Chapter 6

6 The UK's surveillance laws

6.1 Introduction

The activities of GCHQ we described in the previous sections are mainly covered by the Regulation of Investigatory Powers Act 2000 (RIPA) and the Intelligence Services Act 1994. The Government also relies on other legislation such as: the Security Service Act 1989; Data Retention and Investigatory Powers Act (DRIPA) 2014; and the Counter-Terrorism Act 2008.[1] In February 2015, the Counter-Terrorism and Security Act 2015 was also approved by Parliament.

The legal framework governing secret activities is of critical importance in assessing the activities of GCHQ and our secret services. But the disclosures associated with Edward Snowden have revealed that: surveillance is not covered by adequate legislation; existing laws are outdated; and there are serious weaknesses in the processes designed to provide oversight and accountability. Some activities appear to be taking place at the margins of the law. It is not always obvious how the laws might be interpreted or applied, making it difficult to understand the powers the agencies have been granted by Parliament.

The law and courts are the bedrock of accountability for both the agencies and government more widely. The agencies interpretation of the law is also important for the day to day practice within the agencies and for legitimising activities which may not actually be permitted.

However, legal frameworks are not perfect. They may fail to anticipate all possibilities, especially in technological areas where technical developments make it hard for the legal framework to cope, for example, the exponential growth in the power of computing, sources and volumes of data and storage. The Internet, too, has capabilities for communication and espionage that reach much further than previous electronic "signals".

In this chapter, we ask whether mass surveillance is legal. We examine the adequacy of RIPA and we look at how this law deals with bulk collection, and how it defines external and internal communications and metadata. We examine the lack of a legal framework for machine processing of content. We also look at data retention, the use of data from US programs such as PRISM and whether there are safeguards for GCHQ's computer hacking activities.

Since the publication of the Snowden allegations, there have been a number of legal challenges. These have raised questions over the clarity of the law, proportionality, and the applicability of EU law to the UK's data retention laws. Finally, the authorisation framework for bulk collection and analysis is considered, along with the distinctions being made in the law between restrictions in collection and safeguards around analysis.

6.2 Recommendations to improve the UK's legal regime

Our key findings are

- Comprehensive reform is necessary. RIPA and DRIPA must be repealed and replaced by new comprehensive surveillance legislation that complies with human rights law.
- All surveillance decisions (including the interception of communications, access to communications data and receipt of intelligence from foreign agencies) must be subject to prior judicial authorisation and ongoing judicial control, instead of authorisation by the Secretary of State.
- Communications data should be afforded the same protection as the content of communications. The retention of metadata should also be targeted and specific.
- Statutory definitions should reflect modern circumstances – for example, the criteria used to define 'internal' and 'external' communications are no longer adequate.
- Effective and rigorous oversight mechanisms are needed to ensure that the intelligence services are not able to expand their powers in secret.

6.3 Are GCHQ's activities legal?

The Government refuses to acknowledge that mass surveillance programmes exist, while simultaneously claiming their activities are within the law.[2] There is very limited public oversight so it is difficult to assess whether practices comply with the law. Where the law is cited, there are loopholes that are being exploited.

Recently, the security services have been shown to have acted unlawfully. On 6 February 2015 the Investigatory Powers Tribunal (IPT) issued a second judgment in the case brought by Liberty, Privacy International and others.[3] It found that the secret intelligence sharing arrangements between the UK and the US were unlawful prior to December 2014, because the policies governing these arrangements were secret before their disclosure during the IPT proceedings.[4] On February 18 2015 the Government admitted the policies that oversaw the security agencies' capacity to spy on lawyer-client communications were also unlawful, as the result of another case[5].

Liberty, Privacy International and Amnesty International case has shed unprecedented light on the legalities of bulk data collection and mass surveillance.[6] The Government refused to officially confirm the existence of any programmes but confirmed suspicions[7] that authorisation for any systems, if they ever existed, would take place under Section 8(4) of RIPA, which allow the Secretary of State to sign general warrants for external communications (sent or received outside the British Islands). The arguments presented by the security agencies for why this is all lawful centre around two key points.

1. Firstly, they extend the definition of 'external communications' to include communications via web-based platforms that are not to another person, but to a wide audience. This means communications that are posts on Facebook walls, Google plus and Tweets (even if only one person can see them) are communications with the platform, not witj another person or people, and thus are considered to be a communication that ends outside the UK.[8] The Code of Practice for interception[9] makes clear that even if communications leave the country, as long as both ends are in the UK they do not fall under Section 8(4). But the security agencies have built a legal construct to bypass these provisions.

