DON'T SPY ON US:
REFORMING SURVEILLANCE IN THE UK

September 2014

CONTENTS

INTRODUCTION

The Don't Spy On Us campaign is a coalition of organisations that defend privacy, freedom of expression and digital rights. The members of our executive committee are ARTICLE 19, Big Brother Watch, English PEN, Liberty, Open Rights Group and Privacy International.

This policy paper highlights the inadequacies of the existing law for protecting the population from intrusions into the right to privacy and infringements of the right to freedom of expression, following Edward Snowden's revelations last year regarding mass population surveillance. It identifies a number of necessary improvements and outlines some of the recent technological developments that have made reform necessary. The paper makes a series of recommendations that our campaign and its supporters would like MPs and peers to endorse and the next government to implement. This includes the repeal of the Regulation of Investigatory Powers Act (RIPA) and the Data Retention and Investigatory Powers Act (DRIPA) and the introduction of a new, comprehensive piece of legislation governing surveillance powers.

BACKGROUND

In summer 2013 it was revealed that GCHQ was routinely intercepting submarine fibre-optic cables containing the private communications of millions of British residents (the 'TEMPORA' programme). The reported scale of the interception is staggering: each day, GCHQ accesses some 21 petabytes of data – the equivalent of downloading the entire British Library 192 times.

This interception of fibre-optic cables carrying the daily traffic of the internet in and out of the UK has also enabled GCHQ to construct a vast database of 'communications data' (also known as 'metadata') from the communications of millions of ordinary people that it can search without restriction. This disclosure came mere weeks after the government's shelving of the Draft Communications Data Bill in April 2013, revealing that GCHQ had effectively already obtained in secret what Parliament was not prepared to sanction by law.

GCHQ's interception of the fibre-optic cable network is the digital equivalent of opening all the post going in and out of the UK on a daily basis. It is surveillance on an industrial scale; surveillance to rival that of the Great Firewall of China; surveillance that affects the privacy of almost every person in the UK who uses the internet. None of it has ever been authorised by a judge and it cannot be challenged in open court. Its existence was not revealed by any of the statutory oversight commissioners or Parliament's Intelligence and Security Committee, but by a foreign whistleblower.

It is, quite simply, the largest violation of the right to privacy in British history. And it is but one example of grossly disproportionate and unnecessary surveillance that RIPA has done nothing to stop.

The protection of privacy is a fundamental value of our legal system. As early as 1765, Lord Camden condemned as illegal the use of general warrants which allowed the Secretary of State 'to search, seize and carry away all the

papers of the subject'.[1] And in the wake of World War Two, lawyers from the Foreign and Commonwealth Office drafted Article 8 of the European Convention on Human Rights (ECHR) which guarantees that everyone has the right to respect for private and family life, including his or her home and correspondence.[2] The protection of privacy is also essential to the defence of other rights. In particular, the right of people to communicate in private is a key part of their right to speak freely. Failing to protect privacy means damaging the free flow of information and ideas which is the lifeblood of our democracy.

More generally, it is a fundamental principle of the rule of law in any democracy that people must know how the law is being applied, so that they can hold public officials to account for any mistakes as well as take an informed view as to whether the law needs changing. When public officials exercise intrusive powers in secret, it is all the more important that the law sets out clearly the circumstances and conditions in which those powers can lawfully be exercised. And it is especially important for the law to contain strict safeguards when public officials use secret powers to interfere with the fundamental right to privacy.

It is clear that this is no longer the case. RIPA has enabled our intelligence services to intercept the private communications of millions of people covertly by exploiting antiquated statutory definitions, changes in communications technology and without adequate oversight. The law is now being applied in secret, so that we, the public, can no longer know what is being done in our name. The so-called safeguards that RIPA contains have proved woefully inadequate for proper accountability and they have failed to ensure that surveillance powers have been exercised proportionately.

---

1 Entick v. Carrington, 19 State Trials 1030 (1765).

2 Article 8(1) ECHR states that 'everyone has the right to respect for his private and family life, his home and his correspondence'. The courts have since held 'correspondence' to include phone calls, emails and internet use: see e.g. *Copland v United Kingdom* (App no. 62617/00, 3 April 2007).

This problem has become starker in the wake of the judgment of the European Court of Justice (CJEU) in *Digital Rights Ireland* in April 2014, which held that the EU Data Retention Directive entailed 'an interference with the fundamental rights of practically the entire European population.[3] The Court struck down the directive and, as a result, undermined the validity of the implementing legislation in the UK. Despite the fact that the impact of the Court's judgment had been clear from the very outset, and that there was ample time in which to debate proportionate replacement legislation, all three parties instead chose to rush DRIPA through Parliament using emergency procedures in a matter of days some three months after the judgment had been handed down. Not only has DRIPA simply re-enacted the provisions of the Data Retention Directive, which the CJEU already found to breach EU law,[4] but it has also extended the scope of RIPA to cover internet services outside the UK.[5] DRIPA is plainly contrary to existing rights under the European Charter of Fundamental Rights and the ECHR and it was pushed through without sufficient time to enable the public to discuss and debate its proposals.

The Don't Spy On US campaign does not dispute that surveillance is sometimes necessary in order to protect national security and safeguard the lives of British citizens and residents. But it is deeply undemocratic to suggest that any surveillance measures are acceptable, no matter how intrusive or disproportionate. National security should not be a blank cheque. The law demands that measures taken to protect national security must be necessary and proportionate otherwise they risk undermining public trust in our intelligence agencies. It is equally important that laws

3 Cases C-293/12 and C-594/12, *Digital Rights Ireland v Minister for Communications and others* (8 April 2014), para 56.

