Surveillance Activities Conducted by State Intelligence Agencies: Human Rights-Based Approaches to Intelligence Oversight

Eric King, Queen Mary University London

Companies

Expert bodies

Parliament

Intelligence Agencies

Whistleblowers

Courts

Media

Civil Society

Old UK oversight framework

Judicial

- Investigatory Powers Tribunal

Parliamentary

- Intelligence and Security Committee

Expert bodies

- Office of Surveillance Commissioner
- Intelligence Services Commissioner
- Interception of Communications Commissioners Office

+ Independent Reviewer of Terrorism Legislation

New UK oversight framework

Judicial

- Investigatory Powers Tribunal + domestic appeal

Parliamentary

- Intelligence and Security Committee

Expert bodies

- ~~Office of Surveillance Commissioner~~
- ~~Intelligence Services Commissioner~~
- ~~Interception of Communications Commissioners Office~~
- Investigatory Powers Commissioners's Office

+ Independent Reviewer of Terrorism Legislation

Avowals

Power	Avowal
Equipment Interference	Not avowed until the **February 2015** publication of the Equipment Interference Code of Practice. Government relies on warranty under s.5 and s.7 Intelligence Services Act 1994 and and Police Act 1997 to conduct Equipment Interference
Bulk Interception	It was not until the **March 2015** publication of the Intelligence and Security Committee's report earlier this year that Bulk Interception, including that of large international undersea cables, was avowed. The capability was authorised under s.8(4) Regulation of Investigatory Powers Act 2000.
Bulk Acquisition Warrants	It was not until **November 2015** that the Home Secretary herself avowed the fact that MI5 had been using the Telecommunications Act 1984 to collect domestic phone records in bulk.
Bulk Equipment Interferance	GCHQ maintains, in respect of ongoing litigation in the Investigatory Powers Tribunal, that Bulk Equipment Interference has **still not been avowed**. It claims however that if it had previously taken place, it would have been lawful to do so due to s.5 and s.7 Intelligence Services Act 1994.
Bulk Personal Datasets	It was not until the **March 2015** publication of the Intelligence and Security Committee's report earlier this year that the use of Bulk Personal Datasets was avowed.

Avowals

Power	Reference in A Question of Trust
Equipment Interference	Not yet avowed, referenced GreenNet case.
Bulk Interception	Addressed properly
Bulk Acquisition Warrants	Not yet avowed, Not mentioned
Bulk Equipment Interferance	Not yet avowed, Not mentioned
Bulk Personal Datasets	Not yet avowed, Not mentioned

- Bulk not mentioned in oversight reports until 2014/5.
- CNE/EI not mentioned in oversight reports until 2015/6

6.5.30 The circumstances in which a section 8(4) warrant may be issued are that:

- the communications to be intercepted are limited to *external communications* and their related communications data;
- external communications are communications sent or received outside the British Islands (section 20);
- the warrant may also comprise communications not identified in the warrant whose interception is necessary in order to do what the warrant expressly authorises (section 8(5));
- in addition to the warrant, the Secretary of State has to give a *certificate* describing certain of the intercepted material and certifying that the Secretary of State considers that the examination of this described material is necessary for one or more of the statutory purposes (section 8(4)b)), which are;
  - in the interests of national security,
  - for the purpose of preventing or detecting serious crime,
  - for the purpose of safeguarding the economic well-being of the United Kingdom.

Question of Concern

4.27 There is a question of concern I have raised in public as a possibility. It will require detailed examination which we are in the process of undertaking.

4.28 The communications data statistics given above are liable to be misleading. But taking the 514,608 number for Part I Chapter II authorisations and notices at face value, it seems to me to be a very large number. It has the feel of being too many. I have accordingly asked our inspectors to take a critical look at the constituents of this bulk to see if there might be a significant institutional overuse of the Part I Chapter II powers. This may apply in particular to police forces and law enforcement agencies who between them account for approaching 90% of the bulk.

