



Analysis

GCHQ is authorised to “spy on the world” but the UK Interception of Communications Commissioner says this is OK as it is “lawful”

Tony Bunyan

Contents

1. The Commissioner’s Report for 2013	2
1.1. Interception of content warrants	2
1.1.1. Section 8.1 interception warrants	3
1.1.2. Section 8.4 warrants and certificates (“certified warrants”)	3
1.2. The number of warrants issued	4
1.3. Communications data authorisations	5
1.4. An unfortunate coincidence	7
2. “Media disclosure and Public Concerns”	9
2.1. Section 8.4 warrants and Ministerial “certificates”	10
2.2. “Mixed files” including British residents	12
2.3. The Intelligence and Security Committee report: February 2013	13
3. Conclusion: State surveillance is as old as the state	18

This analysis finds that UK “law” itself is part of the problem as it allows the agencies to “lawfully spy on the world”. This is compounded by the agencies’ use of new technologies to act outside of their legal powers. [1] It also questions whether the Interception Commissioner is capable of providing effective oversight of state surveillance activities.

The first part of this analysis examines the 2013 report by the new Interception of Communications Commissioner, Anthony May, which provides greater statistical detail than previous reports. [2] The second part examines the Commissioner’s attempt to refute concerns posed by the Snowden revelations regarding the role of GCHQ, which he fails to do so, despite widespread acceptance by the British media of his conclusion that fears about mass surveillance by GCHQ in cooperation with the USA are unfounded. [3] The role and powers of the Commissioner are set out in the Regulation of Investigatory Powers Act 2000 (RIPA 2000). [4]

Ever since the UKUSA Agreement of 1946 the USA and UK (through GCHQ) have cooperated on the global surveillance of communications. Throughout the Cold War and then the “war on terrorism” this cooperation has become closer and closer. Only now with the Snowden revelations have many of their dubious activities been exposed and fundamental questions asked about oversight and accountability.

1. The Commissioner’s Report for 2013

The first part of the Report deals with interception warrants (telecommunications surveillance) and requests for communications data by law enforcement agencies (LEAs), MI5, MI6 and GCHQ. [5]

1.1. Interception of content warrants

Part I of the Regulation of Investigatory Powers Act 2000 covers the issuing of interception warrants (real-time surveillance – historically known as “telephone tapping”) for all communications of named individuals or entities. [6] These are signed by a Secretary of State. The main secretaries involved are those of the:

Home Office: Police and law enforcement agencies (police, immigration, customs and Special Branches outside London) and MI5 (internal Security Service); **Foreign**

[1] EU agrees rules for remote computer access by police forces – but fails, as usual, to mention – the security and intelligence agencies:

<http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf>

[2] <http://www.statewatch.org/news/2014/apr/uk-interception-comm-2013-report.pdf>

[3] David Cameron welcomes all-clear on spy agencies from Sir Anthony May - Surveillance watchdog's report says authorities do not engage in random mass intrusion into affairs of law-abiding UK citizens:

<http://www.theguardian.com/politics/2014/apr/08/david-cameron-welcomes-all-clear-spy-agencies-surveillance-watchdog-anthony-may> and Spies cleared of Snowden's claims of mass intrusion: Communications watchdog says they did not break any laws:

<http://www.dailymail.co.uk/news/article-2600239/Spies-cleared-Snowdens-claims-mass-intrusion-Communications-watchdog-says-did-not-break-laws.html#ixzz2zSBA2det>

[4] RIPA 2000: <http://www.statewatch.org/news/2014/apr/uk-ripa-2000.pdf>

[5] See Statewatch Observatory: UK: Surveillance statistics: 1937-2014:

<http://www.statewatch.org/uk-tel-tap-reports.htm>

[6] See Code of Practice:

<http://www.statewatch.org/news/2014/apr/interception-comms-code-practice.pdf>

Office: MI6 (external Secret Intelligence Service, SIS) and GCHQ (Government Communications Headquarters); **Defence Ministry:** Defence Intelligence (Defence Intelligence Staff, DIS). [7]

Interception warrants can be signed by a Secretary of State, under Section 5.3 of RIPA 2000 for the following “statutory purposes”:

- “in the interests of national security”;
- preventing or detecting serious crime;
- “safeguarding the economic wellbeing of the UK”; and
- international mutual assistance agreement.

There are two types of interception warrants: **Section 8.1 warrants** and **Section 8.4 warrants** both of which cover the interception of the **content** of the communication and **communications data**. All such warrants include historical and real-time interception.

If issued for the purposes of national security or the economic wellbeing of the UK, the initial duration of a warrant is six months. Warrants issued for serious crimes last three months. Both can be renewed or “modified”. [8]

1.1.1. Section 8.1 interception warrants

Section 8.1 warrants have to give the name of a “person” or premises. However, a **“person” also “includes any organisation or any association or combination of persons”** – so it could cover a single individual, a group of 20 people or an organisation of thousands. Since 1997, single ‘catch-all’ warrants have been issued against a “person” or premises, covering all their communications and internet service providers (CSPs/ISPs) - previously each separate provider had to get a separate warrant, for example for landline phones, mobile phones and internet use. This change disguised the growth in interception warrants from 2007 onwards, as did the introduction of “modifications” which previously required a new warrant to be issued (see below).