4 Statement of the Article 29 Working Part, 1 August 2014 (14/EN, WP 220), in which the EU working group warned that 'national data retention laws and practices should ensure that there is no bulk retention of all kinds of data'.

5 Don't Spy On Us briefing on the fast-track Data Retention and Investigatory Powers Bill (July 2014), https://www.dontspyonus.org.uk/blog/2014/07/21/briefing-on-the-fast-track-data-retention-and-investigatory-powers-bill/

on surveillance are made after proper consideration and debate, having due regard for fundamental human rights, rather than rushing legislation through Parliament without effective scrutiny at breakneck speed.

It has become clear that our surveillance laws are damaging our privacy, our freedom of speech and our very democracy. It is time for significant and urgent change to re-establish the basic tenets of the rule of law, namely transparency, accountability and protection for the fundamental rights of every person.

RECOMMENDATIONS

1. Comprehensive reform is necessary. RIPA and DRIPA must be repealed and replaced by new comprehensive surveillance legislation.

2. All surveillance decisions (including the interception of communications and access to communications data) must be subject to prior judicial authorisation.

3. The interception of communications must always be targeted and specific rather than mass and indiscriminate.

4. Communications data should be afforded the same protection as the content of communications. The retention of metadata should also be targeted and specific.

5. Surveillance should only be carried out for purposes that are more precisely and narrowly defined than at present.

6. The government should cease breaking encryption standards and undermining internet security. Such activity should be explicitly prohibited by legislation.

7. International arrangements governing the collection and sharing of the results of surveillance must be made public, subject to parliamentary and judicial oversight and should allow individuals to foresee when they are likely to be subject to surveillance. This requirement should be set out in legislation.

8. The government should publish aggregate information on the number of surveillance authorisation requests approved and rejected in order to increase transparency.

9. Adequate remedies should be available for the unlawful access to communications data and the unauthorised use of other surveillance techniques.

10. The Investigatory Powers Tribunal should adopt a more open and fair procedure. This should include: hearings; public hearings, unless the government demonstrates that secrecy is required in the particular case; evidence should be disclosed and judgments and reasons published unless the government demonstrates that secrecy is necessary; special advocates should be appointed; decisions should be subject to appeal.

11. The Intelligence and Security Committee should be reformed so that it is: answerable directly to Parliament; empowered to take decisions on reporting and publication; and appropriately funded and staffed. It should have strengthened powers to compel the production of information and witnesses. The chair should be a member of the largest opposition party and the Commons members should be elected not appointed by the Whips.

12. The Intelligence Services Commissioner and the Interception of Communications Commissioner should be properly resourced, report to Parliament and review a far larger number of requests for data.

13. Intercept evidence should be admissible in criminal court proceedings.

OUR DEMANDS

A NEW SURVEILLANCE LAW

We need a new piece of legislation governing surveillance in the UK to replace RIPA. A new law would also address relevant provisions under the Telecommunications Act 1984,[6] the Security Service Act 1989, the Intelligence Services Act 1994 and the Data Protection Act 1998 (DPA).

Although RIPA was originally intended to bring UK law in line with the requirements of the ECHR as incorporated by the Human Rights Act 1998 (HRA), it is clear that its poor drafting and opaque structure have not prevented a massive expansion in the scope of surveillance powers in the last 15 years. It was also drafted before the rapid advances in communications technology, including the rise of social media.

The law in this area simply has not kept pace with the scale of technological change. The protections that Parliament intended to enshrine in RIPA no longer offer adequate oversight of the technical capabilities of Britain's security services. As a result, gaps and weaknesses in the framework have been exploited to enable the collection of our private communications on a previously unimaginable scale. The intelligence agencies, left virtually unconstrained and unsupervised by outdated legislative frameworks, have unilaterally expanded the scope of their activities and the extent of their capabilities.

We need a major overhaul of our surveillance laws. They are no longer fit for the age in which we live. Fresh legislation must be put in place to ensure that surveillance conducted by law enforcement and intelligence agencies is only carried out where it is strictly necessary and proportionate. It must contain statutory definitions that reflect modern circumstances, not the now antiquated framework. It must contain effective and rigorous oversight

6 See e.g. section 94 governing the power of the Secretary of State to make directions in the interests of national security

mechanisms to ensure that the intelligence services are not able to expand their powers in secret. Most of all, the law must be changed in order to ensure that our fundamental rights and the rule of law are protected, rather than undermined.

The Don't Spy On Us campaign calls for the law to be reformed in line with six democratic principles.

1. NO SURVEILLANCE WITHOUT SUSPICION

An end to mass interception of communications

The Snowden revelations regarding the scope of GCHQ surveillance under TEMPORA have highlighted the use of warrants for the interception of so-called 'external communications' under section 8(4) RIPA. It is now clear that section 8(4) warrants have been used as the basis for the mass interception by GCHQ of millions of private communications as well as its bulk collection of communications data. It is also clear that the relevant legislation governing the intelligence services (e.g. the Security Service Act 1989 and the Intelligence Services Act 1994) do not contain any safeguards to prevent GCHQ obtaining the private communications of millions of UK residents from overseas partners such as the NSA.