Admitting that not all Internet traffic would fall under this category, the Government argues that if any internal communications are captured, this would be allowed as long as it is collateral and necessary for the collection of external communications, under RIPA Section 5(6)(a). Furthermore, if any inappropriate information was ever seen by an operative, not an "active intrusion", they would not act on it and quickly forget it anyway. This means that in reality the intelligence agencies are collecting almost everything.

2. Secondly, the security services make a crucial distinction between bulk collection and the selection of a smaller selection for further "reading, looking at or listening to". It appears that the Government may wrongly believe it is only when this happens that the substantive interference with privacy arises. In this step, GCHQ needs further compliance with Section 16 of RIPA, which requires a basic case is made for why it is necessary to access the materials. Section 16 also sets out some provisions
"to limit the extent to which intercepted material can be selected by reference to "factors" that in essence would select communications to or from an individual who is known to be (at the time) in the British Islands".

These arguments are not satisfactory. For a start, it is not clear what level of computer processing is acceptable as long as no human "reads, looks at or listens to" the communications. Computers nowadays can do all these things (see the patented NSA's KODA software[10] for "text summarisation") and carry out other forms of processing and analytics that generate new forms of intrusive information, such as social maps of people who know each other.

The Government states in its open response[11] that intercepted material that does not fall under Section 16, cannot be read, looked at or listened to by anyone. (§ 131.3) It sets out in length what the law says about the controls over intercepted materials. But it does not explain any concrete policies to ensure compliance – we only have their word for it.

In addition, it is not clear whether these restrictions cover the hundreds of NSA officials working directly on the Tempora programme. It is possible that these officials process the raw intercepted materials under a different authorisation and oversight regime, not accessible to UK citizens. The Government's line is simply that "as a matter of principle, a power to share intelligence with a foreign intelligence agency must plainly be capable of being "necessary" for the purposes of Art. 8(2)" of the European Convention on Human Rights.

As we show below, the UK, US and other countries' intelligence agencies have entered into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority – making it almost impossible to assess whether or not they are legal.

6.4 The main regulation of surveillance: RIPA

The Regulations of Investigatory Powers Act 2000 (RIPA) was originally intended to bring UK surveillance in line with the Human Rights Act 1998 (HRA), but its poor drafting and opaque structure have enabled a massive expansion in the scope of surveillance powers in the last 15 years. Below, we look at some of the ways that RIPA is not fit for purpose.

It is worth noting that this law regulates a much broader set of activities than those described in this report in relation to GCHQ. For example, RIPA has ben used in the past by local authorities to spy on residents' dog fouling and school admissions.

6.4.1 Bulk collection

The bulk collection of Internet communications and phone calls under TEMPORA relies on the use of warrants for the interception of so-called 'external communications' (see next section) under section 8(4) RIPA. These also cover the bulk collection of communications data.

There is no requirement for a warrant made under section 8(4) to be restricted in any way to a particular person or premises. The government has admitted that a section 8(4) warrant could include the interception of all communications between the United Kingdom and a particular city abroad, or even a whole country or region. So although we are not the targets[12], these warrants are used to authorise the bulk collection and processing of our daily communications, including phone calls, texts, emails and web searches. We cannot see how such broad warrants can ever be compliant with human rights.

There is no official confirmation of the existence of the Tempora programme, but Government officials have defended the practice of bulk collection of data. The argument is that it is acceptable to collect and process vast amounts of data as long as only a minority is dealt with by human operatives. This is the "needle in the haystack" argument that has since been repeated many times.

The line was first used by an unnamed GCHQ source in declarations to the Guardian[13] at the time of the disclosures:

"Essentially, 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. If you had the impression we are reading millions of emails, we are not."

Sir Iain Lobban, head of GCHQ from 2008 until January 2014, used the metaphor of the "needle in the haystack" in his appearance in Parliament[14] in November 2013, stressing:

"We do not spend our time listening to the telephone calls or reading the e-mails of the majority, the vast majority that would not be proportionate. It would not be legal. We do not do it."

6.4.2 Internal vs external communications

The only real requirement of these 8(4) warrants is that they must target external communications, which either begin or end outside the UK.[15] The Code of Practice for interception[16] makes clear that even if communications leave the country, as long as both ends are in the UK they do not fall under Section 8(4).

However, the Government admitted in May 2014 that it understands the definition of 'external communications' to include communications via web-based platforms that are not to another person but to a wide audience. This means communications that are posts on Facebook walls, Google plus and Tweets (even if only one person can see them) are communications with the platform, not another person or people, and thus are considered to be a communication that ends outside the UK.[17]

The Government has also admitted that technically it cannot distinguish between 'internal' and 'external' communications, so it just captures everything.[18] Because of the way the Internet works, many internal messages may be routed via other countries.