1.1.2. Section 8.4 warrants and certificates (“certified warrants”)

Section 8.4 warrants and certificates are **issued by a Secretary of State and do not have to name or describe a “person” as the target, or name a “single set of premises”**. Section 8.4 warrants are issued where communications are **“outside of the British Islands”**. So, for example, this could cover the surveillance of communications sent or received across the other 27 EU Member States. **Is this a blank cheque to spy on the rest of the world, just like FISA in the USA?** [9]

[7] MOD: <https://www.gov.uk/defence-intelligence#intelligence-collection> and: Wiki: http://en.wikipedia.org/wiki/Defence_Intelligence

[8] “Modification” means changing the requested service providers or the details of the individual(s) or entity: See: Changes in telephone-tapping warrant procedures disguises true figures: <http://www.statewatch.org/news/2004/jul/uk-tel-tap-procedures.htm>

[9] See: The legal loopholes that allow GCHQ to spy on the world: <http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world/print>

It is interesting to note that section 702 of the US FISA Amendment Act 2008 [10] targets the surveillance of “foreigners” (ie: not US citizens) and thus makes “lawful” the foreign surveillance programs used by the National Security Agency (NSA). From 2001, data collection activities of this kind were authorised under the President's Surveillance Program which has a similar scope to the UK's “sent or received” global warrants adopted under RIPA in 2000.[11]

In the UK and EU it is not difficult to construct a scenario in which a “cross-border protest” is planned on climate change - as it was in Copenhagen in December 2009 - where protestors from across Europe assemble. [12] According to a *Guardian* report based on GCHQ documents:

“Lawyers at GCHQ speak of having 10 basic certificates, including a “global” one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus... GCHQ says it can also seek a sensitive targeting authority (STA), which allows it snoop on any Briton “anywhere in the world” or any foreign national located in the UK.”

A Section 8.4 certificate could make “lawful” placing people and groups from the 27 other EU Member States under surveillance while Section 8.1 warrants could be used for those inside the “British Islands”.

The “certified warrants” issued by a Secretary of State under Section 8.4 of RIPA have never been mentioned by any previous Commissioner, as *Statewatch* has noted. [13]

1.2. The number of warrants issued

The number of Section 8.1 interception warrants issued in 2013 was 2,760 (these **do not include sweeping Section 8.4 warrants and certificates** issued by a Secretary of State). The figures for 2011 were 2,911 and 3,372 for 2012.

The new Commissioner breaks ranks with his predecessor (Sir Paul Kennedy, Commissioner from 2006-2013) by publishing the number of warrants “extant” (in place) on 31 December 2013: 1,669. This figure is important. If a similar number were “extant” a year earlier then the number of warrants in operation during 2013 would be 2,760 new warrants issued plus 1,669 warrants already in place from the previous year giving a historically comparative figure of 4,429 operational warrants over the full year. We are not given the number of “modifications” to warrants issued during the year, although these have been provided in the past (from 1998 to 2004

[10]

http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008

[11] The 1978 FISA was directed in Cold War terms towards foreign agents and espionage:

<http://www.statewatch.org/news/2014/apr/usa-fisa-1978.pdf>

[12] Schengen Borders checks implemented

<http://www.statewatch.org/news/2010/mar/denmark-eu-border-controls-6927-10.pdf> and Climate change activist stopped from travelling to Copenhagen:

<http://www.theguardian.com/politics/2009/oct/14/climate-change-activist-held/print> and

Wiki: http://en.wikipedia.org/wiki/2009_United_Nations_Climate_Change_Conference

[13] Interception Commissioner fails to report on Section 8(4) certificates authorising GCHQ's mass data collection: <http://www.statewatch.org/news/2013/dec/uk-interception-reports.htm>

and 2007 to 2010). [14] Historical figures show that the number of "modifications" are, on average, three times the number of warrants issued and extant. This gives a total number of 13,287 warrants on a historical basis for 2013, **the second highest number on record.** [15]

1.3. Communications data authorisations [16]

Part II of the Regulation of Investigatory Powers Act 2000 covers the authorisation of requests for access to "communications data" from service providers. [17]

Communications data, also known as metadata, covers e-mails, faxes, phone lines, mobile phone calls (including their location) and internet usage (which also reveals the content of the communication, the web pages visited, even though under RIPA 2000 access to the content of a communication requires the issuing of a Section 8.1 warrant).

Both the government and the Interception of Communications Commissioner typically respond to criticism of the gathering of metadata with the argument that it only covers "*the 'who', 'when' and 'where' of a communication but **not the content.***" (p.19, emphasis added)

The Commissioner's report fails to address the question of trawling the "**metadata**" based on communication data to create detailed profiles on "targets" and associates. However, metadata can be used to build up a frighteningly detailed picture of an individual's life: all their friends and contacts - and their friends and contacts - and, by what is known as "three hops" - their friends and contacts too. [18] **The collection, searching and analysing of individuals "metadata" (taken from communications data) is not harmless, it is highly intrusive.**

The power to gather communications data comes from an "authorisation" signed by an official from the agency that wishes to acquire the data – it is self-authorising (RIPA Section 22.3). A notice is then sent to the CSP/ISP to hand over the required data (Section 22.4). Both the authorisation and notice are valid for a month but can be renewed.

The scope for issuing notices is similar to that for Section 8.1 warrants but allows a Secretary of State to add further purposes by means of an "affirmative resolution procedure" in parliament (usually nodded through parliament without debate). When "in the interests of national security", authorisations and notices are the responsibility

[14] See Statewatch Observatory: UK: Surveillance statistics: 1937-2014:

<http://www.statewatch.org/uk-tel-tap-reports.htm>

[15] The Commissioner's main critical observation on interception warrants is that: "*related communications data are in some instances retained for a variety of longer periods. I have yet to satisfy myself fully that some of these periods are justified*"

[16] See Code of Practice:

<http://www.statewatch.org/news/2014/apr/code-of-practice-acquisition.pdf>

[17] Service providers are required to retain communications and content data under the Anti-Terrorism, Crime and Security Act 2000 (ATCS):

<http://www.legislation.gov.uk/ukpga/2001/24/contents>

[18] This is critically examined in: The Snowden files: why the British public should be worried about GCHQ: <http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester>

of MI5 except where a role is given to Special Branches (outside London) or the Metropolitan Police Counter Terrorism Command. [19]

The number of authorisations and notices issued were as follows (the figures for 2008-2010 are taken from previous reports):

- 2013: 514,608
- 2012: 570,135
- 2011: 494,078
- 2010: 552,550
- 2009: 525,130
- 2008: 504,073

Yet again no figures are given for the number of “modifications” - where notices are renewed after one month.