There is no requirement for a warrant made under section 8(4) to be restricted in any way, unlike warrants under section 8(1) RIPA which must be targeted at either a particular person or a specific premises. Indeed, the government has since admitted that a section 8(4) warrant could include the interception of all communications between the United Kingdom and another city or country,[7] for example all the emails, texts, phone calls, and internet communications between the UK and the United States.

7 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, para 194.3

The sole limiting factor for section 8(4) warrants is that they are directed at 'external communications', i.e. communications which either begin or end outside the UK.[8] In addition, the intelligence services are prohibited by section 16(1) from examining intercepted communications by reference to a person known to be in the UK.

However, it is now clear that the restrictions in section 8(4) offer no meaningful safeguard against the indiscriminate bulk interception of communications by GCHQ. For the very first time since RIPA was enacted, the government admitted in May 2014 that it understood the definition of 'external communications' to include any communications involving social media (e.g. a post on a friend's Facebook page) so long as the relevant server was outside the UK.[9] This leads to possible instances of surveillance that are not only arbitrary but absurd. For instance, if two friends in Birmingham were to use their mobile phones to call one another to arrange an evening out, that would count as an internal communication and therefore section 8(4) could not be used. If, however, the same two friends were to use their mobile phones to send Facebook posts to one another, that would count as an 'external communication' for the purposes of section 8(4) because Facebook's servers are outside the UK.

In addition, the government has admitted that large numbers of 'internal' communications can also be swept up when intercepting so-called 'external' communications, because of alleged technical difficulties in intercepting communication network connections.[10] This is because the nature of internet-based communications means that it is generally impossible to determine – at the point of interception – whether a particular message is 'internal' or 'external' because many internal messages may be routed via other countries. In other words, millions of private messages between

8 RIPA, Section 20

9 Statement of Charles Farr, the Director General of the Office for Security and Counter-Terrorism, dated 16 May 2014, para 137

10 Statement of Charles Farr, ibid, para 44-45

individuals in the UK are routinely intercepted by GCHQ under section 8(4) warrants because it is impossible to tell whether the messages are internal or external.

These problems with the arbitrary definition of 'external communications' under RIPA are compounded by the lack of effective safeguards for bulk collection under section 8(4). The government has claimed that section 16 prevents the intelligence services from using section 8(4) warrants against UK citizens and residents. However, this is misleading. Section 16(2) only prevents GCHQ from searching the communications they intercept under section 8(4) where the communications are 'referable to a person known to be for the time being in the British Islands'. It does not prevent GCHQ from searching the same communications by reference to other factors which may easily include people currently in the UK. For example, GCHQ could not use 'David Cameron' as a search term if it knew David Cameron was currently in the UK. But it could easily search for other terms in which David Cameron was likely to appear in the search results, e.g. the name of his political party or the school where he was educated.

More importantly, section 16 places 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. Section 16 only restricts the use of the contents of messages intercepted by GCHQ. It places no restrictions on communications data. By relying on the broad scope of section 8(4) warrants to intercept 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.

A third major weakness in the current framework governing interception of communications is the lack of any corresponding restriction on the intelligence services obtaining intercepted material from other countries, even where the communications in question belong to people within the UK. Despite the extremely close cooperation between GCHQ and the NSA, for

example, it is striking that there are no statutory restrictions to prevent the NSA from supplying GCHQ with access to all the private communications it has obtained from its own extensive surveillance programmes on non-US nationals.

We believe that the current distinction between 'internal' and 'external' communications under RIPA is both arbitrary and – in light of current technology – wholly antiquated. 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 is not only discriminatory but nonsensical. 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.

Nor can the mass surveillance of private communications and the bulk collection of communications data without the requirement of reasonable suspicion be justified. If the requirements of targeting a specific person or premises are thought to be necessary safeguards for the purposes of a warrant under section 8(1), there is no justification for abandoning those safeguards in respect of so-called 'external' communications. Indeed, it is impossible to see how such indiscriminate surveillance could ever meet the requirement of proportionality, which is a fundamental part of the protection of the right to privacy.

We therefore recommend that a new legislative framework should:

1. Expunge the internal/external distinction from the threshold criteria for the institution of communications surveillance measures. Save in exceptional circumstances that are both clearly and narrowly defined, all interception warrants should be targeted at a specific individual or premises. In any event, interception warrants should never be so broad as to allow for indiscriminate surveillance.

2. Raise the threshold applied to the interception of communications. Interception should only occur after it is established, on case by case basis, that:

   i. the surveillance is necessary for a legitimate aim, and is proportionate to that aim;

   ii. other less intrusive investigative techniques have been exhausted;

   iii. information accessed will be confined to that reasonably relevant to the investigation, with excess information promptly destroyed or returned; and

   iv. information is only accessible by the specified authority and used for the authorised purpose.

3. The procedural safeguards applied to intercepted material should not differ based on an individual's nationality, residence, location or choice of communications service provider.

Intercepted material provided to the UK by foreign intelligence agencies should be subject to the same protections and safeguards as material intercepted by the UK. The UK should seek and receive assurances that British standards will be complied with when providing intercepted material to foreign partners.

Ending the distinction between the content of communications and communications data

As noted above, the law has traditionally treated access to communications data as a less serious interference with the right to privacy than the interception of the content of private communications. Hence the interception of communications under Part 1 of RIPA requires a warrant from the Secretary of State whereas access to communications data under

Part 2 requires only authorisation by a senior member of the public body involved.

