelligence agencies; instead, these debates should be about the people; the culture of the institution; and the systems in place to safeguard privacy.

Consider a non-democratic alternative: Russia, the country to which Snowden fled. Its surveillance system, the System of Operative-Investigative Measures (SORM), allows the FSB and seven other

399. Schmitt, G., 'Privacy or Security: a False Choice', *The Weekly Standard* 19.20 (2014), available at: http://www.weeklystandard.com/articles/privacy-or-security-false-choice_775317.html, last visited: 18 March 2015.

400. Clegg, N., 'Security and privacy in the internet age', *UK Government*, 4 March 2014.

401. 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', Intelligence and Security Committee of Parliament (2013), available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf.

402. May, A., '2013 Annual Report of the Interception of Communications Commissioner', Interception of Communications Commissioner's Office (2014), p. 59.

403. 'Oral Evidence Taken Before the Home Affairs Committee – Sir Mark Waller, Rt Hon David Davis MP and Nick Pickles, James Brokenshire MP – Questions 723 - 891', *House of Commons – Home Affairs Committee*, 18 March 2014, available at: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/140318.htm, last visited: 18 March 2015.

404. Lobban, I., 'Sir Iain Lobban's valedictory speech - as delivered', *Government Communications Headquarters*, 21 October 2014.

security agencies access to all telephone and mobile data and internet traffic (including social-media platforms). CSPs operating in the country are required to buy and install SORM probes that allow the state to monitor these communications.

According to the New York University Professor Mark Galeotti, "the FSB and other agencies can access metadata through SORM freely, so long as it is 'in pursuit of their operational duties' (which, of course, means anything they want)."[405] While they need a court warrant to access content, they are allowed to start monitoring as soon as they apply, and Galeotti has never heard of an application being refused. Presidential decrees can also give blanket access to data, in certain circumstances (as happened recently in Sochi, with the Winter Olympics).[406] Furthermore, Putin took advantage of Snowden's disclosures to launch further attempts at gaining a tighter control over the internet and telecommunications.[407]

4.2.2 The NSA's and GCHQ's intelligence-gathering methods are the international norm, not the exception

It was reported by a Norwegian newspaper, *Dagbladet*, in November 2013, that the NSA had logged information from 33.19 million Norwegian phone calls between 10 December 2012 and 8 January 2013.[408] However, the head of the Norwegian Intelligence Service was subsequently forced to admit that this collection had actually been carried out by Norwegian intelligence and then shared with the NSA in order to assist in military operations abroad.[409]

Similarly, Spain's *El Mundo* and France's *Le Monde* have accused the NSA of collecting 60.5 million and over 70 million phone records, respectively, between December 2012 and January 2013. Again, this was actually Spanish and French collection subsequently shared with the NSA in support of military operations.[410]

Another interesting example comes from Germany.

In the same month that Snowden's disclosures became known to the press, a German lorry driver was arrested, having carried out at least 762 shootings against other drivers on the autobahn over the previous five years.[411] To catch him, German authorities had used technology which allowed for the logging of the number plates of millions of vehicles.

As well as being generated by CSPs, metadata is also produced by the likes of Radio-frequency Identification (RFID) chips – such as those used in passports and turnstiles in car parks. It can be used to analyse how many of a certain type of vehicle may be on a certain road,[412] or be embedded in licence plates – in order to allow for real-time vehicle identification. These 'e-plates' have an embedded tag with a specific, encrypted identification number that can be detected by RFID readers. This number can be matched to a central database containing data about the vehicle

405. Email exchange with Mark Galeotti, 11 February 2015.

406. Ibid.

407. Soldatov, quoted in: 'How Snowden Empowered Russian Intelligence', *The XX Committee*, 20 January 2014, available at: http://20committee.com/2014/01/20/how-snowden-empowered-russian-intelligence/, last visited: 18 March 2015.

408. 'U.S. logged 33 mln phone calls in NATO ally Norway - report', *Reuters*, 19 November 2013, available at: http://www.reuters.com/article/2013/11/19/norway-usa-snowden-idUSL5N0J41LU20131119, last visited: 18 March 2015.

409. 'Norway denies U.S. spying, said it shared intelligence with U.S.', *Reuters*, 19 November 2013, available at: http://www.reuters.com/article/2013/11/19/us-norway-usa-snowden-idUSBRE9AI0D920131119, last visited: 18 March 2015.