The main purposes of notices and authorisations breaks down as follows:

- 76.9% to “prevent or detect crime or **prevent disorder**” (emphasis added, Figure 7, p. 26);
- 11.4% for purposes of “national security”;
- 11.3% emergencies – to prevent death or injury; and
- 0.4% “Other” including 0.11% for protecting “economic well-being of the UK”.

This is the only place in his report that the Commissioner refers to communications data being accessed for public “disorder” purposes.

The Commissioner does recognise the flaws in the statistics provided: “In my view the unreliability and inadequacy of the statistical requirements is a significant problem which requires attention.” (p.24)

For example, the number of individual items required by the agencies is not recorded – traffic data, subscriber data, service use information or a combination - and some agencies may use a single notice for three or more phone numbers whereas others issue three separate notices. The Commissioner has requested that the Home Office extend the figures to include items broken down by purpose (e.g. crime or national security) and by type of crime. He does not however refer to figures on the number of instances where surveillance has led to arrest and charge, conviction or acquittal. [20]

Overall, the Commissioner admits that the 514,608 notices issued in 2013 “seems to me to be a very large number. It has the feel of too many... [and that there may be] a significant institutional overuse”.

[19] The London/Metropolitan Police Special Branch, founded in 1883, is now part of the Counter Terrorism Command which also carries out a number of national roles. The other 43 police forces in the UK still have Special Branches.

20 The Commissioner notes that there is a significant difference between the interception regime (tapping warrant in Section 8.1) and access to communications data, namely, statutory “destruction provision” – the latter does not have one!

He holds that this is particularly the case because the police and law enforcement agencies (including immigration and customs) account for 87.7% of notices. The figures by agency for notices issued to CSPs/ISPs were:

- Police and law enforcement agencies: 451,243
- MI5 (Security Service): 56,996 [21]
- Other public authorities: 2,603
- Local authorities: 1,776
- GCHQ: 1,406
- MI6 (Secret intelligence Service): 672

Readers might well be surprised that GCHQ and MI6 are at the bottom of the list but it must be remembered that these figures only refer to notices and authorisations issued under RIPA 2000. GCHQ conducts **most of its surveillance via satellites and fibre-optic undersea cables which does not involve issuing notices to CSPs and ISPs.** [22] MI6 gathers most of its intelligence via GCHQ, while Defence Intelligence (DIS), which has its own data-gathering capacity, is not mentioned.

The report notes that “larger users”, like LEAs, have “bespoke workflow systems” which use automated access to CSPs/ISPs. [23] The report does not provide a breakdown by agency for direct interception warrants (Section 8.1), where a single warrant can cover a whole organisation or an association of individuals.

1.4. An unfortunate coincidence

The Commissioner was not to know that the publication of his Annual Report would coincide with the Court of Justice of the European Union (EU) judgment that mandatory data retention is unlawful. [24] The Commissioner is only responsible for **authorisations** (by agencies) and **requests** (to CSPs/ISPs) to hand over communications data under RIPA 2000.

The UK law that requires CSPs to **retain** communications and content data is the controversial **Anti-Terrorism, Crime and Security Act 2001** (ATCSA). [25] It requires CSPs to retain data for the purpose of combating terrorism and related crimes. Its scope is defined as:

- a) *for the purpose of safeguarding national security; or*

[21] In the Commissioner's 2009 report: *"Of all the intelligence agencies the Security Service is the largest user of communications data and it has a **fully automated system** to manage its requirements."*

[22] Mastering the internet: how GCHQ set out to spy on the world wide web: <http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet> and [Chart: Worldwide SIGINT/Defense Cryptologic Platform](#) (jpg) The "double-bubble" over the UK indicates both interception of high speed optical cables and well as satellite collection by GCHQ Cheltenham and Bude and the US base in Menwith Hill, Yorkshire.

[23] In his 2007 report the Commissioner records: *"I am pleased to say that more and more police forces are introducing **automatic systems** for the management of communications data requests"* (emphasis added) *manage its requirements.*" (emphasis added)

[24] CJEU: High Court (Ireland) and the Verfassungsgerichtshof (Austria) and Digital Rights Ireland Ltd: <http://www.statewatch.org/news/2014/apr/eu-ecj-data-ret-judgment.pdf>

[25] ATCSA 2001: http://www.legislation.gov.uk/ukpga/2001/24/pdfs/ukpga_20010024_en.pdf and see: "Data retention and police access in the UK - a warning for Europe": <http://www.statewatch.org/news/2005/nov/01uk-eu-police-access-to-data.htm>

- b) *for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security.*” (Section 102)

Statewatch amongst others pointed out at the time that this Act could not be used to retain data and give access to security, intelligence and law enforcements agencies for **crime in general** as its purpose was limited. In 2002, the Home Secretary introduced a voluntary Code of Practice to extend its scope. [26]

After the EU Directive on Data Retention was adopted in 2006 [27] UK law was brought in line through two more Statutory Instruments, in 2007 and 2009. [28] The Consultation Paper issued before the 2007 change made clear that the retention of data by CSPs/ISPs referred to “fixed line and mobile telephone” – this was extended to “internet access, internet telephone and internet e-mail” in 2009.

The CJEU judgment states:

“The Court of Justice declares the Data Retention Directive to be invalid:

It entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary” [29]

Of particular relevance here is the court’s finding concerning the passing of personal data to third countries, for example US state agencies. It says:

*“[T]he Court states that the directive does **not** require that the data be **retained within the EU**. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.”*
(emphasis in original)

The Court also found that the Data Retention Directive “**exceeded the limits imposed by compliance with the principle of proportionality**” (emphasis in original) and further that it did not limit its scope “to what is strictly necessary”

[26] Statutory Instruments are secondary legislation nodded through both Houses of Parliament, usually without debate.

