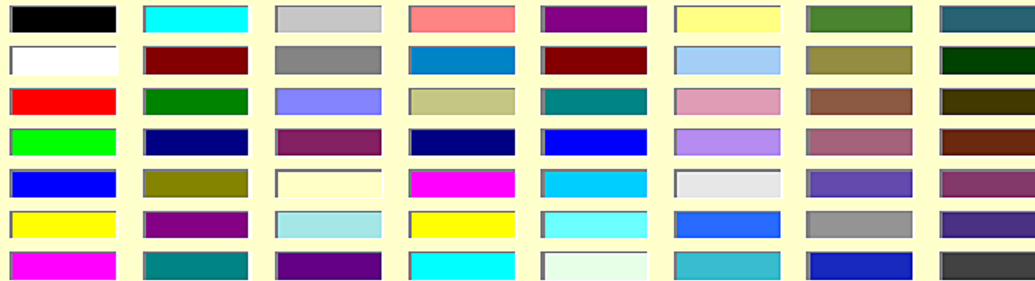


Operational Legalities



 – LA

 – OPP-LEG

Not for display

- Beware: there are several hidden slides in this presentation. If you see this you will also see the other hidden ones.
- To find which are hidden, use slide sorter view
- There's a print option to ignore hidden slides

a hidden slide

Agenda



Legal Framework

Tasking & Targeting
incl Location/Nationality

Coffee/tea

SD

Second Parties

Dissemination & Disclosure

Safeguards & Oversight

Wrap-up

What's OUT

Data Protection

Official Secrets

FOIA



Operational Legalities

Legal Framework

Legal Framework

Intelligence Services Act 1994

- functions; property interference; oversight

Human Rights Act 1998

- public authorities must act in accordance with ECHR

Regulation of Investigatory Powers Act 2000

- interception; safeguards; oversight

Wireless Telegraphy Act 2006

- non-RIPA interception/interference

Intelligence Services Act

- applies to all operations under control of Director GCHQ
- defines GCHQ's SIGINT function
- prescribes purposes for SIGINT function:
 - ... National Security
 - ... Economic Well-being of the UK (EWB)
 - ... Prevention/detection of serious crime

Human Rights Act 1998

- incorporates the ECHR into UK law
- requires all UK public authorities to act in accordance with the ECHR
- allows actions against public authorities by aggrieved parties
- RIPA, ISA and WTA are the vehicles through which ECHR or 'HRA compatibility' are met

The European Convention on Human Rights (ECHR)

Article 8 is of most obvious relevance to GCHQ:

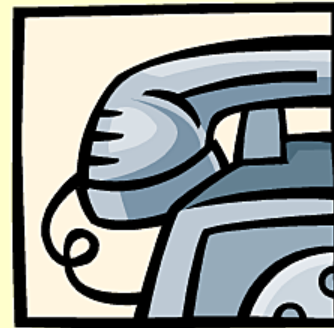
λ 8.1. *“Everyone has the right to respect for his private and family life, his home and his correspondence.”*

λ 8.2. *“There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law** and is **necessary in a democratic society...**”*



The European Convention on Human Rights

- “...in the interests of **national security**, public safety or the **economic well-being** of the country, for the **prevention of disorder or crime**, for the protection of public health and morals, or for the protection of the rights and freedoms of others.”



Need for authorisation

- ensures compliance with requirements of ECHR and HRA
- SIGINT – intercept/CNE – is illegal in UK without it (RIPA/CMA/WTA offences)
- gives visibility of operational activities – to GCHQ seniors & SoS

Authorisation

Regulation of Investigatory Powers Act 2000

Interception & surveillance

Intelligence Services Act 1994

CNE; Effects

Wireless Telegraphy Act 2006

**Interception/interference with wireless
telegraphy**

Regulation of Investigatory Powers Act 2000 (RIPA)

- λ interception in the UK of comms carried on a public or private telecommunications system
- λ surveillance & covert human intelligence source (CHIS) activity
- λ acquisition of comms data
- λ not just applicable to GCHQ

RIPA warrants

s. 8(4) 'external' warrants

- λ authorise 'at least one end foreign' interception
- λ authorise selection according to Certificate entries
- λ target must be outside the UK (absent additional authorisation)
- λ ensure individuals' ECHR rights are protected on a world-wide basis

RIPA warrants

s. 8(1) 'line-access' warrants

- λ warrant authorises **target** (person or premises) **in the UK**
- λ schedules give telecomms addresses
- λ schedules are served on those who can provide the communications (usually CSPs)
- λ PRESTON

RIPA warrants/certificates

- λ 6 months' duration for NS, 3 months for SC
- λ approval and renewal by Secretary of State
- λ can be modified – addresses, categories
- λ urgency provisions

ISA warrants & authorisation

- Computer Misuse Act 1990 (CMA)
- s.5 warrant necessary if target computer is in the British Islands (NS only)
- s.7 authorisation if elsewhere
- mimics RIPA warrantry
- s.7 subject to internal procedures

ISA warrants & authorisation

- 6 months' duration; NS/EWB only not SC for warrant but possible for authorisation
- approval and renewal by Secretary of State

λ no modification

λ urgency/operational effectiveness provisions

Wireless Telegraphy Act

- authorises interception of wireless telegraphy, ie that not covered by RIPA
- Secretary of State issues but without limit of time
- still needs to be proportionate

RIPA Directed Surveillance Authorisations

- GCHQ does directed surveillance when it observes a target with intention of gathering private data on the target's private life, associates and/or activities
- excludes historical research eg computer forensics

Questions?





Operational Legalities

Tasking and Targeting

Principles

1. We operate within the law
2. We can demonstrate that we operate within the law
3. Staff have the information they need to be able to comply with the law

All we do has to be:

- λ **authorised** – where necessary, under law (ISA, RIPA, WTA), or policy (STA/TTA)
- λ **necessary** – NS, EWB or SC; plus more specific intelligence requirements
- λ **proportionate** – manner and extent to which requirement is being met

What activities does that apply to?

tasking

access

targeting

retention

database queries

dissemination

TD

pioneering

SD

Tasking

- λ 'at least one-end foreign' interception is authorised by external RIPA 8(4) warrant
- λ selection is authorised according to Certificate entries
- λ ...ensures individuals' ECHR rights are protected on a world-wide basis

Targeting

- name
- communications addresses
- web service authentication data
- ID card number or passport number
- driving licence number
- car registration number
- bank card/credit card account numbers

BROAD OAK

- strategic target knowledge database
- users justify and review retention of target knowledge
- justification of targeting selectors – separate, but may be cascaded from target. Will be default in future iteration of BROAD OAK

TOP SECRET STRAP1 UK EYES ONLY



Home Search Targeting View Targeting Working Target

- Actions**
- Deactivate Selector
 - Take Ownership
 - Revalidate HRA
 - Show/Hide Previous Sites
 - Show/Hide HRA History

Hints

View the details of the deployment for a selector of a target. For currently targeted selectors the current and past deployments are shown in separate tables.

Click the link on the target's name to view the target for the selector.

Select **Deactivate Selector** to remove the selector from all sites at which it is deployed.

Select **Take Ownership** to seize ownership of this selector. You become responsible for maintaining the legality of targeting for this selector. Note that the existing owner is not informed.

Select **Revalidate HRA** to enter a new HRA justification for the selector.

Select **Show/Hide HRA History** to reveal or hide the HRA history.