In an age when communications between people in the UK routinely take place on US social media platforms any meaningful distinction between 'internal' and 'external' communications makes little sense. The UK must afford all individuals – no matter their nationality or location, regardless of who they communicate with or how – the basic protections required by the rule of law.

6.4.3 Lack of judicial authorization

Unlike some other countries, the UK places authorisations for surveillance as the responsibility of a Secretary of State and senior staff. There is some qualified provision for judicial authorisation respect of intrusive surveillance by police (but not the intelligence services), requests for encryption keys, and for local authorities seeking access to communications data. This arrangement allows the Executive to self-authorise the use of surveillance powers. It is unacceptable that there is no judicial check on the Executive's use of this invasive power. All intrusive, directed and targeted surveillance should be authorised by a serving judge.

English law has long recognised the need for a judicial warrant before a person’s home can be searched by the police. There is no longer any meaningful distinction between the quantity and nature of personal information that can be collected during a premises search and that collected via the targeted surveillance practices permitted under RIPA.

The European Court of Human Rights recognised the desirability of prior judicial authorisation for surveillance as long ago as 1978 in Klass v Germany, citing the benefits of independence and impartiality.[19] The UK's process of political authorisation is completely lacking in independence and impartiality.

6.4.4 Capturing everything

RIPA[20] makes a clear legal distinction between communications – the content of calls and emails – and communications data – the logs of who, when and where communicated, also known as metadata. But in new forms of digital communications, such as social media, they can be very hard to separate, as we explain below. .

The documents revealed by Snowden show that GCHQ collects everything. The law does not provide for any clear limitations on collection once a section 8(4) warrant is in place. Section 5(6)(a) of RIPA states:

"The conduct authorised by an interception warrant shall be taken to include (a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;(b) conduct for obtaining related communications data"

The complications brought by access to raw data streams in international cables are exemplified by the particularly problematic case of the recoding of images of Yahoo Webcams, in a programme called Optic Nerve.

Parliament should seek clarification from GCHQ on the exact legal basis of the Optic Nerve programme. If the response is that RIPA warrants are being used, Parliament should question whether the legislation is fit for purpose and fully complies with Human Rights legislation. Parliament needs to be informed of any other similar undisclosed programmes.

In addition GCHQ should clarify what measures, if any, it took to filter out any webcam users in British soil.

6.4.5 Safeguards, content and metadata

The arguments on safeguards produced by Government focus on the content, but it is not completely clear what happens to the metadata that is sieved and stored in bulk for longer periods. Metadata can be more intrusive than content in certain circumstances.[21]

The safeguards in section 16 of RIPA restrict the use of the contents of messages intercepted by GCHQ, but they place no restrictions whatsoever on the collection of communications data by GCHQ, regardless of whether or not the communication was internal or external and regardless of whether the person in question is known to be in the UK or not.

By relying on the broad scope of section 8(4) warrants to intercept millions upon millions of private communications, section 16 has enabled GCHQ to build up a vast database of the communications data of millions of UK residents which it can search at will without any clear legal authority or effective oversight.

Collecting and analysing content and communications data carry equivalent privacy risks in the digital age. There is a qualitative difference between the data available nowadays, and the data available in the pre-Internet days. Taken together, the availability, quality and

proliferation of new data sources make the distinction between communications data and content unclear in terms of intrusiveness.

Before the Internet, a record of a phone call told an investigator who called whom, when, and where. Even this 'traditional' communications data is intrusive and was deemed to require regulation. Researchers found that telephone metadata is "unambiguously sensitive, even in a small population and over a short time window".[22] They were able to infer medical conditions, firearm ownership, and more, using solely phone metadata.

But digital communications data is even more intrusive. Just looking at the websites we visit can reveal information about us. For example, if someone repeatedly contacts Narcotics Anonymous, or Gaydar, or a political website, it can go some way toward indicating significant aspects of their identity or interests. By combining email, telephone and web access data, and mobile phone location history, one can deduce a detailed picture of an individual's movements, habits and thoughts – certainly a far more detailed picture than a recorded conversation could offer.

Combined metadata allows for intrusion comparable to direct surveillance of an individual. This was illustrated by German MP Malte Spitz, who made six months of mobile phone records available to journalists. These combined with the data from social media and publicly available sources to provide an incredibly detail picture of Mr Spitz's activities.[23] The work of several human operatives to follow the movements and contacts of a target can be achieved just by looking at someone's digital footprints. Yet surveillance regulations considers the former a lot more intrusive.