410. 'Europeans Shared Spy Data With U.S.', *The Wall Street Journal*, 29 October 2013, available at: http://www.wsj.com/articles/SB10001424052702304200804579165653105860502, last visited: 18 March 2015.

411. 'German police catch up with the "autobahn sniper" that fired more than 700 shots at vehicles over five years', *The Independent*, 24 June 2013, available at: http://www.independent.co.uk/news/world/europe/german-police-catch-up-with-the-autobahn-sniper-that-fired-more-than-700-shots-at-vehicles-over-five-years-8671981.html, last visited: 18 March 2015.

412. Acker, A., 'Why the definition of "Metadata" matters to the NSA phone record collection', *HASTAC*, 11 June 2013.

(such as the registration number, make, model, insurance details, etc.).[413] The DoJ has also built a database capable of tracking US vehicle movements, which can scan and store license plates.[414]

German authorities subsequently reconstructed the journeys that the victims shot at had taken, and analysis of the bulk data eventually helped lead to the shooter. Clearly, Germany felt that the lives of its citizens were at threat and used the legal means at its disposal. Yet, it can hardly be said that this use of bulk data was especially less intrusive than that of the NSA or GCHQ; German and US perceptions of privacy clearly just differ.

4.2.3 Incidental collection of our everyday communications is a new reality

The tangling of data streams and external and internal communications means that there must be a public acceptance of the risk of incidental collection of our everyday communications during the NSA's and GCHQ's intelligence work. As General Alexander said:

> [I]f all the terrorists – the bad guys – would go to one sector of the network, call it badguys.com, then all we would have to do is monitor that area and everybody else's communications would flow freely. But the reality is, they use the same devices we do, the same networks and platforms we use, and, as a consequence, the communications are intermingled.[415]

Referring to the need for this collection to take place in bulk, Lobban has commented that "[y]ou can't pick and choose the components of a global interception system that you like (catching terrorists and paedophiles), and those you don't (incidental collection of data at scale): it's one integrated system."[416] He went on to say, "It would be very nice if terrorists or serious criminals used a particular method of communication and everybody else used something else. That is not the case."[417]

As a result, intelligence agencies on the lookout for foreign communications from terrorists inevitably end up capturing domestic communications from innocent citizens. Yet, as long as the correct oversight is in place to ensure that access to this data is not abused – and, so far, there is very little to suggest that it is being – this should not be the cause for huge concern that some have attempted to portray it as.

4.2.4 Private corporations also have access to large amounts of personal data

So much emphasis has been placed on the government's collection of data that the activities of private companies have been given insufficient attention. As President Obama has stated, it is not just the government which is trying to access data: "[c]orporations of all shapes and sizes track what you buy, store and analyze our data, and use it for commercial purposes; that's how those targeted ads pop up on your computer and your smartphone periodically."[418]

Jamie Bartlett, *Demos*'s Director of the Centre for the Analysis of Social Media, recently asked:

413. 'RFID-enabled license plates to identify UK vehicles', *Secure ID News*, 10 June 2004, available at: http://www.secureidnews.com/news-item/rfid-enabled-license-plates-to-identify-uk-vehicles/, last visited: 18 March 2015.

414. 'U.S. Spies on Millions of Drivers', *The Wall Street Journal*, 26 January 2015, available at: http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779, last visited: 31 March 2015.

415. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 09 May 2014.

416. Lobban, I., 'Sir Iain Lobban's valedictory speech - as delivered', *Government Communications Headquarters*, 21 October 2014.

417. 'Spying leaks "help terrorists and paedophiles," says GCHQ director', *London Evening Standard*, 7 November 2013.

418. 'Remarks by the President on Review of Signals Intelligence', *The White House – Office of the Press Secretary*, 17 January 2014. Sir Iain Lobban has also commented, "Who has the info on you? It's the commercial companies, not us, who know everything – a massive sharing of data. The other day I bought a watch for my wife. Soon there were lots of pop-up watches advertising themselves on our computer" ('GCHQ: "This is not Blitz Britain. We sure as hell can't lick terrorism on our own"', *The Telegraph*, 11 October 2014).