In this sense, our surveillance laws are a hangover from the 1970s when the only way to record communications data from telephone calls was for the Post Office to attach a meter to an individual's phone line. When RIPA was debated only 25 per cent of the population was online, now 80 per cent of British residents are online with the average household owning more than three types of internet enabled devices and one in five owning six or more.[11]

Our devices routinely track our location along with the details of the websites we visit and the people with whom we email, text or chat. Our phones no longer store just our phone numbers but also personal information about our family members, our financial status, our medical history, our political affiliation and religious beliefs. By analysing communications data alone, analysts can build up complex pictures of individual lives: where people go, whom they meet, what kinds of services they use and the types of websites they visit without reading a single email or listening to a single phone call.

In June 2014, the US Supreme Court acknowledged this radical change when Chief Justice Roberts noted that 'today many of the more than 90 per cent of American adults who own cell phones keep on their person a digital record of nearly every aspect of their digital lives'.[12] Another US court, ruling on the NSA's bulk communications data programme, concluded that it could not 'imagine a more "indiscriminate" and "arbitrary" invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for the purposes of querying and analyzing it without prior judicial approval.[13] In recent months, ex-NSA General Counsel

---

11 Ofcom, The Communications Market 2013: Internet, http://stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cmr13/internet-web/

12 *Riley vs California*, 573 US (2014) at 19

13 *Klayman vs. Obama*, Civil action no. 13-0851(RJL), United States District Court for the District of Columbia

Stewart Baker has said 'metadata [communications data] absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.'[14] General Michael Hayden, former director of the NSA and the CIA, called Baker's comment 'absolutely correct,' and offered a different perspective on the value that the NSA places on metadata, asserting, 'We kill people based on metadata'.[15]

For these reasons, it has become clear that the existing distinction drawn between content and communications data is untenable. We therefore recommend that the collection of and access to communications data should only be available on the same terms as the interception of communications as outlined above.

Ending the mass retention of communications data

Our surveillance laws must be overhauled to end mass data retention. The CJEU reached this conclusion in April 2014, when it found that the EU Data Retention Directive, which provided for EU States to mandate the retention of communications data on their entire populations for 6-24 months, violated the rights to privacy and data protection under the EU Charter of Fundamental Rights. The CJEU described the regime as a 'wide-ranging and particularly serious interference with those fundamental rights... without... being... limited to what is strictly necessary.'[16] In particular, the blanket retention of communications data was found to be disproportionate,[17] as was the lack of an independent judicial or administrative judicial body to make decisions regarding access to the data.[18]

---

14 David Cole, 'We Kill People Based on Metadata', New York Review of Books (10 May 2014)

15 Ibid

16 Judgment in Digital Rights Ireland case (joined cases C-293/12 and C-594/12) available at http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf, paragraph 65

17 Digital Rights Ireland, para 59

18 Digital Rights Ireland, para 62

The UK government's response was to rush through new 'emergency' legislation in July 2014, just before the summer recess, with only three days of debate in Parliament, motivated by a concern that the judgment would nullify the secondary legislation implementing the directive. The new legislation – DRIPA – does nothing to address the fundamental problems of blanket data retention and the lack of independent authorisation of access. Instead, section 1 of DRIPA puts blanket data retention on a statutory footing, with only minor changes from the previous legislation. It therefore appears to breach our right to privacy on the same grounds as the previous regime. The legislation is now the subject of judicial review proceedings brought by David Davis MP and Tom Watson MP, who argue that it breaches the ECHR as incorporated by the Human Rights Act and the EU Charter of Fundamental Rights.

Retention must be targeted, justified and subject to judicial authorisation. For example, retention of a person's data would be justified where the person is under suspicion or there is reason to believe it would assist the investigation of serious crime. Retention in a particular geographical area or time period may also be justified.[19] DRIPA must be replaced with legislation that prohibits blanket retention and takes account of the other findings of the CJEU.

In addition, the judgment stated there should be exceptions for communications that are subject to an obligation of 'professional secrecy'.[20] Retention periods should be limited to what is strictly necessary and tailored to different data types and circumstances.[21] The government has introduced regulations[22] that provide for 12 months as a maximum retention period, but these still allow all communications data to be retained for the

19 Digital Rights Ireland, para 59

20 Digital Rights Ireland, para 58

21 Digital Rights Ireland, para 63-64

22 The Data Retention Regulation 2014

maximum period without any tailoring. As discussed above, access to the data should be independently and judicially authorised and limited to fewer organisations and circumstances.[23] Safeguards should be applied to the stored data.[24]

2. TRANSPARENT LAWS, NOT SECRET LAWS

Transparency

In a democracy, citizens must be sufficiently informed about the scope and nature of surveillance operations to be able to hold government to account. Increased transparency regarding the scale and reach of surveillance is necessary. The government must begin to publish aggregate information on the number of surveillance authorisation requests approved and rejected so that citizens can understand the scale of surveillance requests made by the intelligence agencies and by government agencies. Among other criteria, this data should contain a disaggregation of the requests by the service provider, including the investigation type and purpose.

Without this information, it is difficult to have an informed debate about the appropriate limits of surveillance. Debate on this issue over the past few years has been based on a misleading picture of present capabilities. For example, the Home Office's arguments regarding the need for the Draft Communications Data Bill were premised on the claim that its interception capabilities were declining when in fact it appears that the intelligence agencies were drastically expanding their capabilities.