View Selector Targeting URN: DCZL293

Selector Details

Type: Email Value: [redacted] Description: Business Email from Haustorium
 Source Reference: **HMRC Intelligence Report** Source Type: OGD Owner: [redacted]

Team Details: CP - Conventional Weapons Targeting Name: [redacted] Status: Targeted
 Content Keywords: [redacted]

Miranda No: **20109** JIC Priority/Purpose: **3NS** Sigint Dev:
 HRA Justification: **SUSPECTED OF PROCURING ARMS FROM IRAN IN CONTRAVENTION OF UN SANCTIONS** HRA Review By: 02/11/2008 HRA Revalidated By:

Legal Authorisation for Targeting: **GX/CP/10** Authorisation Expiry: 02/11/2008
 Warrant for Selector: Warrant Expiry: Legal Amplification:

Reason Off: Date Deactivated: Deactivated By:

Date Submitted: 15/05/2008 Last Updated By: [redacted] Last Updated Date: 15/05/2008
 Urgency: NONURGENT Collection Priority: 3
 ZIP: Cat: 5305
 Reg Country Digraph: GB City/PNAB: N/A

Targeting Protection Security Label: SECRET STRAP1 UK/US/CAN/AUS/NZ EYES ONLY

Current Selector Deployment

Name	SIGAB	PDG	Ownng Agency	Zip/Cat	Collection Priority	Submitted Date	Submitted By	Deactivated Date	Deactivated By
GCHQ C2C	UK-DICT	XX	NONE SUPPLIED	5305	3	25/07/2008	[redacted]		
STRONG_NET	MAN6	XX	NONE SUPPLIED	5305	3	23/05/2008	[redacted]		
SARDICT C2C	UKC-300	XX	NONE SUPPLIED	5305	3	15/05/2008	[redacted]		

Version 3.2.17 developed by Debia Limited 2008
 Served by weblogic host : TSAAppServer2

Source field - be specific

- ✓ GCHQ report ref and date
- ✓ SRI id and date
- ✓ call records including root number
- ✓ unique customer reference

ALWAYS INCLUDE A DATE

x e-mail from customer

x voice

x CRA

Intelligence requirements

- use MIRANDA number that equates to intelligence requirement
- TD - improving specific target knowledge, identifying new sources etc – is justified by the intelligence requirement for that target
- BOT - tick 'SigDevt' box

HRA justification

- explain exactly why you are targeting this individual
- don't just repeat the MIRANDA number but add value
- BOT - cascade of target-level HRA justification to selectors
- your responsibility to amend if necessary
- indirect targeting

HRA justification

- ✓ Russian Minister for Foreign affairs
- ✓ dialling analysis links to Senior Russian energy policymaker
- ✓ wife of Russian Minister, targeted to provide travel details of target
- ✓ Employee at Chinese Embassy in London
- ✓ Presidential Administration Experts Directorate; access to info on Russian policy affecting UK
- x Russian energy
- x Chinese weapons programme

Revalidating targeting

- make sure it is clear why you are continuing to invade this person's privacy, so:
 - record your justification for continuing targeting
 - make sure all fields contain the most recent information available
 - ongoing process
- if you can no longer justify targeting, record your reason for deactivating and then deactivate

Data content retrieval

UDAQ, DISHFIRE, IIB

- not all data in these bases is 'selected'
- retrieval must be:
 - authorised (lawful)
 - necessary
 - **proportionate**
- HRA screens; audit logs
- target in UK – datamining STA

SECRET UK Eyes Only



SOURCE

Intercept | Opensource

Recovery_Intercept Farndale_Kesse Farndale_C2C

Select All Deselect All

PROPERTIES

Query Type: **Transient**

Query Name: [redacted]

Description: [redacted]

Classification:

Unclassified	NZ	STRAP
Restricted	AUS	NOCON
Confidential	CAN	KESSE CARBOY
Secret	UK	KESSE SOUNDER
Top Secret	US	KESSE SCAPEL

SEARCH TERMS

Match: Content Operator: All OF Automatically adds AND between all terms entered

FreeText: [redacted] Add To Query: AND OR NOT

HRA JUSTIFICATION

* Miranda: No --select-- JIC priority

* Purpose: [redacted] [Legal Guidance](#)

* Justification: [redacted]

Description: [redacted]

Expiry Date: [redacted] TD

Structured View | Freeform View

Currently a hidden slide

Toggle Nat | Clear | Group | Undo | Clear All

QUERY EXECUTION

Count Only

Results. Limit to approx items (Max 1000)

Schedule: None

Notify On Completion

Save Save As Search

UFAQ

- λ JIC purpose
- λ use appropriate MIRANDA number
- λ explain why you are running this query
- λ principle applies to use of any Sigint database

Currently a hidden slide

Questions you should ask yourself

- would my justification record be clear to a colleague?
- have I justified invading this person's privacy?
- will my successor understand?

Audits

- IPTs currently carry out targeting audit
 - 10% of entries each year, randomly chosen
 - all UK entries each year, wildcards each audit
- quick check of record & key HRA aspects:
 - source field
 - HRA justification
 - MIRANDA number
 - revalidation
- UDAQ & Events also audited

Questions?





Operational Legalities

Targeting: location and nationality

Location, location, location

- λ Law: specific RIPA authorisation for interception of a target located in the UK
- λ Policy: internal authorisation (STA) for a target outside the UK if nationality and/or location is sensitive
- λ all targets require HRA justification (GCHQ is a public authority interfering with individuals' human rights)





Location?

- without other information, assume:
 - individual is in their country
 - mobile phone is in country of registration
 - email address with country digraph is there

Location: belief & knowledge

- λ belief is not 100% knowledge with hindsight; you must not 'turn a blind eye'
- λ based on the information available at any particular time
- λ this may vary - so should our response



Target arrives or is discovered to be in the UK...what next?

Consider authorisation options

- λ continuation targeting – RIPA s.16(5)
 - λ 5 working days (1 for SC)
 - λ signed by GCHQ Directorate
- λ then over to customer – RIPA s.8(1) warrant or...



Target in the UK...RIPA s.16(3)

- λ frequent visitors to the UK or known targets
- λ SoS signature required – modification to 8(4) certificate
- λ new selectors may be used
- λ ***indirect targeting is not allowed***



If no authorisation is sought...

- λ examine and report traffic intercepted up to time you knew target was in UK*then....*
- λ use B3M HRA 'register' to alert
- λ check location using events or THUGGEE
- λ examine a cut (B3M / UDAQ) every 48 hrs to check whereabouts



Policy authorisations

- STA and TTA provide records of actions where UK &/or British Overseas Territory law does not require authorisation
- respect 2nd Party sensitivities
- actions are validated by a GCHQ senior (or nominated GC8s in ITT)
- we can justify targeting if challenged
- QC is mandatory



Datamining STA

- Datamining STA for target in UK – valid for two days
 - named SCS officer signs STA
 - one-off search
- Count-only searches: no authorisation needed

Special C2C authorisations

- special access to email communications
- NS only; limited criteria
- 16(3) or STA also required if location or nationality sensitive
- SCS or GC6 approval

SRA

- authorises receipt of 2 or 3P intelligence on UK-based targets ...
- ... where GCHQ has no authorisation
- avoids indirect targeting
- limited period only



Operational Legalities

SIGINT Development

SD justification

- Enhancing GCHQ's capabilities is a national security purpose
- TD – improving specific target knowledge, identifying new sources etc – is justified by the intelligence requirement for that target

SD proportionality

Restrict to the minimum necessary:

- refine wide initial terms
- define length of task and/or volumes
- limit dissemination and retention

Aim: sustained targeting as soon as practicable

SD reporting

- you may report from SD traffic
- reporting guidelines reflect HRA requirements

Content or metadata?