> [D]o you ever wonder why it is that we get all these amazing internet services – *Facebook*, *Twitter*, *YouTube*, *Gmail* – for free? […] it costs an awful lot of money to run these platforms: the server space, the highly skilled engineers, the legal teams. We are paying all right […] We pay with our data and our privacy.[419]

A US Senate Committee on Commerce, Science, and Transportation outlined, in a December 2013 report, how exactly companies use this sort of data:

> a wide range of companies known as "data brokers" collect and maintain data on hundreds of millions of consumers, which they analyze, package, and sell generally without consumer permission or input. […Consumers] have no means of knowing the extent and nature of information that data brokers collect about them and share with others for their own financial gain.[420]

> Data brokers sell this information for marketing purposes; credit-risk assessment; and fraud prevention, mining enormous levels of personal data from hundreds of millions of people. This can include addresses, phone numbers, medical conditions, what types of item they shop for online, even the type of car that consumers own.[421] Meanwhile, 'third-party cookies' are issued by advertising companies to follow consumer browsing habits when surfing the internet. This helps explain why you can search for a product on *Amazon*, for example, and then be inundated with adverts selling the same product when you visit another website.

Michael Hayden has offered two reasons as to why, despite these aggressive data-mining policies, corporations have not received the same level of scrutiny as the government:

> One is habit. We in the western world […] are accustomed to our privacy being threatened by government […T]hat instinct [of] "distrust the government, trust these guys" may not be an appropriate response to the modern world. The other thing is more concrete […] *Google*, *Yahoo* and *Microsoft* may squeeze my privacy; they're not going to put me in jail. The government can put you in jail. And so there's also a real concern that you really do want your government more limited than what the private sector may be able to do for profit.[422]

Despite this, concern about how data is being used has been reflected in public polling in the UK. A 2014 *Deloitte* Data Nation report showed that 24% of respondents did not trust any organisation with personal data, while an *Ipsos MORI* and *Royal Statistics Society* poll showed just 6% of respondents felt that companies had their best interests at heart when using data (compared to 11% for the government).[423]

4.2.5 What 'privacy' means is more contentious than ever[424]

These data issues tie in to our perceptions of privacy. As citizens are increasingly choosing to share vast amounts of their private details online, using various social-media platforms, the meaning of privacy is increasingly ambiguous.

419. Bartlett, J., *Orwell versus the Terrorists: Crypto-Wars and the Future of Surveillance* (Random House, 2015), p. 6.

420. 'A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes', United States Senate Committee on Commerce, Science, and Transportation (2013), available at: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577, last visited: 18 March 2015.

421. Ibid.

422. 'State Surveillance', *Munk Debates*, 2 May 2014, available at: https://www.munkdebates.com/debates/state-surveillance, last visited: 18 March 2015.

423. Cited in: Bartlett, J., *Orwell versus the Terrorists*, (2015), p. 9.

424. This is a subject tackled thoroughly by Bartlett, in: *Orwell versus the Terrorists* (2015).

Brad Smith, the Executive Vice President and General Counsel at *Microsoft*, has commented that, "consumers want to share their personal information, but […] they actually want to decide who they share that information with and they want to determine how this information will be used."[425] This may be accurate; it is also, ultimately, unrealistic.

Donald Kerr, one of the top intelligence officials within the George W. Bush administration, made perceptive comments on this front in November 2007, saying that "[t]oo often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture […] but in our interconnected and wireless world, anonymity – or the appearance of anonymity – is quickly becoming a thing of the past".[426] He posited a controversial understanding of what privacy today actually means: "a system of laws, rules, and customs with an infrastructure of inspectors general, oversight committees, and privacy boards on which our intelligence community commitment is based and measured […] it is that framework that we need to grow and nourish and adjust as our cultures change."[427]

If this shift in accepting that both state and non-state actors will inevitably have access to certain private details is not underway yet, then it must begin. Governments have access to all kind of information about citizens – including financial and medical data – and it is far from clear whether the public would be happy to hand over less data or have more transparency if it meant more terrorist attacks or a higher crime rate.