[27] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF>

[28] Under the European Communities Act 1972: Consultation Paper: Home Office:

<http://www.statewatch.org/news/2014/apr/uk-ho-cons-eur-dir-data-ret.pdf>; 2007:

<http://www.statewatch.org/news/2014/apr/uk-data-ret-si-ec-dir-2007.pdf>; 2009:

<http://www.statewatch.org/news/2014/apr/uk-mand-ret-2009.pdf>

See also: SECILE report: Data Retention in Europe: A Case Study:

<http://www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf>

[29] CJEU Press release: The Court of Justice declares the Data Retention Directive to be invalid:

and: Judgment: Press release: <http://www.statewatch.org/news/2014/apr/eu-ecj-data-ret-prel.pdf>
and <http://www.statewatch.org/news/2014/apr/eu-ecj-data-ret-judgment.pdf>

(necessity principle). It also stated the general grounds which seriously affect fundamental rights set out in the Charter:

"[D]ata, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.... the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance." [30]

The European Data Protection Supervisor (EDPS) commented:

*"The judgment also means that the EU **should take a firm position in discussions with third countries, particularly the U.S.A. on the access and use of communications data of EU residents.**"* [emphasis in original][31]

2. "Media disclosure and Public Concerns"

A 24-page section of the report entitled "Media Disclosures and Public Concerns", which was widely reported, contains the Commissioner's defence of the agencies surveillance activities, which he declares to be entirely "lawful":

"If, in my judgment, any of their activities are unlawful or disproportionate, I am obliged to say so in this report and would do so without hesitation. To the extent that this report is in fact supportive, that is because I have been properly satisfied that their activities are lawful and proportionate." (p44)

He says that there is a "general lack of understanding" based on a "widespread lack of informed understanding" (p.45) which he seeks to allay. **But he is only concerned with activities that fall under RIPA 2000.**

The section opens by referring to the "alleged activities" of the USA's NSA and UK's GCHQ and the Commissioner says his role is to report whether UK agencies are acting "unlawfully" under RIPA 2000 Part I. He thus gives the appearance of investigating all the reported and documented activities of GCHQ.

However, there is no mention of interception of fibre-optic cables or satellite transmissions by GCHQ and the massive US base in Menwith Hill in Yorkshire. [32] Neither of these data gathering methods require requests to CSPs/ISPs as the data is taken from undersea fibre-optic cables or from the ether as messages pass up into space and down again. [33] A leaked NSA map sets out the global "Classes of Accesses" including 50,000 "implants", 16 of the 20 "Covert, Clandestine or Cooperative" world-wide accesses to high speed optical cables, 80+ SCS (Special Collections Service) embassy/mission-based spying centres, and FORNSAT (foreign

[30] See: Are national data retention laws within the scope of the Charter?:

<http://eulawanalysis.blogspot.co.uk/2014/04/are-national-data-retention-laws-within.html>

[31] European Data Protection Supervisor (EDPS):

<http://www.statewatch.org/news/2014/apr/eu-ecj-mand-ret-edps-statement.pdf>

[32] "Lifting the Lid on Menwith Hill:

<http://www.statewatch.org/news/2012/mar/uk-menwith-hill-lifting-the-lid.pdf>

[33] NSA-GCHQ-Menwith Hill: Map: <http://www.statewatch.org/news/2013/nov/nsa-cne-map.jpg>

satellite collection). The only "double-bubble" is over the UK which indicates both interception of high speed fibre-optic cables and satellite collection by GCHQ Cheltenham and its Bude base and the US base in Yorkshire.

It is therefore not surprising that no reference is made to GCHQ's remote access to computers [34] nor to bogus websites [35] nor the disruption of "hostile" websites run by the Joint Threat Research Intelligence Group (JTRIG) which focuses on cyber forensics, espionage and covert operations including the **4D's**:

Deny/Disrupt/Degrade/Deceive. Techniques employed include bombarding an individual's phone(s) with calls, deleting their online presence, emailing or texting their friends and colleagues, blogging pretending to be a victim, and stopping someone's computer from working. [36]

No figures are given of the number of Section 8.4 warrants and certificates issued by a Secretary of State nor how many people have been put under surveillance across the world.

2.1. Section 8.4 warrants and Ministerial "certificates"

The Commissioner seeks to defend Section 8.4 warrants and "certificates" at length on the grounds that this power was already in place under the Interception of Communications Act 1985, Section 3(2) to (4). [37] This is quite correct but none of the Annual Reports from the Commissioners appointed under that Act ever mentioned the use of "certificates" concerning "external communications" signed by a Secretary of State.

The Commissioner says that Section 8.4 warrants have given rise to "understandable concern," and notes that:

"Section 8.4 disapplies the provisions of section 8.1 and 8.2 in certain circumstances. This means that a section 8.4 warrant does not have to name or describe one person as the interception subject or a single set of premises as the target of interception. It does not have to have a schedule setting out specific factors identifying the communications to be intercepted." (p.49)

First, it should be noted that the Commissioner's report does not say how many sweeping Section 8.4 warrants and "certificates" signed by a Secretary of State were issued (or renewed) in 2013. [38]

Second, as noted above, a "**person**" can include "**any organisation or any association or combination of persons**". The number of "persons" or

[34] Statewatch analysis: EU agrees rules for remote computer access by police forces – but fails, as usual, to mention – the security and intelligence agencies:

<http://www.statewatch.org/analyses/no-83-remote-computer-access.pdf> and

EU: Welcome to the new world of the interception of telecommunications:

<http://database.statewatch.org/article.asp?aid=30612>

[35] GCHQ: "Squeaky Dolphin":

http://www.statewatch.org/news/2014/apr/snowden_youtube_nbc_document.pdf

[36] Set of GCHQ slides - JTRIG: <http://www.statewatch.org/news/2014/feb/gchq-cyber-attack.pdf>