- voice mail boxes
- SMS text
- an email inside a message
- email subject line
- URL beyond the domain name
(eg <http://www.myrail.com/query-text>)
- an attached routing diagram

Content or **metadata**?

- IP address
- email address
- DTMF (tone dialling)
- a URL up to the domain

(eg <http://www.myrail.com/>)

- location

Content or metadata?

- password

authentication to a communications service –
communications data

other passwords – content

- cookie

depends on data – may be either

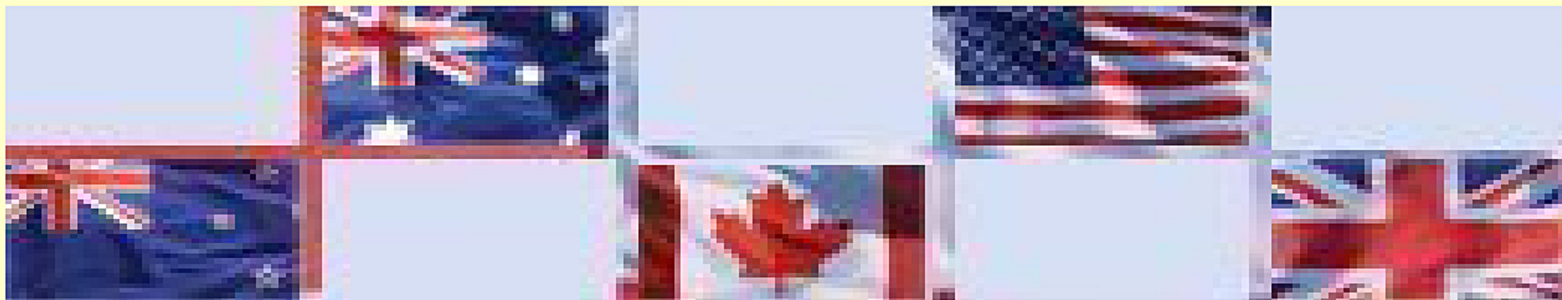
Questions?





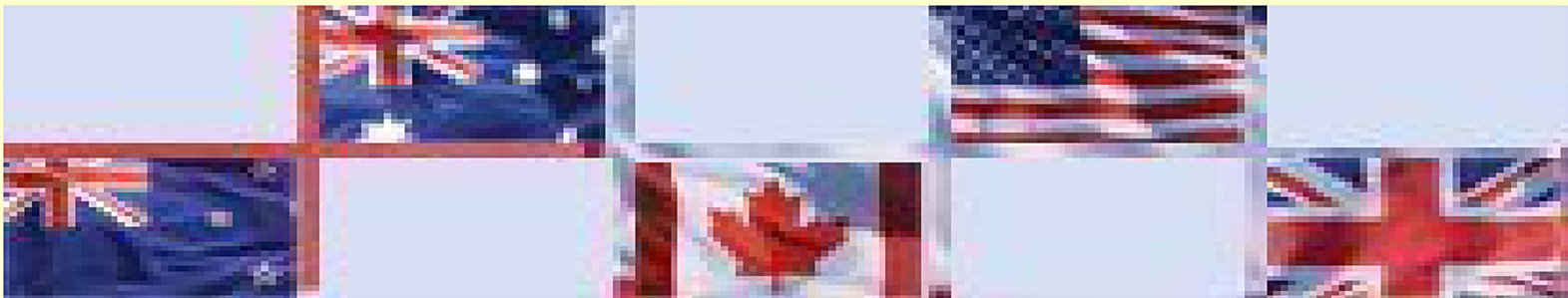
Second Parties

Australia, Canada,
New Zealand & USA



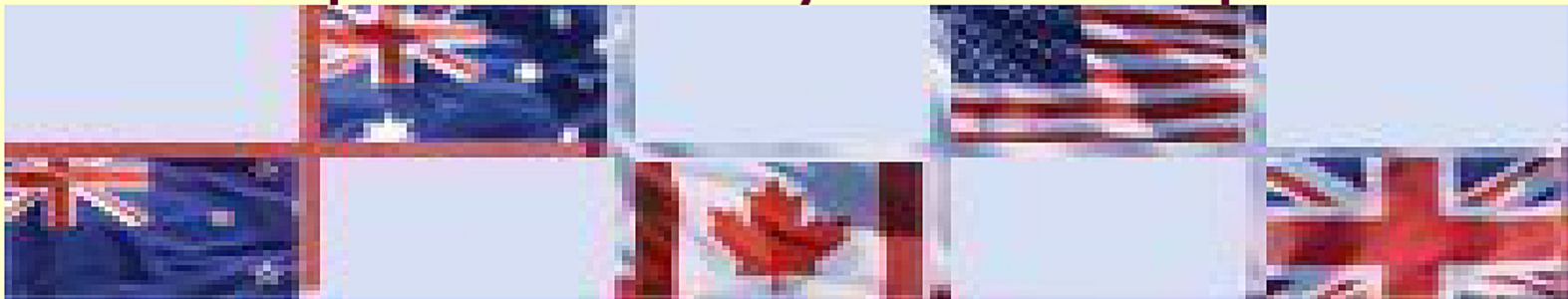
GCHQ and Second Parties

- partners respect each others' laws and policies
 - 2nd parties treat UK nationals as their own
- GCHQ must not ask a 2nd party to do something for which we would need a warrant
- we must not task a 2nd party with targeting that would be unlawful in that country



USSID SP0018

- No interception of persons in US without a warrant
- Court order needed to intercept US persons outside the USA
- your use of NSA collection & databases must respect 2nd Party laws and policies





Operational Legalities

Dissemination & Disclosure

Dissemination

- λ EP is sole vehicle for passing intelligence to customers
- λ Reporting Standards applies proportionality principle to EP

Disclosure

- λ SIGINT collected under RIPA may not be used in court
- λ Relevance to prosecutions
- λ Public Interest Immunity – PII certificates

Questions?








Operational Legalities

Safeguards and Oversight

RIPA safeguards

- λ intercepted material must be destroyed as soon as its retention is no longer necessary...
- λ it must be looked at, copied and disseminated to the minimum necessary...
- λ ...for a purpose authorised under the Act
- λ as a matter of policy, GCHQ applies this ethos to all material it acquires, regardless of source
- λ policies for EP and data retention

Errors and breaches

- λ mistakes happen and we report them
- λ OPP-LEG and LA role: help & advice
- λ an apparent error may be:
 - λ breaking the law 
 - λ a breach of RIPA safeguards 
 - λ nothing to worry about! 
- λ response: procedures, processes & training

Political oversight

- λ **Executive** - a Secretary of State exercises authority over the I & S services and is answerable to Parliament
- λ **Parliament - Intelligence & Security Committee** examines expenditure, administration and policy (not operations); members within the circle of secrecy; reports annually to Parliament

Judicial oversight: Commissioners

- λ **Senior Judges:** independent of HMG and Parliament
- λ **review** Secretary of State's use of powers under RIPA/ISA
- λ **guaranteed access** to agencies
- λ **annual reports** to the Prime Minister

Investigatory Powers Tribunal (IPT)

- comprises 8 independent lawyers
- investigates complaints against Agencies, law enforcement etc
- anyone, anywhere may complain
- more than 40 people within GCHQ assist in responding to complaint; audit logs

The Tribunal will ask...