4.2.6 There could be another Snowden – and the impact may actually harm press freedom

There has been much discussion, and some attempts at reform, in order to "stop the next Edward Snowden".[428] At the NSA, 42 changes have been implemented:[429] for example, the introduction of a "two-person rule" – likely meaning that those copying data from a government network, onto portable storage media, must do so in the company of a second employee.[430]

Yet, over five million US-government employees have security clearances, with over 1.5 million having "Top Secret" clearance.[431] This helps to explain James Clapper's comment that "we will never ever be able to guarantee that there will not be an[other] Edward Snowden" – namely, "because this is a large enterprise composed of human beings with all their idiosyncrasies" –[432] and why Admiral Michael Rogers has said, "Am I ever going to sit here and say […] with 100 percent certainty no one can compromise our systems from the inside? […] Nope. Because I don't believe that in the long run."[433]

425. 'The Future of Global Technology, Privacy, and Regulation', The Brookings Institution (2014).

426. 'US intelligence official: You get privacy when your definition matches ours', *Ars Technica*, 11 November 2007, available at: http://arstechnica.com/tech-policy/2007/11/us-intelligence-official-you-get-privacy-when-your-definition-matches-ours/, last visited: 18 March 2015.

427. Ibid.

428. 'DOD's $5 Billion Push to Stop the Next Edward Snowden', *The Fiscal Times*, 05 December 2013, available at: http://www.thefiscaltimes.com/Articles/2013/12/05/DOD-s-5-Billion-Push-Stop-Next-Edward-Snowden; see also: 'Senators Look to Prevent Another Snowden', *Time*, 12 June 2013, available at: http://swampland.time.com/2013/06/12/senators-look-to-preventing-another-snowden/; see also: 'How to Prevent the Next Edward Snowden', *Foreign Affairs*, 17 June 2013, available at: http://www.foreignaffairs.com/articles/139516/sue-mi-terry/how-to-prevent-the-next-edward-snowden?nocache=1; see also: Byman, D. and Benjamin Wittes, 'Reforming the NSA: How to Spy after Snowden', *Foreign Affairs*, May/June 2014.

429. 'Interview transcript: former head of the NSA and commander of the US cyber command, General Keith Alexander', *The Australian Financial Review*, 9 May 2014.

430. 'NSA Implementing "Two-Person" Rule To Stop The Next Edward Snowden', *Forbes*, 18 June 2013, available at: http://www.forbes.com/sites/andygreenberg/2013/06/18/nsa-director-says-agency-implementing-two-person-rule-to-stop-the-next-edward-snowden/, last visited: 18 March 2015.

431. '5.1 million Americans have security clearances. That's more than the entire population of Norway.', *The Washington Post*, 24 March 2014, available at: http://www.washingtonpost.com/blogs/the-switch/wp/2014/03/24/5-1-million-americans-have-security-clearances-thats-more-than-the-entire-population-of-norway/, last visited: 18 March 2015.

432. 'Spy Chief James Clapper: We Can't Stop Another Snowden', *The Daily Beast*, 23 February 2014.

433. 'New N.S.A. Chief Calls Damage From Snowden Leaks Manageable', *The New York Times*, 29 June 2014.

With this being the case, governments must consider how they would respond next time around. Clearly, there needs to be a free press and there are occasions when whistle-blowing on state wrongdoing can be a public good; yet, the activities that Snowden exposed were not illegal and were, often, not even related to domestic surveillance. In fact, they arguably showed the depth of intelligence agencies' attempts to safeguard security and their advanced capacity to do so. However, this was not a universally accepted interpretation. To some extent (and it differs from country to county), Snowden has eroded public trust in the intelligence agencies' work. Another intelligence dump into the public domain would likely damage security and, potentially (albeit, unfairly), erode trust in our democratically elected governments even further.

In the UK, so far, there has been a reluctance to issue injunctions or Defence Advisory Notices (DA-Notices – the requests by the government, to editors, not to publish a story, out of concerns for national security); Prime Minister David Cameron stated that he preferred that the government appealed to "newspapers' sense of social responsibility."[434] However, he has also warned that, if media outlets "don't demonstrate some social responsibility it would be very difficult for government to stand back and not to act."[435]

If there were to be the threat of another Snowden-style leak, governments may take a significantly more aggressive approach in the future. The breakdown in trust between press and government that could follow would be an unhealthy one for a democratic society to suffer, and one that would only benefit those actors seeking to undermine the US; the UK; and its allies.

4.3 DIPLOMACY

4.3.1 Reining in spying on our allies may be counterproductive

Espionage regarding state-on-state relations is a relatively simple equation: nations spy on each other. The Snowden disclosures showed that the US was exceptionally good at spying on other nations – including its allies – and this was a cause of severe embarrassment to many.