In August 2013, US President Barack Obama outlined his plans to increase transparency and oversight over the US intelligence agencies. A number

23 Digital Rights Ireland, paras 60-62

24 Digital Rights Ireland, paras 66-68

of US Senators independently have proposed legislation to this end. In November 2013, the UN General Assembly passed a resolution tabled by Brazil and Germany demanding that States:

> establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and collection of personal data;[25]

The UK supported this motion. This position is shared by Sir David Omand, the former Director of GCHQ, who recently commented:

> I hope ways will be found to make more information available for the UK so as to enhance public trust in the intelligence work of the police and security authorities.[26]

The UK government must legislate for greater transparency in order to rebuild public confidence.

The purposes of surveillance

It is for Parliament, rather than the executive, to decide the circumstances and conditions under which law enforcement and the intelligence services may have recourse to surveillance powers. New legislation therefore should set out, with much greater clarity than is currently the case, the types of situations in which we may be subject to surveillance.

We note, for instance, that nowhere in RIPA is there any requirement that an investigating body should have reasonable suspicion that a person is

25 United Nations General Assembly, Sixty-eighth sessions, Third Committee, Agenda item 69(b)

26 Sir David Omand, 'Enhancing surveillance transparency: A UK policy framework', Big Brother Watch, (April 2014), http://www.bigbrotherwatch.org.uk/files/briefings/BBW_transparency_2014.pdf

involved in serious crime as a trigger for the use of surveillance powers. Sections 5(3) and 22(2) of RIPA, for instance, set out only the purposes for which surveillance may lawfully be used. The identification of a legitimate aim is a necessary but not a sufficient condition for the use of surveillance powers. In particular, we see no reason why the requirement of 'necessity' should not be brought more closely in line with the requirements of the criminal law in this area. This would assist in narrowing what are otherwise broad definitions, e.g. 'national security' or the statutory definition of 'terrorism' under section 1 of the Terrorism Act 2000.

International cooperation

International arrangements governing the collection and sharing of the products of surveillance must be made public and subject to the oversight of Parliament and the courts. This requirement should be set out in legislation. This would not require disclosure of any detailed information concerning operations, techniques or capabilities but rather the publication and enactment of a legal framework that will apply to the transfer of individuals' sensitive data including that of UK residents.

At present it appears that the UK government has frequently circumvented domestic legal procedures by relying on secret arrangements with its intelligence allies that enable the collection, storage and sharing of significant and substantial amounts of information about individuals' online communications. The intelligence-sharing arrangements struck between the UK and its Five Eyes allies over the past 60 years are kept secret from the public and are therefore hidden from democratic scrutiny and oversight. By keeping these agreements secret, our intelligence agencies have removed our ability to ensure their accountability and compatibility with human rights standards. Intelligence arrangements must be subject to public, legislative and judicial scrutiny. Where the government obtains intelligence from its foreign allies, it must meet the same standards that are applicable to its own surveillance activities and should require that its allies meet similar standards. As noted above, it remains unclear that any legal

framework governs GCHQ's receipt of data from the NSA.

Greater transparency is also required in respect of GCHQ and the NSA's joint operations, where citizen's private data may be shared. The information exchanged appears to be extensive, with pooled resources making it hard to tell who has access to the information and who is ultimately accountable. For example, the joint programme MUSCULAR[27] taps into the internal cables of Google and Yahoo and is run by GCHQ from the UK. It is unclear how information relating to British citizens is protected during processing by the NSA, as privacy protections under US law are limited to US persons. We know that the NSA pays GCHQ substantial amounts of money for its support, some £100m in the three years running to 2013.[28] It is possible that besides funding GCHQ's core capabilities the payments also provide some form of legal and information ownership structure for certain joint activities.

The legal framework for the transfer of suspects between countries is publicly known, by way of extradition treaties and legislation. These public treaties do not damage our national security. Arrangements that relate to the agencies' powers to disclose and receive surveillance information should also be transparent.

3. JUDICIAL NOT POLITICAL AUTHORISATION

Judicial warrants and supervision

All intrusive, directed and targeted surveillance (including interception,

27 'How the NSA's MUSCULAR program collects too much data from Yahoo and Google', Washington Post (30 October 2013), http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/

28 Nick Hopkins and Julian Borger, 'Exclusive: NSA pays £100m in secret funding for GCHQ', The Guardian (1 August 2013), http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden

access to communications data and the use of covert human intelligence sources) should be authorised by a serving judge. This will allow the judiciary to perform its proper function of ensuring the rule of law is upheld. At present this power is exercised by a Secretary of State (in the case of the interception of communications), or a senior member of the relevant agency (in the case of authorisations for access to communications data, directed surveillance and the use of covert human intelligence sources). There is only qualified provision for judicial authorisation under RIPA in respect of the authorisation of intrusive surveillance by police (but, notably, not the intelligence services), in respect of requests for encryption keys under Part 3 of RIPA, and for local authorities seeking access to communications data.

Any arrangement which allows the executive to self-authorise the use of surveillance powers is, in our view, entirely unacceptable. It is the proper constitutional function of the independent judiciary to act as a check on the use of state power. Judges are best suited to applying legal tests to ensure that surveillance is necessary and proportionate pursuant to Article 8(2) of the ECHR. The involvement of judges improves public trust and confidence in the system of surveillance. David Bickford, the former Legal Director of MI5 and MI6, recently told a European Parliament inquiry that judicial authorisation is needed, stating: 'not only does this procedure reduce the risk or perception of collusion but, by removing the executive from these decisions, limits the room for accusations of political interference, and properly complies with the obligations of the state under ECHR'.[29] Polling conducted by the Joseph Rowntree Reform Trust in May 2014 found nearly half of all Britons backed judicial authorisation, with only one in six backing ministerial authorisation.