- what did we do?
- was the action **authorised**?
- was it **necessary**?
- was it **proportionate**?
- did GCHQ act reasonably & within its powers?



Operational Legalities

Wrap up

Key points: 'GCHQ does it legally'

1. Your work must be:

- authorised
- necessary
- proportionate

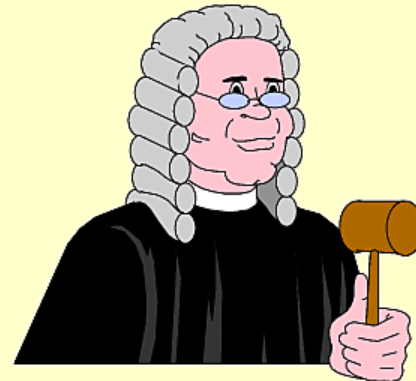


2. Location:

beware UK & UKUSA
– seek authorisation

3. Errors: we are
honest and report them

Currently a hidden slide



What does this mean for me?

- Collection/technical staff: know what you can and cannot intercept
- Collection manager: help analysts ensure selectors are justified and proportionate
- Analyst/linguist: justify your targeting, seek warrant or STA where necessary
- Reporter: report only what is necessary to address the requirement

Currently a hidden slide

Contacts

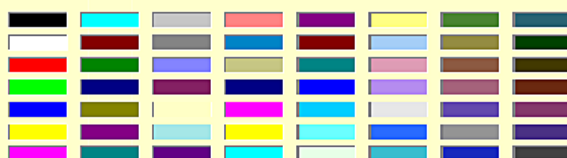
- visit OPP-LEG in B4a
- call RUSSETT 36559
- email [REDACTED]@gchq
- OPP-LEG web pages & compliance website
- speak to your Legal POC.....

Legal & Policy Leads

- AP – [REDACTED]
- BROK – [REDACTED], [REDACTED]
- CP – [REDACTED]
- DIG – [REDACTED]
- GSOC – [REDACTED]
- ITT – [REDACTED], [REDACTED]
[REDACTED], [REDACTED]
- LANG – [REDACTED]
- MENA – [REDACTED], [REDACTED]
[REDACTED]
- RCIT – [REDACTED]
- SC – [REDACTED]
- TSI – [REDACTED]
- W – [REDACTED]
- ACD - [REDACTED], [REDACTED]
[REDACTED]
- ICTR – [REDACTED]
- OPC-CNE [REDACTED], [REDACTED]
[REDACTED]
- JTRIG – [REDACTED]
- NAC – [REDACTED]
- GTAC - [REDACTED]
- GTE - [REDACTED]
- CRFC – [REDACTED]
- Geo – [REDACTED]
- Bude – [REDACTED]

Questions?

Operational Legalities



██████████ – LA

██████████ – OPP-LEG

Protective marking of these notes: **SECRET STRAP1**

Protective marking of slides: **UNCLASSIFIED + CORINTH**

Intro; welcome; aims – legal framework and how to apply this in day-to-day work

GCHQ operates within the law; everyone's responsibility; but we're here to help

Training is part of that

But we also:

- Offer advice (desk, legal inbox, etc) – aim for prompt service; lawyers always on hand as well;
- Deal with warrantry and disclosure
- Help shape new tools and applications
- Develop new policy as new requirements emerge, esp. with new techniques, accesses etc that analysts want to exploit

Our job is to enable Sigint: we have processes that enable us to do things that would be illegal to the man on the street

But with that comes responsibilities.

Not for display

- Beware: there are several hidden slides in this presentation. If you see this you will also see the other hidden ones.
- To find which are hidden, use slide sorter view
- There's a print option to ignore hidden slides

a hidden slide

Agenda



Legal Framework

Tasking & Targeting
incl Location/Nationality

Coffee/tea

SD

Second Parties

Dissemination & Disclosure

Safeguards & Oversight

Wrap-up

What's OUT

Data Protection

Official Secrets

FOIA

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

Structure

Blue = lawyer, green = OPP-LEG-er (red = audience)

30-minute brief intro to legal framework - lawyer

30 minutes on how this is applied to tasking and targeting – OPP-LEG

15 minutes coffee-tea break when you can pick up and read quiz sheets

15 minutes on SD and Second Parties – OPP-LEG

15 minutes in groups to consider quiz

15 minutes led discussion on quiz questions

15 minutes on legal safeguards and oversight

15 minutes for wrap-up and further questions

Handouts on targeting and feedback sheet at the end

Reporting governed by same principles as targeting so covered in general terms, but IPOL do the detailed guidance

Happy to take questions as we go along but if they're on other areas please leave to the the end so we can be sure we've covered the main material first. Ask about jargon!!



Operational Legalities

Legal Framework

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Legal Framework

Intelligence Services Act 1994

- functions; property interference; oversight

Human Rights Act 1998

- public authorities must act in accordance with ECHR

Regulation of Investigatory Powers Act 2000

- interception; safeguards; oversight

Wireless Telegraphy Act 2006

- non-RIPA interception/interference

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] x [redacted] or [redacted]@gchq.gsi.gov.uk

- This is the legal framework that affect GCHQ Sigint operations and sets out the 3 main Acts.

- **ISA** - governs the functions of GCHQ

- **HRA** - helps protect people's privacy in general NOT just their communications eg people round Heathrow's new terminal feel their privacy is being violated

- it gained Royal Assent in 1998 but didn't come into effect until 2 October 2000 when RIPA was set up.

- **RIPA** is the mechanism we use by which we make it ok to carry out interception

- **WTA** covers interception of any wireless telegraphy not covered by RIPA

Background:

- HRA was a manifesto commitment of the new labour govt in 1997 to allow people under ECHR to pursue a case through the UK courts if grievance claim that their HR have been interfered with, rather than taking it to Strasbourg
- Royal assent - act on statute books - signed by Queen
- RIPA 2000 covered for interception and surveillance – comms data provided for 5 January 2004

Intelligence Services Act

- applies to all operations under control of Director GCHQ
- defines GCHQ's SIGINT function
- prescribes purposes for SIGINT function:
 - ... National Security
 - ... Economic Well-being of the UK (EWB)
 - ... Prevention/detection of serious crime

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Until 1994, GCHQ and SIS did not have an act in law to define their function.

BSS have the Security Services Act; ISA followed this.

Definition: to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material

Advice and assistance about languages (GLASS); and cryptography

Broad – covers passive collection; now also covers computer network exploitation; rare to find something that it doesn't cover. BUT Act does closely prescribe **purposes** for which GCHQ can exercise this function. **3 purposes.** Jonny stealing a Mars Bar example!

We are driven by customer requirements and need to make sure that what we are asked to do falls within these 3 categories

(SC has four definitions, defined under RIPA).

This is the **hard law**; it's the basic starting point; once we have established that work meets this, move onto other considerations.