37 Interception of Communications Act 1985:

<http://www.statewatch.org/news/2014/apr/uk-1985-intcept-comms-act.pdf>

[38] GCHQ taps fibre-optic cables for secret access to world's communications:

<http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

organisations or informal “associations” of “persons” is therefore **limitless and global** under Section 8.4 warrants, so too the number of targeted “premises” (which may cover tens or hundreds of people). Third, and crucially, a schedule of the “communications to be intercepted” is **not** required under a Section 8.4 warrant and under Section 8.5 can extend to communications “not identified” in the warrant. [39]

For Section 8.4 there are no specified “person(s), premises or named CSPs/ISPs – the warrant’s targets are **limitless and global and not restricted to data provided by CSPs/ISPs – thus making “lawful” the massive trawling of communications and their content from satellite and fibre-optic cables.**

As with FISA in the USA, it is “lawful” for GCHQ to “spy on the world” as long as it does not spy on people in the British Islands (see below).

In the words of the Commissioner there are limits:

- Section 8.4 warrants “are limited to *external communications*” (emphasis in original). **Such a limitation directly echoes the USA’s FISA.**
- The “certificate” issued by the Secretary of State, in addition to the warrant, has to meet the following very broad “statutory purposes”: be in the “interests of national security”, to prevent or detect serious crime or to safeguard the UK’s “economic well-being”.

The Commissioner then asserts, in all seriousness, that:

“The intercepted material which may be examined in consequence is limited to that described in a certificate issued by the Secretary of State.”

But there are no limits on the *external communications* which can be gathered and trawled and the “statutory purposes” for examining the intercepted material are very, very broad.

The report then says that there are “extra safeguards” on the use of Section 8.4 warrants in Section 16. Intercepted material can only be **examined** (no mention of collected, see below) if it “does not relate to the content of communications of an individual who is known to be for the time being in the British Islands.”

Again, “spying on the rest of the world” is OK.

Does this mean people in the British Islands are safe? No. In general Section 8.4 excludes those in the British Islands but there are two exceptions set out in Sections 16.3, 16.4 and 16.5. Under 16.3, intercepted material (content and traffic data) can be examined under a Section 8.4 certified warrant where the certificate refers to “the **individual** in question” (note the use of the term “individual” not “person”) for the “statutory purposes” of national security (6 months or 3 months for serious crime and economic well-being) (16.3). Under Sections 16.4 and 16.5, material “acquired” under a Section 8.4 certified warrant “for a **person** who is within the British Islands” can be examined on the authorisation of a senior official for a short period of time where it is found that a person believed to be abroad has then entered the British Islands. The

[39] A Section 8.1 interception warrant schedule would identify the named “person(s)”, premises and CSPs/ISPs to whom the warrant is served.

argument is that “essential intelligence” is not lost if either a normal Section 8.1 warrant or a Section 16.3 certificate is issued.

In summary, the communications of a person in the British Islands can be intercepted under a Section 16.3 certificate (which is similar to a Section 8.1 warrant).

The Commissioner provides little detail of how Section 8.4 certified warrants are used except by referring to the need to “filter” “significant volume(s) of data” so as to leave material “which is strongly likely” to include data which can lawfully be examined – the rest is “immediately discarded” (p.52). This he uses to back up his argument that certificates are used “lawfully” for “statutory purposes”.

However, it is not acceptable in a democratic society to undertake mass surveillance, treating everyone as a potential suspect. This raises the second issue: the criteria used to “filter” what data to keep and examine and what to discard. If threats to “national security” are narrowly drawn then only terrorist groups and their direct support groups would be targeted. But if the lines are drawn to include “poetry” deemed to support terrorism [40] and individuals not suspected of having committed any terrorist offence but perceived by LEAs and security and intelligence agencies to be conveying “Radical Messages”, defined as embracing “Extreme right/left, Islamist, nationalist, anti-globalisation etc.,” these are bridges too far. [41] Are cross-border protests or national protests against fracking or austerity threats to “national security”? What of those detained and questioned under Schedule 7 [42] at ports and airports, or Green Party Councillor Ian Driver who was monitored by the Metropolitan Police for campaigning against the export of live animals from Ramsgate and Dover ports? [43]

2.2. “Mixed files” including British residents

One of the major concerns in the USA is that the NSA is using FISA to spy not just on people outside the country (“foreigners”) but also those living there too which is supposed to be unlawful – a problem recognised by the Obama report concerning what are termed “mixed files” (covering US citizens as well as “foreigners”). [44]

The same problem affects GCHQ. The Commissioner admits that:

“[I]t is not at the moment technically feasible to intercept external communications without the risk that some internal communications may also be initially intercepted.”

This is “legitimised” by Section 5(6)(a) of RIPA 2000 by the provision:

[40] Samina Malik, the self-described “Lyrical Terrorist”, was the first woman to be convicted under the UK’s 2000 Terrorism Act: http://en.wikipedia.org/wiki/Samina_Malik

[41] Intensive surveillance of “violent radicalisation” extended to embrace suspected “radicals” from across the political spectrum - Targets include: “Extreme right/left, Islamist, nationalist, anti-globalisation etc”:

<http://www.statewatch.org/analyses/no-98-eu-surveillance-of-radicals.pdf>

[42] Schedule 7 detentions link: <http://schedule7stories.com/>

[43] Files on politicians, journalists and peace protesters held by police in “domestic extremist” database: <http://database.statewatch.org/article.asp?aid=32963>

[44] Obama Directive: <http://www.statewatch.org/news/2014/jan/us-pres-dir.pdf>

“[A]ll 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.”

The Commissioner comments that:

“[T]he unintended but unavoidable initial interception of some internal communications under Section 8(4) warrant is lawful.... The volume of internal communications lawfully intercepted is likely to be an extremely small percentage of the totality of internal communications and of the total available to an interception agency under a Section 8(4) warrant.”