To the extent that it has existed, the post-Snowden backlash from Europe has been led by Germany.[436] The country's vigour on this issue is partly because of recent memories of the East Germany security agency, the Stasi, although also due to domestic outrage at the fact that Angela Merkel herself was subject to surveillance from the NSA.

In response, the German government extended its surveillance and counter-espionage operations to all foreign-intelligence agencies operating on German soil, including those from Britain and America. This was the first time that this had occurred since 1945 – effectively subjecting both countries' intelligence operations to the same counter-espionage measures as China, Russia, and Iran. The German government also requested that the CIA station chief leave the country.[437] In October 2013, Merkel said that "spying on friends is not on at all";[438] by February 2014, she had even proposed the creation of a European communications network – "so that one shouldn't have

434. 'David Cameron makes veiled threat to media over NSA and GCHQ leaks', *The Guardian*, 28 October 2013, available at: http://www.theguardian.com/world/2013/oct/28/david-cameron-nsa-threat-newspapers-guardian-snowden, last visited: 18 March 2015.

435. Ibid.

436. 'EU court rejects requirement to keep data of telecom users', *Reuters*, 8 April 2014, available at: http://www.reuters.com/article/2014/04/08/us-eu-data-ruling-idUSBREA370F020140408; see also: 'Germany axes contract for US telecoms giant Verizon over Snowden and NSA spying', *The Drum*, 28 June 2014, available at: http://www.thedrum.com/news/2014/06/28/germany-axes-contract-us-telecoms-giant-verizon-over-snowden-and-nsa-spying. One US Congressional staffer I spoke to said that Germany and France were "at the forefront of being unhelpful".

437. 'Germany to "spy on US and UK intelligence gathering" for the first time in 45 years', *The Telegraph*, 24 July 2014, available at: http://www.telegraph.co.uk/news/worldnews/europe/germany/10988939/Germany-to-spy-on-US-and-UK-intelligence-gathering-for-the-first-time-in-45-years.html, last visited: 18 March 2015.

438. 'Angela Merkel: NSA spying on allies is not on', *The Guardian*, 24 October 2013, available at: http://www.theguardian.com/world/2013/oct/24/angela-merkel-nsa-spying-allies-not-on, last visited: 30 April 2015.

to send emails and other information across the Atlantic [to the US]".[439]

Part of this is for show. Germany has gained significantly from NSA intelligence in the past and continues to work with the agency;[440] this co-operation has been stepped up even further with the rise to power of the Islamic State.[441] This is also relevant to the UK; one German intelligence official has been quoted as saying that, when it comes to tracking returning fighters from Iraq and Syria, "[w]ithout the information from British signals intelligence we would be blind".[442] Furthermore, a parliamentary inquiry in Berlin concluded that Germany had actually been spying on other EU member states and sharing this intelligence with the US for over a decade.[443] There has clearly been a great deal of hypocrisy and feigned outrage from Germany following the Snowden disclosures.

However, Chris Inglis has acknowledged that not all of the NSA's work has "withstood […] the above the fold […] of the newspaper test", and that people might perceive certain aspects of it as causing "more damage than good".[444] This means that, in the future, there may be greater emphasis placed on whether certain types of intelligence gathering – on allies, for example – is worth carrying out if it were to be exposed.[445]

Yet, it is not just the US that has an aggressive spying strategy. In January 2014, President Obama said that "the intelligence services of other countries – including some who feign surprise over the Snowden disclosures – are constantly probing our government and private sector networks, and accelerating programs to listen to our conversations, and intercept our emails, and compromise our systems."[446] This includes not only adversaries such as China and Russia, but allies as well: consider the recent stories that emerged of Israel and the US spying on each other with regard to the latter's negotiations with Iran.[447]

4.3.2 NSA and GCHQ interest in state-run corporations is understandable, but will be returned in kind

There is a careful surveillance line to navigate when what is a state-run and what is a privately run corporation begins to blur.