1.2 My first aim is to fulfil my statutory obligation for 2013 to report annually to the Prime Minister. My second aim is to address, so far as I am able in a report to be laid before Parliament, public concerns relevant to my statutory function raised by media publications based on disclosures reportedly made during 2013 as a result of Edward Snowden's actions.

IOCCO 2013 report

Approaches to NCND

- Another major processing system by which GCHQ may collect communications is targeted at an even smaller number (just ***%) of the bearers that make up the internet (these are a subset of those accessed by the process just described). GCHQ apply *** 'selection rules' and, as a result, the processing system automatically discards the majority of the traffic that is carried across these bearers. The remainder – which GCHQ consider most likely to contain items of intelligence value – are collected (paragraphs 65–73).

...TEMPORA?

Parliamentary oversight

- Makes law! Approve budget [UK has Single Intelligence Account, but only created in 1950s]

- Intelligence and Security Committee
  - Looks at expenditure, administration, policy and operations
  - May request disclosure, but can be vetoed by secretary of state.
  - Reports provided to Prime Minister, who redacts
  - Does not have access to classified information received from foreign agencies

- Different models exist.
  - Belgian Monitoring Committee of the Chamber of Representatives oversees the expert bodies who oversee the agencies!
  - Swedish State Defence Intelligence Commission has power to stop on-going signals intelligence and subsequently order its destruction
  - German G10 committee can compel witnesses to appear in public and has used this for detailed information about how SIGINT technically operates.

Investigatory Powers Tribunal

- No standing requirements [although now must show there is a basis for ‘asserted belief’ post *HRW*]
- Claims brought from anywhere in world [although ‘present in UK’ jurisdiction test now applied post *HRW]*
- Operates using ‘assumed facts’ to protect NCND
- Has fact finding function, but doesn’t search ‘unanalysed material’ meaning accountability gap for bulk powers.
- No authority to compel disclosure of material. Never tested.
- No technical staff to advice, although can task IPCOand others.
- 2001-14; 1500 complaints, upheld 10.
- Only takes cases brought to it. Not proactive. Hasn’t accepted referrals.
- Considered competent (per *Kennedy*) although *10 Human Rights Orgs* challenging its compliance.

Account of the Data Handling Presentation to the IPT and the following discussion on Conduct and Service response to IPT complaints

1. ***Senior official*** (assisted by [REDACTION]) explained the nature and extent of the Service's data holdings, including the distinction between:

(a) **Service data generated on individuals in the course of Service investigations** – i.e. this includes people in respect of whom we have generated data whether or not they themselves are targets; and

(b) **reference data** – which consist of large datasets (i.e. our bulk data-sets) about the general population, and which help us to (i) identify targets from fragments of intelligence, and (ii) track their activities. ***The relevant teams*** used three practical examples (including an introduction to the ***analytical systems***) to demonstrate the benefit to national security provided by reference data and the steps we take to satisfy the tests of **necessity** and **proportionality**.

Proportionality?

- 19 RIPA s.(8)4 warrants ~ 50 billion communications daily
- 5 ISA s.5 warrants ~ 400,000 implants globally
- Watson + Schrems + Zakharov = no bulk collection?

Review of effectiveness

REPORT OF THE BULK POWERS REVIEW

by

DAVID ANDERSON Q.C.

Independent Reviewer of Terrorism Legislation

Presented to Parliament
by the Prime Minister
by Command of Her Majesty

August 2016

Cm 9326

Best practice?

- “There is no Council of Europe member state whose system of oversight comports with all the internationally or regionally recognised principles and good practices [...] and [...] there is no one best approach to organising a system of security service oversight.”
- Council of Europe Commissioner for Human Rights (2015), p. 7

Notification

- Likewise, the competent national authorities to whom access to the retained data has been granted **must notify the persons affected**, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.
  -- *Watson/Tele2*

Notification

- Strasbourg has long provided for for notification
  - *Klass and Others v Germany 1978:* "linked to this issue is the question of subsequent notification, since there is in principle **little scope for recourse to the courts by the individual concerned unless he is advised** of the measures taken without his knowledge and thus able retrospectively to challenge their legality."
  - *Weber and Saravia v Germany 2006:* **[A]s soon as notification can be carried out** without jeopardising the purpose of the restriction after the termination of the surveillance measure, **information should be provided to the persons concerned**."
  - *Szabo and Vissy v Hungary 2016***: Individuals should have a legal right to be notified** that they have been subjected to communications surveillance or that their communications data has been accessed by the State.