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

29 David Bickford CB, European Parliament LIBE Enquiry, Judicial Scrutiny of Intelligence Agencies (7 November 2013)

information that can be collected during a premises search and that collected via the targeted surveillance practices permitted under RIPA.

The introduction of prior judicial authorisation for all surveillance powers is, in our view, long overdue. The European Court of Human Rights recognised the desirability of prior judicial authorisation for surveillance in *Klass v Germany* in 1978, saying: '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.' In its recent decision in *Digital Rights Ireland*, the Grand Chamber of the CJEU similarly expressed the view that retention of communications data should be subject to 'prior review carried out by a court or by an independent administrative body'.[30] Under no circumstances could a Secretary of State or a senior member of the same public body be described as meeting these necessary requirements of independence and impartiality.

The shortcomings of self-authorisation have also been highlighted by the Metropolitan Police's misuse of authorisations for covert human intelligence sources, leading to gross privacy violations and harm to individuals. In recent years, undercover officers have infiltrated peaceful environmental groups, establishing long-term relationships and fathered children. It has also been revealed that undercover officers surveilled the family of Baroness Doreen Lawrence.

A new surveillance law should contain a clear set of requirements that must be satisfied before any surveillance can be authorised by a judge, namely the requirements of Article 8 ECHR (set out under point 2 of the recommendations for a new legislative framework on page 8).

In conducting the assessment of whether a particular instance of surveillance is justified, a judge would consider whether it pursues a specified

30 Digital Rights Ireland, para 62

legitimate aim, whether it is necessary to achieve that aim and whether it is proportionate i.e. the least intrusive way of achieving the aim identified.

New surveillance legislation must mandate judicial authorisation of all surveillance decisions including the interception of communications and access to communications data. Access should also be limited to a smaller number of public bodies and restricted to data that is necessary for the prevention, detection or prosecution of serious crimes.

4. EFFECTIVE DEMOCRATIC OVERSIGHT

Parliamentary oversight

The Intelligence and Security Committee (ISC) is a committee of MPs and peers tasked by the government with scrutinising the intelligence agencies. To date, the committee has consistently, and sometimes very publicly, failed in its duty to challenge these agencies. The ISC was established by the Intelligence Services Act (1994) at the same time as the intelligence agencies were placed on a statutory footing. This legislation arose after a whistleblower, Cathy Massiter, highlighted the intrusive surveillance by the intelligence agencies of trade unions and individuals such as Harriet Harman and Patricia Hewitt of the National Council for Civil Liberties (now Liberty), which was challenged in the courts. The recent Snowden revelations once again demonstrate that further reform is needed in order to protect individual privacy rights and freedom of expression.

To strengthen the ISC, the committee should have the status of a committee of Parliament, answerable directly to Parliament rather than to the prime minister. The ISC must take its own decisions on reporting and publication. The committee must be appropriately funded and staffed with independent experts able to undertake detailed forensic investigations and an independent secretariat, including independent legal and technical advice. The committee should have strengthened legal powers to require the production of information and to compel the attendance of witnesses.

In accordance with recommendations by the Home Affairs Committee, the chair of the committee should be a member of the largest opposition party and the Commons members of the committee should be elected.[31]

The operation of the ISC continues to be hindered by non-disclosure. As Parliament's Joint Committee on Human Rights (JCHR) has noted, the level of redaction of ISC reports is sometimes so great that 'it can be difficult to follow the Committee's work and to understand its reports.' The Home Affairs Committee has concluded: 'we do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability, and to the credibility of Parliament itself'.[32]

The failings of the ISC are well recorded. Following revelations that UK security services were complicit in the ill-treatment of detainees after 9/11, the JCHR reported that the security services account of the treatment of British Guantanamo detainee Binyam Mohamed was 'presented apparently without challenge' by the ISC. In the end it was left to the courts and investigative journalists to uncover the truth.

A further flurry of public criticism followed the revelation, during the course of the inquest into the 7/7 bombings, that there were 'inaccuracies' in the information provided to the ISC by the security services. In her Coroner's Report, Lady Justice Hallett made clear that 'the ISC, may have been inadvertently misled and thus that its reports may not have sufficiently addressed some of the central issues before it'. The poor scrutiny provided by the ISC was thrown into sharp focus by the much heralded public evidence session in which the heads of MI5, MI6 and GCHQ were publicly

---

31 Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 158, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

32 Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 157, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

questioned by the committee in November 2013. The questioning proved meek and nothing was revealed which was not already a matter of public record.

There must be concrete reform of the ISC if it is to provide meaningful parliamentary oversight of the security services.

The commissioners

The offices of the Intelligence Services Commissioner and the Interception of Communications Commissioner should be reformed. Both should report to Parliament and be insulated from executive influence. The commissioners are only part-time, inspect a small proportion of intercept warrants, have not publicly found a warrant to be disproportionate, have refused to provide adequate statistics and are under-resourced. Reform is long overdue.