An example of this is the NSA's monitoring of the Brazilian petrol giant, *Petrobras*, which is majority-owned by the state. When the story broke, there were accusations that the US was attempting to gain economic advantage for its own companies, and one commentator declared that "[t]he only ones scrutinizing Petrobras should be its investors, analysts at Wall Street's banks, credit rating agencies, and the people of Brazil who implicitly own the company", not a US spy agency.[448]

439. 'Data protection: Angela Merkel proposes Europe network', *BBC News*, 15 February 2014, available at: http://www.bbc.co.uk/news/world-europe-26210053, last visited: 18 March 2015.

440. For example: 'Operation Alberich: How the CIA Helped Germany Foil Terror Plot', *Der Spiegel*, 10 September 2007, available at: http://www.spiegel.de/international/germany/operation-alberich-how-the-cia-helped-germany-foil-terror-plot-a-504837-3.html; see also: 'Spying Together: Germany's Deep Cooperation with the NSA', *Der Spiegel*, 18 June 2014, available at: http://www.spiegel.de/international/germany/the-german-bnd-and-american-nsa-cooperate-more-closely-than-thought-a-975445.html, last visited: 18 March 2015.

441. 'Backlash in Berlin over NSA spying recedes as threat from Islamic State rises', *The Washington Post*, 29 December 2014, available at: http://www.washingtonpost.com/world/national-security/backlash-in-berlin-over-nsa-recedes-as-islamic-state-rises/2014/12/29/c738af28-8aad-11e4-a085-34e9b9f09a58_story.html, last visited: 31 March 2015.

442. 'Britain "threatens to stop sharing intelligence" with Germany', *The Telegraph*, 5 February 2015, available at: http://www.telegraph.co.uk/news/worldnews/europe/germany/11392943/Britain-threatens-to-stop-sharing-intelligence-with-Germany.html, last visited: 16 April 2015.

443. 'Coverup claims over revelation that Germany spied on EU partners for US', *The Guardian*, 30 April 2015, available at: http://www.theguardian.com/world/2015/apr/30/germany-spied-on-european-partners-on-behalf-of-us-for-years?CMP=share_btn_tw, last visited: 30 April 2015.

444. 'Transcript: NSA Deputy Director John Inglis', *NPR*, 10 January 2014.

445. Ibid.

446. 'Remarks by the President on Review of Signals Intelligence', *The White House – Office of the Press Secretary*, 17 January 2014.

447. 'Israel Spied on Iran Nuclear Talks With U.S.', *The Wall Street Journal*, 23 March 2015, available at: http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201, last visited: 25 March 2015.

448. For example, see: Fontevecchia, A., 'There Is No Reason Why The NSA Should Be Spying On Petrobras', *Forbes*, 10 September 2013, available at: http://www.forbes.com/sites/afontevecchia/2013/09/10/there-is-no-reason-why-the-nsa-should-be-spying-on-petrobras/, last visited: 18 March 2015.

Yet, as James Clapper has said, the US wants "early warning of international financial crises which could negatively impact the global economy", and "insight into other countries' economic policy or behavior which could affect global markets."[449] On that front, monitoring a seemingly corrupt, state-run company to which the US has loaned billions of dollars and whose performance has a significant impact on the stability of Brazil and, subsequently, all of South America was defensible.[450]

The logic behind this was proved when *Petrobras* became embroiled in the centre of a major corruption scandal towards the end of 2014. Brazilian authorities have alleged that *Petrobras* has funnelled money earned on inflated contracts into the coffers of domestic political parties, including the governing Workers' Party.[451] Dozens of Brazilian politicians have been accused of accepting large cash sums in payments, and huge protests have taken place demanding the impeachment of President Dilma Rousseff.[452]

It is likely that the NSA applies a broad remit as to the kind of state-owned companies which it monitors. With that being the case, there cannot be much surprise if other nations take an interest in the communications of Wall Street banks, for example; they likely already have done so.

4.4 A WAY FORWARD

4.4.1 Translucency, not transparency

States need secrets, for intelligence and military purposes; criminal investigations; and a host of other reasons. Yet, they also need public consent, in order to operate with credibility, and the intelligence agencies may have been overly secretive. As Michael Hayden has said, "the sum of individually defensible classification decisions is creating a lack of public confidence in the intelligence community's lawfulness";[453] something defensible in isolation is, perhaps, indefensible when taken in totality.