The law however recognises the privacy risks in metadata. Article 29 Working Party of European Data Protection Commissioners argued that the now void Data Retention Directive (Directive 2006/24/EC) involved:

"an inherently high risk level that requires appropriate technical and organisational security measures. This is due to the circumstance that availability of traffic data allows disclosing preferences, opinions, and attitudes and may interfere accordingly with the users' private lives and impact significantly on the confidentiality of communications and fundamental rights such as freedom of expression."

The EU Privacy and Electronic Communications Directive, implemented in the UK as the Privacy and Electronic Communications Regulations,[24] sets strict restrictions on what communications companies can do with traffic and location data.

The former head of of GCHQ, Sir David Omand, has made the case[25] that the debate on metadata has been blown out of proportion. He argues that the legal definition in RIPA of "communications data" is a much smaller subset of the general metadata from Internet use and social media. According to Omand, most such metadata would probably be classified as "content" in the UK, and accordingly receive stronger legal protections.

The definition of communications data in RIPA – in section 21 – does not appear narrow at all. But it is not even clear that this is the definition that applies in the case of metadata from GCHQ's mass surveillance programs. Metadata caught in the dragnet of externally focused mass surveillance, could technically be defined as collateral to communications content and receive lower protections.

The blurring of the lines between metadata and content that David Omand refers to should be an important consideration though. The Home Office acknowledged in their evidence to the Intelligence and Security Committee (ISC): "the distinction between data and content, you can argue, is muddied in the Internet world".[26]

6.4.6 Targeting UK communications

The Government has claimed that section 16 of RIPA prevents the intelligence services from using section 8(4) warrants against UK citizens and residents. However, this is misleading.

Section 16(2) prevents GCHQ from searching the communications they intercept under section 8(4) in terms 'referable to a person known to be for the time being in the British Islands'. But it does not prevent GCHQ from searching the same communications by reference to other factors, which may easily include people currently in the UK. It also creates an unreasonably high standard by stating an individual must be "known to be" in the British Isles, rather than reasonably believed to be in the British Isles or a similar standard.

6.4.7 Machine processing of content

Defenders of the status quo, such as former Director of GCHQ, David Omand, argue that surveillance only takes places when humans are involved in accessing materials:

"Furthermore, the media fall into the category error that has crept into much of the recent public debate of not distinguishing bulk access by computers to the Internet – which the US and UK certainly do have – and so- called 'mass surveillance', which they do not conduct. Mass surveillance implies observers, human beings who are monitoring the population."[27]

In principle, the intelligence services are prohibited by section 16(1) of RIPA from examining intercepted communications by reference to a person known to be in the UK. But this section only refers to how "intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant".

Unfortunately RIPA is not clear on the safeguards prior to that human intervention, including for computer processing of the content of communications. As we saw in chapter three, the developments in machine learning since the time when RIPA was created make the lack of strong regulations on automated processing risky.

Elsewhere the argument has been made that bulk collection only starts when data is transferred to long term storage and analytics programmes, while the tapping of cables and initial selection of data – including temporary storage of a few hours – is simply access capability. This view was repeated in the US report on technical solutions to the problem of bulk collection, under Barack Obama's Presidential Policy Directive 28 (PPD 28).[28] We

fundamentally disagree with this perspective. It is impossible to separate the initial steps from the rest of the process. As we saw above the initial processing can include rules to favour types of data, but these are dynamic and cannot guarantee who is or is not included.

The Court of Justice of the European Union in their ruling on the unlawfulness of the EU Data Retention Directive was unequivocal in their consideration that collection of data in itself is intrusive.[29] How it is used will or will not add more layers of intrusion.

Any review must consider the detailed regulation of computer processing of all types of data or content directly obtained or intercepted. Regardless of any safeguards applied, it is crucial to remember that the interference with the right to privacy occurs when the communication is intercepted, whether or not someone looks at or reads it.

This is because intercepted data can be looked at retrospectively, there are risks of data leaks and also risks associated with future data sharing.

6.5 Access to data from providers: DRIPA

Access by the security services to communications data stored by service providers is not based on interception warrants, but on requests to the companies that hold the data: telephone services and Internet providers. These companies were forced by the EU Data Retention Directive 2006 to keep communications records for a period of time in order to make them available to security and intelligence agencies.

But this legislation was ruled incompatible with human rights and struck down in spring 2014 by the Court of Justice of the European Union (CJEU), thus removing the legal obligation on communication providers to retain the data.

Three months after this ruling, the Government rushed through "emergency" legislation in July 2014 to preserve the status quo of data retention, with only three days of debate in Parliament.