Without the numbers it is hard to know what this means – a small percentage of millions of messages is still an awful lot. In June 2013, *The Guardian* revealed the vast scale of the UK’s TEMPORA programme which is used for the interception of undersea fibre-optic cable messages:

“The documents reveal that by last year GCHQ was handling 600m “telephone events” each day, had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time.” [45]

At the core of the “statutory purposes” and the “lawful” surveillance of communications for Section 8.4 warrants and certificates is the scope of “**sent or received**” outside the British Isles. During a NATO exercise in December to January 2010 it is known that millions of external communications and their content were intercepted by intelligence agencies in Italy, France, Spain and the Netherlands, an exercise justified on the grounds that it was “in support of military operations” but which inevitably would have gathered information on citizens of those countries. [46] A NATO exercise where each of its 26 European members trawled communications on the basis of “sent or received” from outside their own country would catch everyone’s communications.

Logically, communications sent to the UK from other countries and ones received “outside” in other countries (but originating from the UK) can be “lawfully” intercepted anywhere in the world, then analysed, fed into domestic or international intelligence assessments and operations, and passed onto the “Five Eyes” partners and its extended networks. [47]

2.3. The Intelligence and Security Committee report: February 2013

The Commissioner’s report tries to give the impression that it covers GCHQ’s data gathering operations, but admits some of these activities are strictly outside his remit. There is no reference to data gathered by the other Five Eyes or NATO and

[45] <http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>

[46] A coincidence or part of a much wider trawl of communications across the EU?

<http://www.statewatch.org/news/2013/nov/eu-usa-surveillance.htm>

NSA ‘monitored 60m Spanish calls in a month’:

<http://www.bbc.co.uk/news/world-us-canada-24699733?print=true>

US spy agency ‘monitored millions of French phones’

<http://www.france24.com/en/20131021-usa-spy-agency-nsa-recorded-millions-french-phone-calls>

[47] http://en.wikipedia.org/wiki/Five_Eyes

then passed to the UK, nor is there reference to PRISM and TEMPORA. As the Commissioner recognises himself:

“I am not appointed or authorised to oversee all of the activities of the intelligence agencies, only those specified in Section 57(2) of RIPA.” [48]

The Commissioner makes reference to the Intelligence and Security Committee (ISC) report, *Access to communications data by the intelligence and security Agencies*, published in February 2013 – prior to the Snowden revelations in June 2013 – but it is instructive to take a look at it before examining the Commissioner’s assertions as to the “lawfulness” of all GCHQ activities. [49]

First, in the ISC report the Home Office acknowledged that “the distinction between data and content, you can argue, is muddled in the Internet world.” (p.5)

Second, on filtering for “targets”:

*“[M]ost of GCHQ’s work is against **targets overseas**, it makes relatively few requests for CD [communications data] and CD is therefore used *** to help decide quickly, with minimal intrusion and cost, whether contacts of ‘subjects of interest’ are innocent and of no further interest, or are potential co-conspirators.” (***) in original, p.9)*

The reason much of GCHQ’s trawling is “overseas” is because:

*“A complete call or message between two individuals may involve **a large number of overseas CSPs and network providers... Overseas CSPs, especially those based outside the EU, may not be obliged to retain the CD of most relevance to the authorities.** Even if they hold the relevant data, they cannot be obliged to provide it to UK authorities, and may be unwilling to do so voluntarily.” (emphasis added, p.11)*

Third, there are new forms of communications which create “problems” for law enforcement agencies’ data-gathering, but the intelligence and security agencies (GCHQ, MI5 and MI6) “are able to work around the problem through the use of **other national security capabilities**” (emphasis added, p.13). This is presumably an oblique reference to the mass trawling of data from undersea fibre-optic cables and satellite interception. A footnote states: “We have not sought to detail these here.”

Fourth, the question is posed whether RIPA 2000 is fit for purpose:

“The Home Office, police, and the Agencies have explained that... the current legislation governing data retention does not cover many of the new forms of communication.” (p.11)

In slightly more detail:

[48] <http://www.iocco-uk.info/sections.asp?sectionID=8&chapter=4&type=top>

[49] The ISC report concerned the later-abandoned Communications Data Bill: <http://www.statewatch.org/news/2014/apr/uk-isc-access-communications-by-secint-agencies.pdf>

“[T]he existing legislation (RIPA) does not cover the problems of emerging technology, or provide the mechanism for asking overseas CSPs to retain CD.” (p14)

Fifth, what data do the intelligence and security agencies need and how do they get it?

*“[T]hree broad sets of data: IP address subscriber details; data identifying which internet services or websites are being accessed; and data from **overseas CSPs.**” (emphasis added, p.19)*

Under RIPA 2000, communications data can be formally requested from UK-based CSPs/ISPs, but because much of this data is passed to overseas based providers, GCHQ, MI5 and MI6 collect data en masse and then filter it using:

*“[V]ariations of... technology in their day-to-day business. GCHQ told us: We already use in GCHQ similar sorts of **technology that allow complex federated queries to be made from different data sources.**” (emphasis added, p22)*

With this official testimony in mind it is time to return to the Commissioner’s report.

2.4. Commissioner sets and answers his own questions

The Commissioner asks himself a number of questions, for example: do the agencies misuse their powers? He says “emphatically no”, because:

“The interception agencies do not engage in indiscriminate random mass intrusion by misusing their powers under RIPA 2000 Part I. It would be completely unlawful if they did.”

Time and again the “lawfulness” of the agencies’ practices under RIPA 2000 are emphasised, suggesting that, in many cases, it is the law itself which is the problem – just as it is in the USA.

He argues that one party may be innocent and another not, but unless all the information is gathered it is not possible to tell in advance which may be of interest “and which may not”. The Commissioner says that there have been:

“[R]umblings publicly expressed undertones that the interception agencies may be operating the section 8(4) interception procedures unlawfully or to the outer limits of legality, so as to produce disproportionate invasion or potential invasion of people’s privacy.” (p.58)

He concludes that “this is simply not so”. [50]

As to the role of governments:

“There is, in my judgment, no risk that the Government would or could require the interception agencies to undertake activity which would be unlawful under RIPA 2000 Part I. I ask the question only to dismiss it...” (p.59)

[50] The Commissioner has a single reservation the application of the section criteria for Section 8.4 certified warrants.