Notification

- Other countries provide for notification in statue
  - Sweden has default notification provisions, even for SIGINT, although not regularly used.
  - Denmark has a general obligation to inform the individuals at the end of surveillance
  - Romania requires notification if the collected data does not justify a referral to the criminal investigating authorities and does not justify a continuation of the surveillance.
  - US Wiretap Act requires notification once investigation closed.

Notification

- IPA 2016 doesn't provide for default notification.
- Doesn't provide for notification **even if error occurred results in breach of convention rights.**
  - Requires **'serious error'** (s.231(a)) to have occurred which 'caused **significant prejudice or harm** to the person concerned' (s.231(2)) and **'is in public interest** for person to be informed' (s.231(b))
  - Expressly states that **breach of convention rights is 'not sufficient by itself for an error to be a serious error'** (s.231(3))
  - Must have regard for whether **notification would be prejudicial to national security** et al (s.231(4)b(i)) and the 'continued discharge of the functions of any of the intelligence services (s.231(4)b(iv))

Role of media?

- Potentially getting more restrictive? [Law Commission Espionage Act]
  - Whistleblowers not afforded a public interest defence
- Judge what's in 'public interest' is challenging

Companies

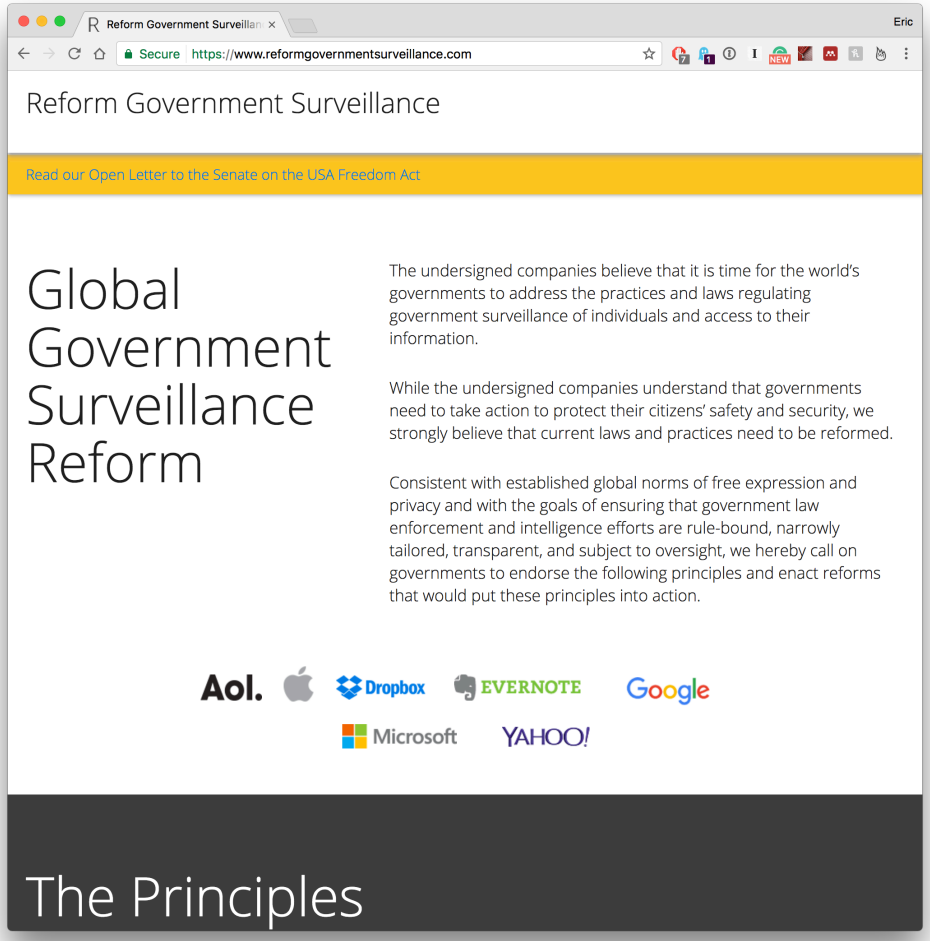
- Facebook, Google, Microsoft, BT, Vodafone all providing own transparency reports.
- Responsibility to challenge overly broad requests?