In the absence of prior judicial authorisation for surveillance decisions, it is vital that all decisions be subject to ex post facto scrutiny by a judge. Unfortunately, however, the Interception of Communications Commissioner inspects only a small proportion of warrants made by the Secretary of State, somewhere between five and ten per cent. We note the recommendation of the Home Affairs Committee that this figure should be at least 50 per cent and that the commissioners should be full-time.[33]

Secondly, it is notable that the Interception of Communications Commissioner has never publicly stated that he has found a warrant or request for communications data to be disproportionate. In the commissioner's 2013 report whilst he found no disproportionate invasion of people's privacy, he listed caveats to this view, which included a handful

33 Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 163, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

of communications data errors which were not entirely isolated.[34]

A number of commissioner roles have been created to provide after-the-event oversight of the use of surveillance powers. Like the ISC, the Intelligence Services Commissioner and the Interception of Communications commissioner both report to the prime minister, although their reports are laid before Parliament. The bulk of the Intelligence Services Commissioner's reports are taken up with the restatement of the duties of his office. The remainder represents little more than a rubber stamping exercise. This appears to be a view shared by the JCHR which has noted that 'the reports of the commissioners, after redaction, give an indication of workload but are not otherwise illuminating'.

The Intelligence Services Commissioner has consistently refused to publish statistics on warrants or authorisations issued to the Security and Intelligence Services on the basis, repeated verbatim in every annual report, that disclosure would 'assist those unfriendly to the UK were they able to know the extent of the work of the Security Service, Secret Intelligence Service and Government Communications Headquarters in fulfilling their functions'. At a time when credible allegations of complicity in torture were emerging, the overarching message of the commissioner's reports was that the security services were 'conscientious, trustworthy and dependable'.

The Home Affairs Committee has also voiced 'serious doubts that either the Interception of Communications Commissioner role or the Intelligence Services Commissioner role should be part-time'. The committee recommended that the roles are full-time positions and that resources are increased to allow commissioners to examine half of the requests for information.[35]

---

34 2013 Annual Report of the Interception of Communications Commissioner, the Rt Hon. Sir Anthony May, para 4.28

35 Home Affairs Committee - Seventeenth Report, Counter-terrorism, 30 April 2014, paragraph 167, available at http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23102.htm

If the commissioners are to offer effective oversight, they must be empowered to conduct searching investigations, with adequate resources and the requirement to publish key statistics.

5. THE RIGHT TO REDRESS

Judicial oversight

This section considers the reform of the Investigatory Powers Tribunal (IPT). The IPT allows for secret procedures, offers little (if any) rationale for its decisions and is not subject to appeal in any court of law.

All legal challenges against the use of surveillance powers granted under RIPA are currently heard by the IPT (under Part IV of RIPA). The procedure operated by the IPT is seriously flawed and unfair to complainants. The IPT is under no duty to hold oral hearings. Even if it chooses to hold a hearing, all of its proceedings, including oral hearings, can be conducted in private. The IPT cannot disclose to a complainant the fact that a closed hearing is taking place, the identity of any witness or any information provided at the hearing, unless those attending the hearing, the witness, or the provider of the information consent. There is no provision for special advocates to represent the interests of the excluded party at any closed hearing (although the tribunal does on occasions appoint counsel to the tribunal). If the IPT finds against a complainant it cannot give reasons for its decision; this 'neither confirm, nor deny' policy leaves individuals unclear whether they were subject to lawful surveillance that was authorised under RIPA or not subject to surveillance at all. If the tribunal upholds a complaint it is only required to provide the complainant with a summary of its determination. It is telling that in the first decade of the tribunal's operation, it upheld only ten complaints, five of which came from members of the same family and concerned surveillance by a local authority that the authority admitted.[36]

36 The Investigatory Powers Tribunal, 'Operation – Cases Upheld', http://www.ipt-uk.com/section.aspx?pageid=9

There must be provision for appealing a decision of the IPT. After more than a decade worth of cases in which the Court of Appeal, the House of Lords and now the UK Supreme Court have each heard numerous appeals from closed proceedings in the High Court and SIAC[37] in cases involving national security, we can see no reason why the IPT's decisions should be insulated from challenge. In our view, the appropriate way forward would be to grant a right of appeal on points of law to the Court of Appeal.

Consistent with the conclusions of the UK Supreme Court in *Bank Mellat*, the overriding presumption must be that the IPT will hold public hearings in open court, save where the tribunal is satisfied that private or closed proceedings are necessary in the interests of justice. Any party excluded from closed proceedings should likewise be entitled to sufficient disclosure of the case of the other parties so that they can bring an effective challenge to any surveillance decision, and/or give effective instructions to any special advocate representing their interests.

Individuals should be notified that they have been subject to surveillance after the event, unless there is a specific reason for maintaining secrecy, so that they may have the opportunity to bring proceedings to obtain an effective remedy for any violation of their right to privacy.

Statutory remedies

Alongside the reform of the IPT, there must be adequate legal remedies both for unlawful access to communications data and additional unauthorised state use of surveillance techniques.

These infringements of fundamental rights should attract penalties which properly reflect the grave breach of trust involved. It is an offence to

37 Special Immigration Appeals Commission

intercept communications unlawfully, but there is no offence dealing with other forms of unlawful surveillance, such as misuse of communications data or covert human intelligence sources. There is an offence of unlawfully accessing personal data under section 55 of the Data Protection Act 1998 with the sanction of a fine. Whilst most people will never know whether or not their data has been improperly retained or accessed, for those who do find out, often their only option is to bring a claim under the Human Rights Act. However, such actions must ordinarily be taken before the Investigatory Powers Tribunal (IPT), a flawed and secretive process as outlined above. A stronger and more accessible system of redress is necessary to enable citizens to enjoy their human rights.