And the agencies themselves?

“Unlawful and unwarranted intercept intrusion of any kind, let alone “massive unwarranted surveillance”, is not and, in my judgment could not be carried out institutionally within the interception agencies themselves. The interception agencies and all their staff are quite well aware of the lawful limits of their powers. Any form of massive unwarranted intercept intrusion would as a minimum require a significant unlawful internal conspiracy which would never go undetected.” (p.59)

Can the public trust the agencies?

*“I am, however, personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals **or individuals who are potentially involved in actions which could raise national security issues for the UK** can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant.” (emphasis added, p.61)*

Such a conclusion quite simply flies in the face of the evidence used in this Analysis, as do the Commissioner’s answers to the following questions.

The crucial question the Commissioner sets himself is:

“Do British intelligence agencies receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK and vice versa and thereby circumvent domestic oversight regimes?” (p.62)

Essentially, the Commissioner says everything is OK because it is “lawful”.

It is worth citing in full. He says an intelligence agency in country A is allowed to “share intelligence” with an intelligence agency in country B if:

- i. the intelligence is lawfully acquired in country A; and*
- ii. it is lawful in country A for its intelligence agency to share the intelligence with the intelligence agency in country B.*
- iii. it is lawful in country B for its intelligence agency to receive the intelligence; and for good measure*
- iv. (iv) it would have been lawful for the intelligence agency in country B to acquire the intelligence in country B, if it had been available for lawful acquisition in that country.*

His response to “(i) and (ii) and generally” is that: “I have no expertise in US law and have not personally investigated so much of it as might be relevant. **I have however received appropriate assurances in this respect.**” (emphasis added)

By this logic, all intercepts carried out by the NSA under FISA on targets outside the USA from the rest of the world were “lawful” because the USA government said so. Similarly, all the intercepts and mass exchange of personal data between GCHQ and

the NSA and the other “Five Eyes” states was “lawful” because their governments said so. [51]

“As to (ii), if country A is the UK, I have had particular regard to section 15(2) of RIPA 2000 which strictly limits the lawful dissemination of intercept material to the minimum that is necessary for the authorised purposes.”

15(2) does indeed say that the use of intercepted material is “limited to the minimum that is necessary for the authorised purposes”. However, the Snowden revelations have shown that in this context the concepts of “minimum” and “necessary” have no limits. Indeed, RIPA 2000 itself sets out few limits. Under Section 15(3) the collection and use of intercept data is defined as anything “necessary for facilitating the carrying out of any of the functions under this Chapter of the Secretary of State”.

As argued above, Section 8.4 warrants are limitless. The concept of “necessary” is defined in Section 5.3 of RIPA in the following way:

“a warrant is necessary on grounds falling within this subsection if it is necessary -

“(a) in the interests of national security;

“(b) for the purpose of preventing or detecting serious crime;

*“(c) for the purpose of safeguarding the economic well-being of the United Kingdom; or for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any **international mutual assistance agreement.**”*

The concept of “necessary” thus defines itself in a way that is self-justifying.

With regard to point (iii) (“it is lawful in country B for its intelligence agency to receive the intelligence”), the Commissioner says:

“I know of no principle that an intelligence agency is disentitled from receiving intelligence information offered by a third party which a third party lawfully has, provided that its receipt is within the established statutory function of the intelligence agency, as to which see the Intelligence Services Act 1994. It happens all the time.” [52]

What about UK collusion with the CIA in rendition and the awareness of intelligence agencies of “inappropriate interrogation techniques” recorded by the Gibson Inquiry? [53] The inquiry stated that:

“Documents indicate that in some instances UK intelligence officers were aware of inappropriate interrogation techniques and mistreatment or

[51] The 1946 UKUSA Agreement soon led to the creation of the the “Five Eyes” who are: USA, UK, Canada, Australia and New Zealand; The “Nine Eyes” are the Five Eyes plus Denmark, France, the Netherlands and Norway and the “Fourteen Eyes”, are the same as the Nine Eyes plus Germany, Belgium, Italy, Spain and Sweden: http://en.wikipedia.org/wiki/UKUSA_Agreement

[52] Intelligence Services Act 1994: <http://www.legislation.gov.uk/ukpga/1994/13/contents>

[53] The Report of the Detainee Inquiry (2013):

<http://www.statewatch.org/news/2013/dec/uk-report-detainee-inquiry-rendition-dec-2013.pdf>

allegations of mistreatment of some detainees by liaison partners from other countries.

“Documents indicate that Government or its Agencies may have become inappropriately involved in some cases of rendition.”

And what about the 2005 security sweep across Greece, after the 7 July London bombings, which took place at the behest of MI6 – who supplied a list of named mobile phone users to the Public Order Ministry. 5,432 people were checked, 2,172 were “probed” and 1,221 were arrested for “other reasons”. 28 Pakistani men were abducted, held in secret houses, questioned and subjected to violence. [54]

The Commissioner’s response to point (iv) is that:

*“Information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available. If it is to be lawfully provided from abroad, it is sometimes appropriate for the interception agencies to apply explicitly **by analogy** the RIPA 2000 Part I principles of necessity and proportionality to its receipt here **even though RIPA 2000 Part I does not strictly apply**, because the interception did not take place in the UK by an UK agency. This is responsibly done in a number of appropriate circumstances by various of the agencies...”*
(emphasis added)

The notion that the mass surveillance and exchange of intercept data has been and is “proportionate” begs belief. As to necessity, see above.