Hayden has also commented that the intelligence community "has got to show a lot more leg […] otherwise we won't get to do *any* of what we want to do, because the public support will be so withdrawn, that politically, no one is going to give us the authorisation."[454] Similar sentiments were voiced by Sir David Omand, in a paper that he co-authored with Jamie Bartlett and Carl Miller of *Demos*: "Democratic legitimacy demands that where new methods of intelligence gathering and use are to be introduced they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved".[455] Since Snowden's disclosures, James Clapper has stated that the US government should have made the Section 215 programme public.[456]

Yet, as Shane Harris, the journalist and author of *@War*, recently commented, such statements are

449. Clapper, J., 'Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage', *Office of the Director of National Intelligence*, 08 September 2013, available at: http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence, last visited: 18 March 2015.

450. Helman, C., 'Of Course The NSA Should Be Spying On Petrobras', *Forbes*, 10 September 2013, available at: http://www.forbes.com/sites/christopherhelman/2013/09/09/of-course-the-nsa-should-be-spying-on-petrobras/?partner=yahootix, last visited: 18 March 2015.

451. 'Petrobras scandal: Brazilian oil executives among 35 charged', *Associated Press*, 12 December 2014, available at: http://www.theguardian.com/world/2014/dec/12/petrobras-scandal-brazilian-oil-executives-among-35-charged, last visited: 19 March 2015.

452. 'Brazil protests demand impeachment of President Dilma Rousseff', *CNN*, 16 March 2015, available at: http://edition.cnn.com/2015/03/15/americas/brazil-protests/index.html, last visited: 24 April 2015.

453. Hayden, M., 'Beyond Snowden: An NSA Reality Check', *World Affairs*, January/February 2014, available at: http://www.worldaffairsjournal.org/article/beyond-snowden-nsa-reality-check, last visited: 18 March 2015.

454. 'Getting Counterterrorism Right: A Transatlantic Conversation', *The Henry Jackson Society*, 30 September 2013.

455. Bartlett, J., Miller, C., and David Omand, '#Intelligence', Demos (2012), available at: http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327, last visited: 18 March 2015.

456. 'Spy Chief: We Should've Told You We Track Your Calls', *The Daily Beast*, 17 February 2014, available at: http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html, last visited: 18 March 2015.

"very easy […] to say in hindsight".[457] There is little precedent for intelligence agencies seeking the opportunity to disclose large amounts of important information (and, arguably, correctly so). Harris severely doubted that if the next NSA Director or DNI was given the opportunity, "unprompted by a leak, [to disclose] some significant level of detail about a domestic intelligence-gathering programme, that he or she will actually do it".[458]

Finding the balance on knowing when and where intelligence agencies can open up is not easy. One UK official commented that the right time to talk about aspects of the intelligence agencies' work is "before things become contentious", and that the problem with the Snowden leaks was that the public's broad understanding of state capacity had not caught up with what that actual capacity was.[459] However, even those officials who are open to more transparency warn of an "irreducible core" of methods that cannot be revealed; could be quite broad; and will be defended, by them, to the hilt.[460]

There must always be a level of diffusiveness as to how intelligence is gathered, and the concept of 'translucency, not transparency' has been coined by Michael Leiter, the former head of the National Counterterrorism Center. As explained by Michael Hayden, with "[t]ranslucent, you can see through the thick glass. You get the broad outline of the shapes. You get the broad patterns of movements. But you don't get the fine print."[461]

This is a vital distinction. There must be broad public consent for the work being done by intelligence agencies; yet, clearly, the public cannot be given the operational details. Making this translucency approach a reality is a vital task for intelligence agencies in the future.

457. 'The Lawfare Podcast, Episode #110: Shane Harris and Benjamin Wittes with Serious Jokes on Surveillance', *Lawfare*, 10:00, 14 February 2015, available at: http://www.lawfareblog.com/2015/02/the-lawfare-podcast-episode-110-shane-harris-and-benjamin-wittes-with-serious-jokes-on-surveillance/, last visited: 18 March 2015.

458. Ibid., 10:14.

459. Private conversation.

460. Private conversation.

461. 'Former NSA Head Michael Hayden: The Agency "Cannot Survive Without Being More Transparent"', *Stanford Graduate School of Business*, 7 November 2014, available at: http://www.gsb.stanford.edu/insights/former-nsa-head-michael-hayden-agency-cannot-survive-without-being-more-transparent, last visited: 18 March 2015.