Human Rights Act 1998

- incorporates the ECHR into UK law
- requires all UK public authorities to act in accordance with the ECHR
- allows actions against public authorities by aggrieved parties
- RIPA, ISA and WTA are the vehicles through which ECHR or 'HRA compatibility' are met

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk

ECHR: post WW2, nations combined to ensure atrocities didn't happen again

- as a public authority it is unlawful for GCHQ to act in a way which is incompatible with a convention right
- Public authorities are of 3 types:
 - government depts/health authorities/armed forces/police (NOT parliament)
 - courts and tribunals
 - person/org carrying out functions of public nature (eg Railtrack when acting as safety regulator but not as commercial property developer)
- Some are **absolute**: eg. right to life, to protection from torture, inhuman and degrading treatment and punishment
- Some are **limited** eg. the right to liberty (unless you commit an offence) and to a fair trial can be limited under explicit and finite circumstances defined in the Convention itself.
- Others are

Term HRA will be known to many of you if you target, use Corinth – easy to forget that this is part of UK law

The European Convention on Human Rights (ECHR)

Article 8 is of most obvious relevance to GCHQ:

- λ 8.1. “Everyone has the right to respect for his private and family life, his home and his correspondence.”
- λ 8.2. “There shall be no interference by a public authority with the exercise of this right except such as is **in accordance with the law** and is **necessary in a democratic society...**”



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA requests to GCHQ via [redacted] or [redacted]@gchq.gsi.gov.uk

Obvious why relevant to GCHQ – examining forms of intercept; very intrusive.

e.g. Heathrow night flights; partially successful.

8.2 is key – right to privacy is not absolute. Public authorities may interfere with this if certain conditions are met.

Brings concept of **proportionality** into UK law for first time. **Ends must justify means**; Sigint as last resort.

The European Convention on Human Rights

- “...in the interests of **national security**, public safety or the **economic well-being** of the country, for the **prevention of disorder or crime**, for the protection of public health and morals, or for the protection of the rights and freedoms of others.”



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

'Just' 3 at the moment. No reason why GCHQ's remit could not be changed in future but this is what we are allowed to do at the moment.

Need for authorisation

- ensures compliance with requirements of ECHR and HRA
- SIGINT – intercept/CNE – is illegal in UK without it (RIPA/CMA/WTA offences)
- gives visibility of operational activities – to GCHQ seniors & SoS

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

1. Hard reason – criminal offence. Give example of journalist recently jailed.

Civil servants are not immune from prosecution.

2. Soft reason. Means that someone, usually SoS, makes a judgement of proportionality and necessity.

3. Policy.

Authorisation

Regulation of Investigatory Powers Act 2000

Interception & surveillance

Intelligence Services Act 1994

CNE; Effects

Wireless Telegraphy Act 2006

Interception/interference with wireless telegraphy

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

(Other considerations e.g. oversight) but this is what each one authorises.

More detail on RIPA and ISA to follow

Surveillance – for GCHQ, tends to be electronic surveillance (JTRIG) although covers more 'traditional' forms of surveillance

WTA – e.g. police broadcasts

Regulation of Investigatory Powers Act 2000 (RIPA)

- λ interception in the UK of comms carried on a public or private telecommunications system
- λ surveillance & covert human intelligence source (CHIS) activity
- λ acquisition of comms data
- λ not just applicable to GCHQ

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] x [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

•RIPA -

- provides for interception and surveillance by public authorities since HRA came into force
- It focuses on rights of individuals located in the UK (regardless of nationality) and provides for warrants to be issued to authorise interception of comms (including comms outside UK)
- Point 2 – GCHQ could do this in law but hasn't to date; Joint Section work with SIS; covered by their warrants.
- Point 3 – covers data direct from CSPs
- Also police, fraud office, anyone carrying out intercept

RIPA warrants

s. 8(4) 'external' warrants

- λ authorise 'at least one end foreign' interception
- λ authorise selection according to Certificate entries
- λ target must be outside the UK (absent additional authorisation)
- λ ensure individuals' ECHR rights are protected on a world-wide basis

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

[Pass round copy of certificate - later]

Mention SD and DefMon are covered

We have 10 – one 'global' that covers Bude, MHS, Cyprus

-others for special source accesses

Selection of material governed by Certificate, specifying general categories of material, rather than a specific individual/selectors. Categories broadly mirror JIC requirements.

Slide 4 – individual's rights protected on world-wide basis; also allows for anyone anywhere in the world to complain about our actions; means we can demonstrate to Tribunal that we have acted lawfully.

RIPA warrants

s. 8(1) 'line-access' warrants

- λ warrant authorises **target** (person or premises) **in the UK**
- λ schedules give telecomms addresses
- λ schedules are served on those who can provide the communications (usually CSPs)
- λ PRESTON

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

RIPA makes no distinction based on nationality (cf. 2Ps); there'll be a slide on this later.

The address can be a tel no or an email address ; warrant signed by SoF but

Schedules can be modified by WLD (Whitehall liaison department) or by a Director in an emergency

GCHQ – all current warrants are against premises rather than individuals because of demarcation of responsibilities (us: foreign intel; BSS – internal UK – although we may do intercept for them)

GCHQ – must have schedule served on it to target selectors on our external warrant; see error report in legal inbox 26/10/2007.

Expand CSPs if not mentioned already – once served by a schedule, have to comply with it (law). GCHQ can also be served by schedules. GCHQ therefore insists on seeing copies of warrant schedules before taking action because of previous muck-ups which have had to be reported to the Commissioner. Involves simple, well-established comms process between OPP~LEG and SS warrantry team.

Say: No schedule No targeting!

RIPA warrants/certificates

- λ 6 months' duration for NS, 3 months for SC
- λ approval and renewal by Secretary of State
- λ can be modified – addresses, categories
- λ urgency provisions

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Urgency:

-GCHQ senior official (on list) may sign:

- urgent 8(1) warrant if expressly authorised by SoS
- 8(1) schedule modification
- 16(3) urgent modification

ISA warrants & authorisation

- Computer Misuse Act 1990 (CMA)
- s.5 warrant necessary if target computer is in the British Islands (NS only)
- s.7 authorisation if elsewhere
- mimics RIPA warrantry
- s.7 subject to internal procedures

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

1. Criminal offence to interfere with someone's computer unless properly authorised.

Viewed seriously in the UK; possible jail terms due to increase to between 5-10 years.

2. Signed by SoS.

3. Signed by SoS but individual operations signed by DO, allows CNE more flexibility.

ISA warrants & authorisation

- 6 months' duration; NS/EWB only not SC for warrant but possible for authorisation
- approval and renewal by Secretary of State

λ no modification

λ urgency/operational effectiveness provisions

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Urgency:

- GCHQ senior official (on list) may sign:
 - Urgent s.5 warrant to do something already authorised abroad under a s.7 authorisation
 - 5-day grace extension when machine enters UK

Wireless Telegraphy Act

- authorises interception of wireless telegraphy, ie that not covered by RIPA
- Secretary of State issues but without limit of time
- still needs to be proportionate

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

RIPA Directed Surveillance Authorisations

- GCHQ does directed surveillance when it observes a target with intention of gathering private data on the target's private life, associates and/or activities
- excludes historical research eg computer forensics

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Signed internally

JTRIG including JEDI pods

Passive internet monitoring

Questions?



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk



Operational Legalities

Tasking and Targeting

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk

So you've heard about the principal laws that affect our work. So the next part is what that means to us in practice.

Principles

1. We operate within the law
2. We can demonstrate that we operate within the law
3. Staff have the information they need to be able to comply with the law

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

All we do has to be:

- λ **authorised** – where necessary, under law (ISA, RIPA, WTA), or policy (STA/TTA)
- λ **necessary** – NS, EWB or SC; plus more specific intelligence requirements
- λ **proportionate** – manner and extent to which requirement is being met

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Some fields in Corinth/UDAQ (and others in due course) are there for legal compliance reasons. Not a 'nice-to-have'. Used by OPP~LEG to audit actions.