The new law, the Data Retention and Investigatory Powers Act (DRIPA), does not address blanket data retention and the lack of independent authorisation of access, which were two of the key criteria identified by the CJEU. DRIPA should also be repealed and replaced with legislation that complies with fundamental human rights.

6.6 Lack of regulation of international data sharing

It has been alleged that GCHQ circumvented UK law by accessing the content of communications obtained through the NSA's PRISM programme without proper authorisation. Having taken evidence from GCHQ, the ISC concluded that these allegations were unfounded, and that any request for intelligence from the US conformed with the requirements contained in the Intelligence Services Act 1994 and RIPA.[30] The ISC stated that "in each case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place"'.[31]

However, in October 2014 it was revealed that the UK intelligence services do not require a warrant to receive unlimited "unanalysed" intelligence from foreign agencies such as the NSA, where it would “not be technically feasible” for the UK to obtain it itself.[32] GCHQ was forced to reveal information about the secret internal “arrangements” during legal proceedings brought by Privacy International, Liberty and Amnesty International (see below for further details).

It also appears that the UK intelligence agencies can trawl through this intelligence and keep it for up to two years.[33] On 6 February 2015 the IPT ruled that the secret intelligence sharing arrangements between the UK and the US were unlawful prior to December 2014, because the policies governing these arrangements were secret before their disclosure during the IPT proceedings.[34]

This demonstrates that RIPA is inadequate to regulate intelligence agency co-operation and that the UK is able to access and analyse US gathered intelligence without complying with UK legal requirements. We may also infer that material gathered by UK agencies is likely provided to the US under similarly lax arrangements and may not be subject to sufficient protections under UK law or US law.

The UN Special Rapporteur on the protection of human rights while countering terrorism has noted that intelligence agencies have entered into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority.[35] The Five Eyes agreements are a very good example. He highlighted that information “may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards” and cited “credible evidence that some Governments have systematically routed data collection and analytical tasks through jurisdictions with weaker safeguards for privacy”. The Special Rapporteur stated that the such practices “make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the Covenant [International Covenant on Civil and Political Rights]”.[36]

Importantly, as raised by privacy activist Caspar Bowden, the US regime does give any proper rights to foreign citizens abroad, which means that GCHQ creates a fundamental lack of safeguards for British citizens in its dealings with the NSA.

6.7 The legality of mass hacking

As extensively documented in the previous sections, GCHQ is heavily involved in countless acts of what is normally considered hacking, interference with equipment, networks and other more aggressive forms of cyber attacks.

This is not covered by the legislation we describe above and it appears to be the one area where GCHQ – and the ministers overseeing it – may have more to answer from a legal standpoint. The US has tried to defend the practices[37] but the UK government has been conspicuously silent.

As we described in chapter four, the NSA has build the QUANTUM system for the hacking of computers through impersonation and interference. There are many references to GCHQ in relation to these hacking techniques, including their use in the Belgacom attack.

But Journalist Ryan Gallagher[38] has established from leaked files disclosed by Swedish broadcaster SVT[39] revealed that as recently as April 2013 GCHQ was reluctant to get involved in deploying the QUANTUM malware due to "legal/policy restrictions."

Similarly explicit concerns were raised by GCHQ staff at international meetings discussing hacking on mobile networks:[40]

"An additional concern in the UK is that performing an active attack, such as the Man-in-the-Middle attack proposed in the Lawful Interception solution...may be illegal. The UK Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material. A Man-in-the-Middle attack causes modification to computer data and will impact the reliability of the data."

Despite these concerns, the agencies have ploughed through with expanding these hacking operations.

The Home Office has published for consultation a Draft Code of Practice on Equipment Interference.[41] In our view the draft code seeks to make lawful what, up until now, has been a murky area, expanded out of control. The code appears to legitimise computer network exploitation (CNE) under sections 5 and 7 of the Intelligence Services Act 1994, which has not openly been used for this kind of activity until now.

One critical aspect of all these activities would be whether they target UK or foreign objectives. The latter may find legal cover in relation to Section 7 of the Intelligence Services Act, but attacking UK targets would in principle more restricted under Section 5.

The ISA 1994 follows a similar structure of internal and external activities as RIPA. But as we saw with RIPA these distinctions are becoming difficult to sustain. The hacking of equipment attached to the submarine cable network in the UK, e.g. in the NIGELLA project is one such case. We expect the agency will make the case that the targets are foreign communications. But the interference allows for UK communications to be ingested too.

The safeguards proposed in the draft code are too weak, with very few limitations on what the security services can do as long as they tick all the compliance boxes. Particularly troubling are the provisions for the targeting of innocent second parties, separately from unintended collateral damage. As we have sen this is common practice and a proper debate should take place on whether it is appropriate.