United Kingdom	Type of demand	
	Lawful Interception	Communications Data
Statistics	Vodafone disclosure unlawful (1) Government publishes (2)	Government publishes (2)
Key Note (1)	Section 19 of the Regulation of Investigatory Powers Act 2000 prohibits disclosing the existence of any lawful interception warrant and the existence of any requirement to provide assistance in relation to a warrant. This duty of secrecy extends to all matters relating to warranted lawful interception. Data relating to lawful interception warrants cannot be published. Accordingly, to publish aggregate statistics would be to disclose the existence of one or more lawful interception warrants.	
Key Note (2)	The Interception of Communications Commissioner's Office (pdf, 1.85 MB) publishes statistical information related to lawful interception and communications data demands issued by agencies and authorities.	
	For a summary of the most important legal powers relating to law enforcement demands on a country-by-country basis, see our Law enforcement legal powers country-by-country annexe (pdf, 1.84 MB).	

Detailed Data

Reporting Period	User Data Requests	Users/Accounts	Percentage of requests where some data produced
January to June 2015	**3,146**	**6,056**	**75%**
Legal Requests	2,844	4,690	73%
Emergency Disclosure Requests	302	1,366	92%
Preservation Requests	67	140	—
July to December 2014	**2,080**	**2,755**	**75%**
Legal Requests	1,890	2,403	73%
Emergency Disclosure Requests	190	352	94%
Preservation Requests	70	123	—

Companies



1

Limiting Governments' Authority to Collect Users' Information

Governments should codify sensible limitations on their ability to compel service providers to disclose user data that balance their need for the data in limited circumstances, users' reasonable privacy interests, and the impact on trust in the Internet. In addition, governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications.

Companies

- Difficult problems with competing standards
- How to manage different statistical requirements?

We also believe that governments should:

- balance national security and law enforcement objectives against the state's obligation to protect the human rights of all individuals;
- require all relevant agencies and authorities to submit to regular scrutiny by an independent authority empowered to make public – and remedy – any concerns identified;
- enhance accountability by informing those served with demands of the identity of the relevant official who authorised a demand and by providing a rapid and effective legal mechanism for operators and other companies to challenge an unlawful or disproportionate demand;
- amend legislation which enables agencies and authorities to access an operator's communications infrastructure without the knowledge and direct control of the operator, and take steps to discourage agencies and authorities from seeking direct access to an operator's communications infrastructure without a lawful mandate;
- seek to increase their citizens' understanding of the public protection activities undertaken on their behalf by communicating the scope and intent of the legal powers enabling agencies and authorities to access customer data; and
- publish regular updates of the aggregate number of law enforcement demands issued each year – meeting the proposed criteria we specify earlier in this report – or at the least allow operators to publish this information without risk of sanction and – as we also explain earlier – on the basis of an agreed cross-industry methodology.

Internal controls

- Ashley Deeks concept of ‘peer constraint’
- Appointment of Privacy and Civil Liberties Officers within US NSA
- Use of Integrity Protection Council at Swedish FRA
- Internal Compliance Team at GCHQ ex-post internal audit
- Belgian attempts to build privacy protections as functional goals inside engineering SIGINT team devleopment
- Publishing of reports by Croatian on national security developments.

Thanks!