Proportionate – often the most challenging. **Given the aim, the conduct proposed is reasonable.**

What activities does that apply to?

tasking

access

targeting

retention

database queries

dissemination

TD

pioneering

SD

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk

Tasking

- λ 'at least one-end foreign' interception is authorised by external RIPA 8(4) warrant
- λ selection is authorised according to Certificate entries
- λ ...ensures individuals' ECHR rights are protected on a world-wide basis

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Pass round copy of certificate – NB 'eyes' marking

Mention SD and DefMon are covered

We have about ten – one 'global' that covers Bude, MHS, Cyprus

-others for special source accesses

-Renewal every 6 months – you might have been asked for highlights

-Certificate entries refine Intelligence topics

-New entries can be made e.g. Electronic Attack

Targeting

- name
- communications addresses
- web service authentication data
- ID card number or passport number
- driving licence number
- car registration number
- bank card/credit card account numbers

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Any of these terms are referable to an individual so need to follow the A, N, P rule.

BROAD OAK

- strategic target knowledge database
- users justify and review retention of target knowledge
- justification of targeting selectors – separate, but may be cascaded from target. Will be default in future iteration of BROAD OAK

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Storage of TK not quite so sensitive/intrusive but still need to justify.

BOT will replace Corinth (Release 4, Mar 09).

The screenshot shows a web-based interface for 'Targeting'. The main content area is titled 'View Selection Targeting'. It contains several sections:

- Source:** HMIC Intelligence Report (circled in red)
- Friends:** SUSSEX (circled in red)
- HRA Justification:** SUSPECTED OF PROSECUTING JERMS FROM STATE BY CONTRAVENTION OF UN SANCTIONS (circled in red)
- Legalisation for Targeting:** WARRANT (circled in red)
- Authorisation:** WARRANT (circled in red)

At the bottom, there is a table titled 'Common Selection Deployment':

Name	ID	Type	Priority	Collection Points	Scheduled Date	Submitted By	Targeting Type	Declassified By
GDHQ-COC	UK-ESCT	CC	SOME SUPPLIED	0305	3	25/05/2008		
SPR-SAS_RPT	HMIC	CC	SOME SUPPLIED	0308	3	25/05/2008		
SPRDET-COC	UK-ESCT	CC	SOME SUPPLIED	0305	3	25/05/2008		

At the bottom of the page, there is a disclaimer: 'This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ECHQ on [redacted] or [redacted]@cchq.gov.uk'

Show the fields that are there for legal compliance reasons:

- Source
- MIRANDA number
- JIC purpose (in this case 3 NS)
- HRA Justification
- Authorisation: in this case a Warrant number cos target in UK

Source field - be specific

- ✓ GCHQ report ref and date
- ✓ SRI id and date
- ✓ call records including root number
- ✓ unique customer reference

ALWAYS INCLUDE A DATE

- x e-mail from customer
- x voice
- x CRA

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Needs to be traceable as well as specific

Intelligence requirements

- use MIRANDA number that equates to intelligence requirement
- TD - improving specific target knowledge, identifying new sources etc – is justified by the intelligence requirement for that target
- BOT - tick 'SigDev't' box

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Address indirect targeting issues; will come onto UK issues

HRA justification

- explain exactly why you are targeting this individual
- don't just repeat the MIRANDA number but add value
- BOT - cascade of target-level HRA justification to selectors
- your responsibility to amend if necessary
- indirect targeting

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Address indirect targeting issues; will come onto UK issues

Indirect targeting – the use of a selector to identify and select the communications of one individual with a view to selecting and reporting the activities of another individual – the target; such targeting requires an authorisation appropriate to the location and nationality of the real target

Indirect targeting is getting sustained intelligence on A by targeting B. (Wanting intelligence on B as well doesn't get you off the hook.)

Point to note: it is using another selector to get at the **communications of the target**, not to find **information about him**. So it is fine to target a Swedish girl-friend of a person in the UK to find out info about him, as long as you defeat communications between the two of them.

HRA justification

- ✓ Russian Minister for Foreign affairs
- ✓ dialling analysis links to Senior Russian energy policymaker
- ✓ wife of Russian Minister, targeted to provide travel details of target
- ✓ Employee at Chinese Embassy in London
- ✓ Presidential Administration Experts Directorate; access to info on Russian policy affecting UK
- x Russian energy
- x Chinese weapons programme

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

All about proportionality

I hid two lines at the foot of this slide (reset font colour) – not sure I can justify rejecting them! [REDACTED]

We could do with some non-ITT examples

suspected terrorist temporarily removed

Revalidating targeting

- make sure it is clear why you are continuing to invade this person's privacy, so:
 - record your justification for continuing targeting
 - make sure all fields contain the most recent information available
 - ongoing process
- if you can no longer justify targeting, record your reason for deactivating and then deactivate

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Revalidation – new requirement in BOT; it will be audited

Data content retrieval

UDAQ, DISHFIRE, IIB

- not all data in these bases is 'selected'
- retrieval must be:
 - authorised (lawful)
 - necessary
 - **proportionate**
- HRA screens; audit logs
- target in UK – datamining STA

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Basis: data from authorised intercept, normally selected using a TND but scope could include some unselected data, eg from a survey

Includes UDAQ (mixed), SAMDYCE (selected), DISHFIRE (mixed), MAMBOOKIE (selected)

Issue: database users run queries and have potential to infringe human rights of innocent people through reading their communications

Normal A – J – P implemented by the analyst

Hence HRA screen

Also logging of queries for audit and queries (more later)

Querying is a form of targeting – hence STA requirement

UDAQ - New Query - Microsoft Internet Explorer provided by ECHQ

SECRET UK Eyes Only

UDAQ

SCWeb | GCSearch | Print Book

Home | New Query | Manager | Preferences | Help

SOURCE

Intercept | OpenSource

Recovery_Intercept Parndale_Resse Parndale_C2C

SEARCH TERMS

Match: Content Operator: All of Automatically adds AND between all terms entered

FreeText:

Structured View | Freeform View

PROPERTIES

Query Type: **Transient**

Query Name:

Description:

Classification:

Unclassified	NC	STRAP
Restricted	AUS	NOCON
Confidential	CAN	WESSE CARBOY
Secret	UK	WESSE SOUNDER
Top Secret	US	WESSE SCAPLE

HRA JUSTIFICATION

* Mandate: **No** IC priority

* Purpose: [Legal Substans](#)

* Justification:

Description:

Expiry Date: TD

QUERY EXECUTION

Count Only

R: Results: Limit to approx. items (Max: 1000)

Schedule: None

Notify On Completion

Currently a hidden slide

To comply with a request under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ECHQ on [redacted] or [redacted] by email on [redacted]

6 Lock Assistant

UDAQ

- λ JIC purpose
- λ use appropriate MIRANDA number
- λ explain why you are running this query
- λ principle applies to use of any Sigint database

Currently a hidden slide

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Questions you should ask yourself

- would my justification record be clear to a colleague?
- have I justified invading this person's privacy?
- will my successor understand?

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Hidden – replaced by previous slide

Audits

- IPTs currently carry out targeting audit
 - 10% of entries each year, randomly chosen
 - all UK entries each year, wildcards each audit
- quick check of record & key HRA aspects:
 - source field
 - HRA justification
 - MIRANDA number
 - revalidation
- UDAQ & Events also audited

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Audit mandated by SOB

Not meant to be onerous

IPTs conduct audit in different ways.

Now finding that fewer entries need changing => compliance levels going up (education)

Next stage – audit of other databases.

Questions?