In the context of the agencies capabilities for industrial scale hacking, the new code would give the agencies access to anyone's devices .Highly significant proposals such as these

should be set out in primary legislation, not in a code of practice, as they deserve intense scrutiny.

As GCHQ themselves appear to acknowledge, many of these actions would have to contend with stringent provisions in UK law against computer crime.

Denial of Service attacks are considered to constitute a criminal offence within section 3 of the Computer Misuse Act 1990[42] (added by section 36 of the Police and Justice Act 2006). This covers "unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc." The offence includes intentionally or recklessly preventing or hindering access to any program or data held in any computer.

Some are calling for Denial of Service Attacks (DOS) to be legalised as a form of protest online. For example, some forms of DOS not involving hijacking third party computers that do not attempt to extort money from server owners could be more akin to a sit in or picket than to malicious sabotage. On the other hand, DOS can be highly damaging to computers not directly targeted as they can affect network quality. In any case if the agencies are to be legally empowered to use these techniques, there should be a public debate. We believe that either these attacks are illegal no matter who carries them out, or we should discuss openly any harms caused by these actions.

The use of intrusion technology and spyware is also believed to constitute an offence under section 3 of the Computer Misuse Act 1990 (as well as under section 1).[43] Mobile devices are thought to qualify as "computers". An offence is committed even where the effects of the action are only temporary and causing an action to be done is also an offence.

The hacking of Internet and communications services is also capable of constituting an offence under the same provisions of the Computer Misuse Act for the same reasons.[44] In the case of hacking the impairment additionally includes "undermining security features such as encryption and intrusion prevention" and impairing "the actual network infrastructure owned and operated by the Internet and communications service providers, and the services and programs run on the infrastructure".[45]

In the case of QUANTUM or other automated systems for directing attacks, Privacy International has argued that the infection of a computer device pursuant to an automated process would represent an offence by the person directing the process as there is an intrusion that impairs the target by draining battery life and using bandwidth and other computer resources. The section 10 exception (which applies to accessing a computer for inspection, search or seizure) does not apply to modifying material under section 3(1).[46]

Some of the more offensive hacking actions we described in chapter five may even cause enough violence to fall under the definition of the laws of war. In these cases, disproportionately and purposefully targeting civilians could be very problematic. The Government must clarify these aspects as a matter of urgency.

6.8 Legal challenges

Several legal actions have been brought against GCHQ and the security services:

Open Rights Group, English PEN, Big Brother Watch and Constanze Kurz have filed an application at the European Court of Human Rights (ECtHR). It challenges GCHQ's TEMPORA programme and the receipt and use of data from the NSA's PRISM programme.[47] We argue these activities and the legislative regime fail the "in accordance with the law" and proportionality requirements of Article 8 ECHR. The case has been given a priority designation by the Court, but is currently on hold pending the decision of the Investigatory Powers Tribunal in the below case.

Liberty, Amnesty International and Privacy International brought a case before the Investigatory Powers Tribunal in which the arguments raised are very similar to those in the ECtHR claim. They argued there is a breach of Articles 8 and 10 ECHR. The IPT issued a judgment on 5 December 2014,[48] in which it held that mass surveillance under section 8(4) RIPA is in accordance with the law, though it has not yet ruled on proportionality. The IPT also held that UK access to NSA intelligence material is now lawful, following the disclosure during the proceedings of secret policies on intelligence sharing. The IPT considers that the Intelligence Services Act 1994 gives the authority for GCHQ to enter into intelligence sharing arrangements, then RIPA s.15 s.16 provides the framework for ensuring information is only kept for the right reasons, deleted and searched.

On 6 February 2015 the IPT issued a second judgment.[49] It found that the secret intelligence sharing arrangements between the UK and the US were unlawful prior to December 2014, because the policies governing these arrangements were secret before their disclosure during the IPT proceedings.[50] The ruling is highly significant as it is the first time the IPT has found the UK's intelligence services to be in breach of human rights law.