3. Conclusion: State surveillance is as old as the state

The surveillance of communications by the UK state is as old as the state itself. The 1957 Birkett Committee report on the interception of communications sought to find a legal basis for the practice of telephone-tapping – a task that was to prove insoluble. [55]

Justification was sought for the age-old practice of mail opening by the state. In 1516, the monarchy created its own postal service which was later extended to private individuals. By Acts of 1657 and 1660 the Crown was given the right of monopoly over the postal service. The 1657 Act explicitly recognised that this was the best means to “Discover and prevent any dangerous and wicked Designs against the Commonwealth”.

Technology may have moved on from the days when it was the Post Office which opened mail and in those days carried out telephone-tapping too, but how little has really changed in the state’s targets? Historically, the state has always targeted spies and agents of foreign powers on the one hand and “subversives” who sought to change society on the other (the “internal enemy”) – both were, and are, seen as “threats” to “national security”.

[54] <http://www.statewatch.org/news/2006/jan/08greece-security-sweep.htm>

[55] Report of the Committee of Privy Councillors appointed to inquire into the interception of communications (1957) known as the Birkett Committee: <http://www.fipr.org/rip/Birkett.htm> and see Chapter 5 of Tony Bunyan, *The Political Police in Britain* (1977).

The “war on terrorism” initiated after 11 September 2001 made it justifiable for the state to pour vast resources into state surveillance technology at the same time that the control of multinational companies over communications data was growing massively – which they often share with the state. The dominant ideology was simply put:

"In this day and age if you've got the technology then it's vital to use that technology to track people down." [56]

With this sound-bite, former Prime Minister Tony Blair set out his own view which for generations has been the philosophy of the security and intelligence agencies. In the 1980s, BT, was able to list all the numbers called by a subscriber (the norm now, but not then) through ‘System X’, which made use of a printometer. BT supplied this information to law enforcement, intelligence and security agencies unbeknownst to the people or governments in the UK. [57] This was technologically possible but not lawful, and it was only made so thirty years later under RIPA 2000.

It was later revealed that not only were phone calls logged, itemised and passed over but that a new system, ISDN, allowed phones to be turned into “bugs” - listening devices spying on your living room. [58] Yet again the law only caught up under RIPA 2000 - it is now called “intrusive surveillance” and supplemented by microscopic listening devices.

Thus a lesson from the past is that state agencies – especially at the time of rapid technological advances – will use new surveillance, control and enforcement systems as they become available and let the law catch up later. At the same time, the agencies rely on useless systems of oversight and accountability to give them freedom of action and freedom from exposure (with some rare and notable exceptions). As a general rule, the exposure of state practices, such as the outrageous use of undercover police officers spying on protest movements, represents just the “tip of the iceberg” – most of their work remains hidden from public view.

The Snowden revelations are an exception to this general rule and represent a unique opportunity to bring about meaningful change, but only if we ask the right questions and act on them. Previous major revelations like those on the ECHELON surveillance system (also run by the “Five Eyes”) raised public consciousness but little changed. [59]

So what is to be done? Freedom from surveillance requires effective data protection and enforceable privacy rights. This means there can be no “compromises” when the EU negotiates with the USA: either the USA meets all of the standards in a new EU Data Protection Regulation or it does not – in which case there can be no agreement. But to be effective we have to look at the whole picture. This involves

[56] PM champions new DNA technology:

http://news.bbc.co.uk/1/hi/uk_politics/6075930.stm

[57] System X (telephony): http://en.wikipedia.org/wiki/System_X_%28telephony%29

[58] The new "System X": Statewatch database:

<http://database.statewatch.org/article.asp?aid=1524>

[59] European Parliament Echelon report (2001): <http://www.statewatch.org/news/2014/apr/ep-echelon-report.pdf> and Appraisal of Technologies of Political Control by Steve Wright:

<http://www.statewatch.org/news/2013/jul/KAT1.pdf>

looking at how surveillance data is used and against whom (the “targets”) and by whom (the “users”, the agencies). In the USA this is the CIA, FBI, and a plethora of other security and intelligence agencies and programmes. [60] In the EU, this is the internal security and intelligence agencies (SECINT), law enforcement agencies in the Member States and the EU institutions. Enforceable data protection and privacy are vital but are not the only issues. Nor does surveillance solely involve communications and the internet - it encompasses undercover policing, informers, digitised video “shots” of protestors and gathering personal data from other state agencies (like automatic car number plate recognition, tax and social security) and multinationals to add to the profiles of their targets. The agencies *use* the products of surveillance to effect social control and enforcement in defence of the status quo. Only when we take in this whole nexus can meaningful mechanisms for oversight and review and hence of accountability and legitimacy be set out for the UK and the EU. [61]

Finally, this examination of the annual report of the UK Interception of Telecommunication Commissioner tells us that:

1. UK law allows and legitimates “spying on the world” at home and abroad. The “lawfulness” of mass surveillance is thus part of the problem.
2. The Commissioner and his annual reports are quite inadequate to ensure meaningful oversight, review and accountability of interception and surveillance.
3. The CJEU has found the EU Directive on mandatory data retention – which the UK is signed up to - to be “unlawful”. This does not guarantee the law will be struck down – legal challenges have been launched but will take time to be resolved.
4. History teaches that secretive agencies and their governments do not simply abandon their practices. They will, unless fully exposed, tinker with the system to ensure that “normal service is resumed” as soon as possible.

May 2014

© Statewatch ISSN 1756-851X. Personal usage as private individuals/"fair dealing" is allowed. We also welcome links to material on our site. Usage by those working for organisations is allowed only if the organisation holds an appropriate licence from the relevant reprographic rights organisation (eg: Copyright Licensing Agency in the UK) with such usage being subject to the terms and conditions of that licence and to local copyright law.

[60] Monitoring America: Washington Post: “*there are 3,984 federal, state and local organizations working on domestic counterterrorism*”: <http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/print/>

[61] I will explore this strategy in greater detail in the forthcoming issue of the Statewatch Journal, “The EU and Uncle Sam” (June 2014).