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gov.uk

15 minute break



Operational Legalities

Targeting: location and nationality

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk

Pick up from lawyer's words on territoriality.

RIPA – location – UK matters

Policies address nationality issues

Cause of a great many queries to OPP-LEG!

Location, location, location

- λ Law: specific RIPA authorisation for interception of a target located in the UK
- λ Policy: internal authorisation (STA) for a target outside the UK if nationality and/or location is sensitive
- λ all targets require HRA justification (GCHQ is a public authority interfering with individuals' human rights)



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

Distinguish serendipity from indirect targeting. (Don't scare people off doing valid and legal reporting)

Location = law

Nationality = policy

Any 2Ps in the audience?

Expand on Sensitive target – not covered later.

May wish to mention here policy that a target entering a Second Party country must be detasked from all Second Party collection systems



Location?

- without other information, assume:
 - individual is in their country
 - mobile phone is in country of registration
 - email address with country digraph is there

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Sensitive always trumps non-sensitive

Location: belief & knowledge

- λ belief is not 100% knowledge with hindsight; you must not 'turn a blind eye'
- λ based on the information available at any particular time
- λ this may vary - so should our response



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] x [redacted] or [redacted]@gchq.gsi.gov.uk

- Not going into religion or philosophy – frequent topic of questions to OPP-LEG
- The main thing is to record why you made your decision so that, if later it turns out to be incorrect, you have noted the reasons for believing what you did.
- possibly BROAD OAK comments field
- relies on honesty from analysts - in good faith
- it's your judgement call – try to get collateral if possible to help make the decision - but do the best you can possibly do

Target arrives or is discovered to be in the UK...what next?

Consider authorisation options

- λ continuation targeting – RIPA s.16(5)
 - λ 5 working days (1 for SC)
 - λ signed by GCHQ Directorate
- λ then over to customer – RIPA s.8(1) warrant or...



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

Target comes to UK – no longer have to take targeting off cover. In fact we should probably be more interested in why a target has come to the UK and want to do some work on this. There are other options.

16(5) – 5 days from moment analyst realises target is in UK (1 day for SC). After this, need to apply for a warrant or drop targeting. Warrant could have schedule served on us. 16(5) on 8(4) collection. Only selectors you know about at the time, can't add new ones in.

Target in the UK...RIPA s.16(3)

- λ frequent visitors to the UK or known targets
- λ SoS signature required – modification to 8(4) certificate
- λ new selectors may be used
- λ ***indirect targeting is not allowed***



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

NB currently used only for counter-terrorism, serious crime, CP and Russian intelligence officers (March 2008)

16(3) – you might know the name of the target; or it's a suspicious selector used by one or more unknown targets; business case from IPT, goes through various internal checks; OPP~LEG puts it into appropriate format -> SoS; renewed every 6 months (3 for SC); update it with current knowledge.

Directorate may authorise urgent additions

Indirect targeting – the use of a selector to identify and select the communications of one individual with a view to selecting and reporting the activities of another individual – the target; such targeting requires an authorisation appropriate to the location and nationality of the real target

Indirect targeting is getting sustained intelligence on A by targeting B. (Wanting intelligence on B as well doesn't get you off the hook.)

Point to note: it is using another selector to get the **communications of the target**, not to find **information about him**. So it is fine to target a Swedish girl-friend of a person in the UK to find out info about him, as long as you defeat communications between the two of them.

e.g. Your target's in South Africa, his wife's in India. Targeting her phone no. to get his comms = indirect targeting, but is ok as long as you can demonstrate necessity and proportionality. But if target comes from SA to UK, you'll need additional authorisation to continue to target the wife's phone no.

If no authorisation is sought...

- λ examine and report traffic intercepted up to time you knew target was in UK*then....*
- λ use B3M HRA 'register' to alert
- λ check location using events or THUGGEE
- λ examine a cut (B3M / UDAQ) every 48 hrs to check whereabouts



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA requests to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

All this assumes they can't be bothered with any of the authorisation options . Ask what this says about the level of justification of the target in the first place.

Note no alert system on text repositories, only voice [and we don't know how widely used the B3M mark up is used, tho I think it's reasonably well known]

These days, esp for voice, call records are a better way of tracking where someone is, and they're less intrusive

NB B3M flag only for target in the UK

Policy authorisations

- STA and TTA provide records of actions where UK &/or British Overseas Territory law does not require authorisation
- respect 2nd Party sensitivities
- actions are validated by a GCHQ senior (or nominated GC8s in ITT)
- we can justify targeting if challenged
- QC is mandatory



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

No legal authorisations required but action is still sensitive.

Reassurance to Commissioner/IPT.

Datamining STA

- Datamining STA for target in UK – valid for two days
 - named SCS officer signs STA
 - one-off search
- Count-only searches: no authorisation needed

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

STA is handled by OPA-DCSD

SCS sign TTA and datamining STA for targets in the UK – save Directorate when novel or sensitive

For out of hours authorisations the SDO can approve all STA and TTA requests as appropriate but authority from one of the above officers must be obtained at the earliest opportunity.

Datamining for targets in the UK – a **one-off search per repository; must perform search within 2 days but can go back further; can examine all hits returned; count-only**

ZTA – ITT only

Special C2C authorisations

- special access to email communications
- NS only; limited criteria
- 16(3) or STA also required if location or nationality sensitive
- SCS or GC6 approval

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

STA is handled by OPA-DCSD

SCS sign TTA and datamining STA for targets in the UK – save Directorate when novel or sensitive

For out of hours authorisations the SDO can approve all STA and TTA requests as

appropriate but authority from one of the above officers must be obtained at the earliest

opportunity.

Datamining for targets in the UK – a **one-off search per repository; must perform search within 2 days but can go back further; can examine all hits returned; count-only**

ZTA – ITT only

SRA

- authorises receipt of 2 or 3P intelligence on UK-based targets ...
- ... where GCHQ has no authorisation
- avoids indirect targeting
- limited period only

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Max 6 months



Operational Legalities

SIGINT Development

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

By its nature, SD can be intrusive to many people's human rights, as it can involve large-scale interception of many innocent people, cf. interception using strong, known selectors with valid HRA justifications.

SD – can be for technical development or to find target communications from bulk data.

SD justification

- Enhancing GCHQ's capabilities is a national security purpose
- TD – improving specific target knowledge, identifying new sources etc – is justified by the intelligence requirement for that target

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Capabilities – vital for the future of SIGINT; may embrace research

Both are referred to in RIPA certificate.

If asked, MIRANDA number for system testing is 20141

SD proportionality

Restrict to the minimum necessary:

- refine wide initial terms
- define length of task and/or volumes
- limit dissemination and retention

Aim: sustained targeting as soon as practicable

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Capabilities – vital for the future of SIGINT; may embrace research

If asked, MIRANDA number for system testing is 20141

SD reporting

- you may report from SD traffic
- reporting guidelines reflect HRA requirements

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Capabilities – vital for the future of SIGINT; may embrace research

If asked, MIRANDA number for system testing is 20141

Content or metadata?

- voice mail boxes
- SMS text
- an email inside a message
- email subject line
- URL beyond the domain name
(eg <http://www.myrail.com/query-text>)
- an attached routing diagram

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Content or **metadata**?

- IP address
- email address
- DTMF (tone dialling)
- a URL up to the domain

(eg <http://www.myrail.com/>)

- location

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

DTMF = dual tone multi-frequency = touch-tone dialling

- usually metadata but can be content (credit card number)

URL: not for acquisition

- yes for queries

Location is generally metadata too.