Liberty is representing Tom Watson MP and David Davis MP in a judicial review of the lawfulness of the new Data Retention and Investigatory Powers Act 2014 (DRIPA). They argue section 1 DRIPA is incompatible with Article 8 European Convention on Human Rights and Articles 7 and 8 of the EU Charter of Fundamental Rights. Open Rights Group and Privacy International are third party interveners in the case and have argued the importance of the pre-existing EU legal regime governing data retention, in particular the E-Privacy Directive, and why DRIPA fails to comply with EU law.[51]

Privacy International (PI) is involved in several cases disputing surveillance practices. In addition to the case discussed above PI is challenging:

- Intrusion technology and spyware, in the IPT (PI contends that GCHQ, with the NSA, is using spyware and Trojans to infect mobile phone and laptops in order to unlawfully gain access to users' devices for the purposes of surveillance. They allege this is not proportionate under Articles 8 and 10 ECHR and fails the "in accordance with the law" test[52] as there is no legal basis for the conduct, which would be criminal if by an individual);

- Hacking of Internet and communications services, in the IPT (the case was filed by GreenNet and other companies and facilitated by PI. The complaint contends that GCHQ, with the NSA, is attacking and exploiting Internet and communications services, including core telecommunications infrastructure. They submit there is an unlawful act under the Computer Misuse Act and a contravention of Article 1 of the First Protocol to the European Convention on Human Rights, as well as Articles 8 and 10 ECHR); and

- The Five Eyes arrangement, in the ECtHR (PI filed FOI requests for the details of the agreement. GCHQ invoked a blanket exemption and the same exemption was invoked in respect of mundane information such as GCHQ's cafeteria menu. PI argues that the use of a blanket exemption has violated the right of Privacy International to freedom of expression guaranteed under Article 10 ECHR and there is no effective remedy in violation of Art 13.

- The Bureau of Investigative Journalism is also challenging the failure to protect journalists' sources and communications from government scrutiny and mass surveillance in the ECtHR.[53]

6.9 Conclusion

The current legal framework is plainly inadequate. The Snowden revelations have disclosed government programmes that are surprising in their breadth. The legislation has permitted extremely broad kinds of collection.

The authorisation mechanism has been a particular point of failure. Even if the legitimacy of bulk collection is accepted —which we do not—it is not acceptable for a Secretary of State to be able to extend the capabilities of GCHQ by issuing broad warrants.

The legislation and the practices conducted under it fail to comply with international human rights law. The framework governing the intelligence agencies' receipt of information from the NSA and other intelligence partners remain inadequate to meet the 'in accordance with the law' requirement of Article 8 ECHR. There must be a 'sufficient legal basis' and to meet the 'quality of law' test the law must be accessible and foreseeable. We know that GCHQ obtains unlimited "unanalysed" intelligence from foreign agencies without a warrant and relies on previously secret policies to provide the legal basis.

Section 8(4) RIPA has allowed the TEMPORA programme of mass interception of external communications under non-specific, blanket, rolling warrants. This fails to comply with the mandatory requirements of Article 8 ECHR. It does not meet the 'quality of law' test owing to insufficient statutory restrictions and safeguards and an absence of independent authorisation and effective oversight. Generic intercept based only on the means of transmission (by transatlantic fibre-optic cables) is also an inherently disproportionate interference. Again this means it fails to comply with Article 8 ECHR.

This chapter has also highlighted the government's expansive interpretations of the legislation, that insufficient safeguards are applied to collected data (in particular in respect of communications data) and the 'collateral' collection of internal communications. It has emphasised that the substantive interference with privacy arises on the collection of data, not only on its inspection. We have also identified the legal problems associated with Denial of Service attacks, intrusion technology and the hacking of Internet and communications services.

We have shown the lack of proper legal frameworks for other important activities of the agency. International data sharing with the NSA relies on secret agreements that do not appear to take into account human rights. As a first step the Five Eyes agreements must be made public.

The hacking activities of GCHQ come under a particular spotlight. The rushed Code of Practice on Equipment Interference should be scrapped and a proper legislative process that limits the agencies activities started instead. The government must clarify what may constitute cyberwar activities.

It is a truism to say that technology overtakes the law, which always lags behind. However, the onus should be on oversight bodies to remind Parliament when the law needs updating. Why these mechanisms have failed to alert Parliament to such significant changes in surveillance powers, is explored in the next chapter.