Intercept evidence

The bar on the admissibility of intercept evidence should be lifted to allow criminal prosecutions to take place where surveillance has been properly and proportionately gathered against criminal suspects. At present, intercept material (likely to have been gathered as part of criminal investigations, including into allegations of terrorism) cannot be used as evidence in court under section 17(1) of RIPA. In legal terms this bar is an anomaly. Elsewhere in the world, intercept evidence has been used effectively to convict those involved in terrorism and other serious crimes. Moreover, while we cannot use information gained from interception in this country in the criminal courts, foreign intercepts are increasingly used in civil proceedings and the ban on intercept admissibility has been used to justify major incursions into traditional fair trial protections (e.g. control orders, TPIMs, secret courts). There are no fundamental human rights objections to the use of intercept material, properly authorised by judicial warrant, in criminal proceedings.

Successive Directors of Public Prosecutions namely Sir David Calvert, Lord Ken Macdonald and Sir Keir Starmer, have called for the bar to be lifted.[38] GCHQ, meanwhile, is known to have actively resisted efforts to amend laws restricting the use of intercept evidence in court proceedings, stating that allowing the admission of such evidence would reveal the scale of interception conducted by the intelligence agencies and could prompt a 'damaging public debate' about the compliance of interception with Article 8 of the European Convention on Human Rights. This highlights the important role that admissibility could play in keeping the activities of law enforcement and intelligence agencies in check. The European Court of Human Rights has previously found that the possibility of excluding illegally obtained surveillance was 'an important safeguard, as it discouraged the investigating authorities from collecting evidence by unlawful means'. It is recommended that the bar on the use of intercept evidence in criminal trials should be lifted, allowing more prosecutions to be brought against terror suspects and providing increased judicial oversight.

6. A SECURE INTERNET FOR ALL

The government has undermined encryption standards and weakened commercial security online for the purpose of mass population surveillance. This risks undermining the trust essential for online financial transactions. More importantly, as this section will outline, undermining online security opens the door for authoritarian regimes to breach our collective security.

Despite a complete absence of any specific legal power, the UK's intelligence agencies have infiltrated almost every aspect of modern communications systems. From breaking encryption standards, hacking phones, computers

38 Mr Keir Starmer QC, ref: Oral Evidence of Director of Public Prosecutions, Keir Starmer QC to the Home Affairs Select Committee (10/11/09) available at: http://www.publications.parliament.uk/pa/cm200910/cmselect/cmhaff/117-ii/9111001.htm; Ken MacDonald QC, ref: Law Society Gazette, 'Human rights lawyers back Goldsmith call to use intercept evidence in court', 28 September 2006; Sir David Calvert-Smith QC, ref: The Observer, 'Juries should hear phone taps to nail crime gangs', by David Rose, 8 September 2002 and quoted in Parliament by: Ms Vera Baird, Hansard.

and networks, to exploiting system vulnerabilities and mandating the building of backdoors into communications infrastructure. GCHQ has required communications service providers to place taps into undersea fibre-optic cables to facilitate mass data interception and paid them to do so. The scale of this operation has undermined the integrity and security of the internet as a whole. GCHQ's 'Edgehill' programme has focused on gaining access to encrypted traffic on the 'big four' webmail service providers: Hotmail, Google, Yahoo and Facebook. By 2015, GCHQ hoped to have cracked the codes used by 15 major internet companies and 300 Virtual Private Networks (VPNs) used by businesses to provide secure remote access.[39] This is in spite of the government having no specific legal power to do so. This may constitute a breach of the Computer Misuse Act 1990. Fatally-weakened encryption standards not only make our private data vulnerable for misuse by agencies of our own government, but also make it equally vulnerable to surveillance from foreign intelligence agencies in hostile states.

The breach of trust by the NSA and GCHQ is having a major economic impact. Not only do broken encryption standards leave customers vulnerable to theft and fraud by online criminals, but the breakdown in trust in US and UK high-tech firms is now becoming clear.

Daniel Castro, an analyst at the Information Technology and Innovation Foundation predicts the US cloud computing industry could lose $35 billion by 2016. Recent analysis by Forrester Research, a technology research firm, said the losses could be as high as $180 billion, or 25 per cent of US industry revenue, based on the size of the cloud computing, web hosting and outsourcing markets and the worst case for damages.[40] The Global Network Initiative – a multistakeholder group including Google, Facebook,

---

39 James Ball, Julian Borger and Glenn Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security', The Guardian (6 September 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-securit

40 James Staten, The Cost of PRISM Will Be Larger Than ITIF Projects (14 August 2013) http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects

Microsoft and Yahoo – has raised concerns about the impact of surveillance on commerce and opposed the fast-tracking of the DRIPA legislation.

As the private sector designs and maintains the networks, hardware and software that make up our communications systems, private sector entities should be empowered to resist government demands for cooperation with surveillance activities and have such claims mediated by the judiciary. Increased transparency will support corporate push-back against unreasonable government demands. If companies cooperate in breaching human rights they should be held responsible.

DON'T SPY ON US

About us

Don't Spy On Us is a coalition of the most influential organisations who defend privacy, free expression and digital rights.

We've come together to fight back against the system of unfettered mass state surveillance that Edward Snowden exposed. Right now, the UK's intelligence services are conducting mass surveillance that violates the right to privacy of internet users and chills freedom of expression.

Executive Committee

ARTICLE 19 · OPEN RIGHTS GROUP · ENGLISH PEN · PRIVACY INTERNATIONAL · LIBERTY80 PROTECTING CIVIL LIBERTIES PROMOTING HUMAN RIGHTS · BIG BROTHER WATCH