[GCHQ policy is to treat it pretty much all the same whether it's content or metadata.]

Content or metadata?

- password

authentication to a communications service –
communications data

other passwords – content

- cookie

depends on data – may be either

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Current ruling: content – moving towards metadata, need to flesh out a few examples passwords to web sites are metadata; banking etc would be content.

There are specific exemptions, eg PILBEAM, PRIMORDIAL SOUP, NEO PUDDING (but getting to be too many exceptions for OPP~LEG liking)

Future of C2C exploitation.....?

WIP to redefine as metadata if possible

Other measures possible, eg limit access to these elements of content – being explored for HAUSTORIUM

Questions?



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gov.uk



Second Parties

Australia, Canada,
New Zealand & USA

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk



GCHQ and Second Parties

- partners respect each others' laws and policies
 - 2nd parties treat UK nationals as their own
- GCHQ must not ask a 2nd party to do something for which we would need a warrant
- we must not task a 2nd party with targeting that would be unlawful in that country

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Example: a target entering a Second Party country must be detasked from all Second Party systems.

Must not search against 2nd party targets in 2nd party databases.



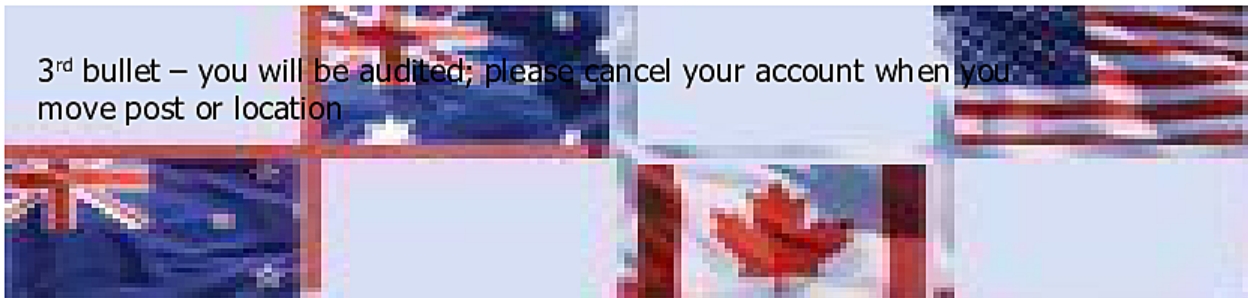
USSID SP0018

- No interception of persons in US without a warrant
- Court order needed to intercept US persons outside the USA
- your use of NSA collection & databases must respect 2nd Party laws and policies

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

2nd bullet – was US Attorney General, but FAA changed to FISA Court.

3rd bullet – you will be audited; please cancel your account when you move post or location





Operational Legalities

Dissemination & Disclosure

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Dissemination

- λ EP is sole vehicle for passing intelligence to customers
- λ Reporting Standards applies proportionality principle to EP

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Do not send intelligence in emails! - you could end up in court!!

Disclosure

- λ SIGINT collected under RIPA may not be used in court
- λ Relevance to prosecutions
- λ Public Interest Immunity – PII certificates

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Do not send intelligence in emails! - you could end up in court!!

Warranted intercept under RIPA can not be used in court (at the moment)

PII – used for other intelligence not covered by RIPA eg second party reissues.

Public Interest Immunity (PII) certificate. This document sets out the damage that could be caused by exposing GCHQ capabilities. Whilst the Foreign Secretary signs the certificate, it is the Judge who has the ultimate say as to whether it is upheld (See [Background notes on PII](#) for further details). If the Judge orders in favour of disclosure, the only remaining option is to drop part or all of the case;

Drop the case. If the Judge rejects the PII certificate and orders that disclosure should be made in the public interest, we would seek to have that part of the case, or in extreme circumstances the case in its entirety, dropped.

Questions?



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk



Operational Legalities

Safeguards and Oversight




This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk

RIPA safeguards

- λ intercepted material must be destroyed as soon as its retention is no longer necessary...
- λ it must be looked at, copied and disseminated to the minimum necessary...
- λ ...for a purpose authorised under the Act
- λ as a matter of policy, GCHQ applies this ethos to all material it acquires, regardless of source
- λ policies for EP and data retention

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Errors and breaches

- λ mistakes happen and we report them
- λ OPP-LEG and LA role: help & advice
- λ an apparent error may be:
 - λ breaking the law 
 - λ a breach of RIPA safeguards 
 - λ nothing to worry about! 
- λ response: procedures, processes & training

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

Political oversight

- λ **Executive** - a Secretary of State exercises authority over the I & S services and is answerable to Parliament
- λ **Parliament - Intelligence & Security Committee** examines expenditure, administration and policy (not operations); members within the circle of secrecy; reports annually to Parliament

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Judicial oversight: Commissioners

- λ **Senior Judges:** independent of HMG and Parliament
- λ **review** Secretary of State's use of powers under RIPA/ISA
- λ **guaranteed access** to agencies
- λ **annual reports** to the Prime Minister

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Interception Commissioner – Sir Paul Kennedy

Intelligence Services Commissioner – Sir Peter Gibson

Investigatory Powers Tribunal (IPT)

- comprises 8 independent lawyers
- investigates complaints against Agencies, law enforcement etc
- anyone, anywhere may complain
- more than 40 people within GCHQ assist in responding to complaint; audit logs

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gov.uk

The Tribunal will ask...

- what did we do?
- was the action **authorised**?
- was it **necessary**?
- was it **proportionate**?
- did GCHQ act reasonably & within its powers?

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk



Operational Legalities

Wrap up

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Key points: 'GCHQ does it legally'

1. Your work must be:

- authorised
- necessary
- proportionate



2. Location:

beware UK & UKUSA
– seek authorisation

3. Errors: we are honest and report them

Currently a hidden slide



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]@gchq.gsi.gov.uk

1. You are responsible for this
2. Location – law
nationality – policy
3. We will help you and agree measures to prevent recurrence

What does this mean for me?

- Collection/technical staff: know what you can and cannot intercept
- Collection manager: help analysts ensure selectors are justified and proportionate
- Analyst/linguist: justify your targeting, seek warrant or STA where necessary
- Reporter: report only what is necessary to address the requirement

Currently a hidden slide

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Contacts

- visit OPP-LEG in B4a
- call RUSSETT 36559
- email [REDACTED]@gchq
- OPP-LEG web pages & compliance website
- speak to your Legal POC.....

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk

Don't forget to sign the attendance sheet or you'll have to come all over again!

...or add your name if it's not there.

Legal & Policy Leads

- AP – [REDACTED]
- BROK – [REDACTED]
- CP – [REDACTED]
- DIG – [REDACTED]
- GSOC – [REDACTED]
- ITT – [REDACTED]
- LANG – [REDACTED]
- MENA – [REDACTED]
- RCIT – [REDACTED]
- SC – [REDACTED]
- TSI – [REDACTED]
- W – [REDACTED]
- ACD – [REDACTED]
- ICTR – [REDACTED]
- OPC-CNE [REDACTED]
- JTRIG – [REDACTED]
- NAC – [REDACTED]
- GTAC – [REDACTED]
- GTE – [REDACTED]
- CRFC – [REDACTED]
- Geo – [REDACTED]
- Bude – [REDACTED]

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ECHQ on [REDACTED] or [REDACTED].

Don't forget to sign the attendance sheet or you'll have to come all over again!

...or add your name if it's not there.

Questions?

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [REDACTED] or [REDACTED]@gchq.gsi.gov.uk