1 Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al, IPT/13/92/CH, The Respondents' Open Response, https://www.liberty-human-rights.org.uk/sites/default/files/The%20Intelligence%20Services%20open%20response%20to%20Liberty's%20and%20Privacy%20International's%20claims%2015th%20November%202013.pdf
2 http://www.bbc.co.uk/news/uk-politics-28006739
3 http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf
4 http://www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf
5 http://www.reprieve.org.uk/press/government-concedes-polices-on-lawyer-client-snooping-were-unlawful
6 https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/open_govt_response.pdf
7 http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world
8 See the statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, dated 16 May 2014, at para 137, https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf
9 http://www.statewatch.org/news/2014/apr/interception-comms-code-practice.pdf
10 http://www.nsa.gov/research/_files/tech_transfers/nsa_technology_transfer_program.pdf
11 https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/open_govt_response.pdf
12 See para 194.3 of the Government's Open Response to the claims brought by Liberty and Privacy International before the Investigatory Powers Tribunal in relation to Prism and Tempora.
13 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
14 http://www.bbc.co.uk/news/uk-politics-24848186
15 See section 20 RIPA.
16 http://www.statewatch.org/news/2014/apr/interception-comms-code-practice.pdf
17 See the statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, dated 16 May 2014, at para 137, https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf
18 Statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, 16 May 2014, at para 44-45.
19 The court stated: 'The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and proper procedure.'
20 http://www.legislation.gov.uk/ukpga/2000/23/contents
21 http://www.realprivacy.ca/content/uploads/2013/07/Metadata.pdf
22 http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/
23 http://www.zeit.de/datenschutz/malte-spitz-data-retention
24 http://ico.org.uk/for_organisations/privacy_and_electronic_communications
25 Loch K. Johnson, Richard J. Aldrich, Christopher Moran, David M. Barrett, Glenn Hastedt, Robert Jervis, Wolfgang Krieger, Rose McDermott, Sir David Omand, Mark Phythian & Wesley K. Wark (2014): An INS Special Forum: Implications of the Snowden Leaks, Intelligence and National Security, DOI: 10.1080/02684527.2014.946242
26 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf
27 Loch K. Johnson, Richard J. Aldrich, Christopher Moran, David M. Barrett, Glenn Hastedt, Robert Jervis, Wolfgang Krieger, Rose McDermott, Sir David Omand, Mark Phythian & Wesley K. Wark (2014): An

INS Special Forum: Implications of the Snowden Leaks, Intelligence and National Security, DOI: 10.1080/02684527.2014.946242

28 http://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options

29 https://www.openrightsgroup.org/assets/files/pdfs/reports/data_retention_briefing.pdf

30 UK Parliament, Intelligence and Security Committee Standard Note, SN/HA/2178, 29 October 2013

31 ISC Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme, https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130717_ISC_statement_GCHQ.pdf?attachauth=ANoY7co8Dk6ZPSV__fqGmcMCc8pStcFbFKI3ofH2373-hdgod80xU8C6nxN6w5BHzl1xOsg0-8I0ncj7CsJkDF29q_oRO_sYhjc9e-Tedc1ji2aPIdcYS2YHlFUoN-9PVsFyTej8hrf7Dxp6reaI6oaykgkc3M8DK6TP_M8N6nFibuY4tjVmdOFXM0Do7_RdduDqBQVs5ddG7yHdbGwUSvzsz7H0jjFImP4d4_ydwApRmgQZi8jGkhc%3D&attredirects=0

32 Privacy International, https://www.privacyinternational.org/?q=node/436

33 Privacy International, ibid

34 http://www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf

35 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc A/69/397, para 44 http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

36 ibid

37 https://firstlook.org/theintercept/2014/03/15/nsa-facebook-malware-turbine-non-denial-denial/

38 http://notes.rjgallagher.co.uk/2013/12/gchq-quantum-hacking-surveillance-legality-nsa-sweden.html

39 https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html

40 http://www.scribd.com/doc/100875514/3GPP-Estonia-2010

41 Draft Code of Practice: Equipment Interference, February 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf

42 http://www.legislation.gov.uk/ukpga/1990/18/section/3

43 https://www.privacyinternational.org/sites/privacyinternational.org/files/litigations/pi_hacking_case_grounds_0.pdf, paragraph 36

44 https://www.privacyinternational.org/sites/privacyinternational.org/files/litigations/final_grounds_-_gchq_attacking_providers.pdf, paragraph 49

45 ibid

46 https://www.privacyinternational.org/sites/privacyinternational.org/files/litigations/pi_hacking_case_grounds_0.pdf, paragraph 37

47 https://www.privacynotprism.org.uk/news/2013/10/03/legal-challenge-to-uk-Internet-surveillance/

48 http://www.bailii.org/cgi-bin/markup.cgi?doc=/uk/cases/UKIPTrib/2014/13_77-H.html&query=%22privacy+and+international%22&method=boolean

49 http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf

50 http://www.ipt-uk.com/docs/Liberty-Order6Feb15.pdf

51 https://www.openrightsgroup.org/ourwork/reports/submission-filed-by-org-and-privacy-international-in-dripa-case

52 https://www.privacyinternational.org/news/press-releases/privacy-international-challenges-gchqs-unlawful-hacking-of-computers-mobile

53 http://www.thebureauinvestigates.com/2014/09/14/bureau-files-echr-case-challenging-uk-government-over-surveillance-of-journalists-communications/