CONCLUSION

Snowden has kick-started a debate on surveillance that otherwise may not have happened. However, this is only a positive to the extent that, as Chris Inglis puts it, "somebody who burned my house down has given me the opportunity to perhaps build it in a way that I would prefer."[462]

Even if, for the sake of argument, we accept that *The Guardian* and *The Washington Post* have been responsible with what they have disclosed, Snowden stole huge amounts of data – including military and intelligence capabilities – and left it to their discretion as to what to publish. It was wildly reckless and irresponsible.

From certain sections of civil society, through to technology giants, the Snowden disclosures have shaken trust in intelligence agencies. This is an ill-deserved outcome after decades of vital work. Furthermore, the media has begun to use 'mass surveillance' and 'bulk collection' as synonyms;[463] it is entirely inaccurate to do so. Analysts at the NSA, GCHQ, and such agencies are looking to distil the relevant information and set aside the extraneous; they want to discard irrelevant data, not explore it.[464] With GCHQ, even when it can confirm that communications are relevant to a known target, it still does not have the capacity to read all of them; it is constantly prioritising on a case-by-case basis.[465]

Ultimately, Snowden only exposed that our agencies are essentially doing what we ask: they are not spying on the phone calls of ordinary citizens or brazenly looking at our e-mails; they are legally intercepting certain communications, in an attempt to advance the national interest. We may not like components of how it is done – sweeping up bulk data, for example – and we may be surprised at the methods used; but it is done for a good reason, and the state giving up these powers invites attack from terrorists; cyber criminals; or a host of other state and non-state actors.

However, the system is not perfect. Tweaks to legislation and oversight have already been made and will continue to be made. It is vital that this process persists. For intelligence agencies to be effective, there must be a broad public consensus about the types of work that they are understood to be carrying out; otherwise, politicians will be unwilling to give them the authorisation to carry out the kind of work that they currently are. Therefore, agencies may have to open up further than they have in the past. Equally, however, civil society has to accept that unalloyed transparency is not always a positive, and that there are good reasons for certain state secrets.

Such is the scale of security threats facing the West, building this consensus cannot wait any longer.

462. 'Transcript: NSA Deputy Director John Inglis', *NPR*, 10 January 2014.

463. For two examples from just one day, see: 'Mass surveillance regime is lawful, says secret UK tribunal', *The Financial Times*, 5 December 2014, available at: http://www.ft.com/cms/s/0/72dbfe5c-7c85-11e4-9a86-00144feabdc0.html#axzz3L2iK39cS; see also: 'UK mass surveillance laws do not breach human rights, tribunal rules', *The Guardian*, 5 December 2014, available at: http://www.theguardian.com/uk-news/2014/dec/05/uk-mass-surveillance-laws-human-rights-tribunal-gchq, last visited: 18 March 2015.

464. Private conversation.

465. 'Privacy and Security', Intelligence and Security Committee of Parliament (2015), p. 4.

In the spring of 2013, former National Security Agency contractor Edward Snowden stole a large quantity of classified government files. Via select journalists, Snowden revealed how intelligence agencies were tapping into fibre-optic cables containing telephony and internet-traffic data; intercepting and storing webcam images; and carrying out alleged 'warrantless' surveillance.

His actions have had a profound impact. There are calls for intelligence agencies to reform and be more transparent in order to rebuild trust. Yet the expectation that they stop terrorist attacks and serious crimes remains. Intelligence agencies are in a particularly unenviable position: asked to be less intrusive; more transparent; and yet, just as effective.

Surveillance After Snowden: Effective Espionage in an Age of Transparency studies the ways in which Snowden's actions have impacted the US and the UK (particularly in terms of national security) and what lessons may be learned for the future.

'If you believe in the cause of freedom, then proclaim it, live it and protect it, for humanity's future depends on it.'

Henry M 'Scoop' Jackson
(May 31, 1912 – September 1, 1983)
US Congressman and Senator for
Washington State from 1941 – 1983

THE HENRY JACKSON SOCIETY
DEMOCRACY · FREEDOM · HUMAN RIGHTS

First published in 2015 by
The Henry Jackson Society

The Henry Jackson Society

Millbank Tower, 21-24 Millbank,
London, SW1P 4QP

Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

ISBN 978-1-909035-18-8

£10.00 where sold