ANNEXES

Annex 1: LIST OF ACRONYMS

Below are detailed the acronyms used in this Report.

AAT: Administrative Appeals Tribunal (Australia)

ACPO: Association of Chief Police Officers

ATCSA 2001: Anti-Terrorism Crime and Security Act 2001

ASIO: Australian Security Intelligence Organisation

ASIS: Australian Secret Intelligence Service

CCTV: Closed Circuit Television

CAFT: Corporate Anti-Fraud Team

CEOP: Child Exploitation and Online Protection Centre

CHIS: Covert human intelligence sources

CIU: Communications Intelligence Unit

CJEU: Court of Justice of the European Union

CMA: Competition and Markets Authority

CNE: Computer Network Exploitation

CPS: Crown Prosecution Service

CRASBO: Criminal Anti-Social Behaviour Order

CSE: Communications Security Establishment (Canada)

CSEW: Crime Survey for England and Wales

CSIS: Canadian Security and Intelligence Service

CSPs: Communications Service Providers

CTSA 2015: Counter Terrorism and Security Act 2015

DRIPA 2014: Data Retention and Investigatory Powers Act 2014

DP: Designated Person

DPA 1998: Data Protection Act 1998

DPI: Deep Packet Inspection

DWP: Department for Work and Pensions

ECA 1972: European Communities Act 1972

ECHR: European Convention on Human Rights

ECtHR: European Court of Human Rights

EO 12333: Executive Order 12333 (USA)

EU: European Union

EU Charter: European Union Charter of Fundamental Rights

FBI: Federal Bureau of Investigation (USA)

FISA 1978: Foreign Intelligence Services Act 1978 (USA)

FISC: Foreign Intelligence Surveillance Court (USA)

GCHQ: Government Communications Headquarters

GCSB: Government Communications Security Bureau (New Zealand)

GPS: Global Positioning System

HMRC: Her Majesty's Revenue and Customs

HRA 1998: Human Rights Act 1998

ICCPR: International Covenant on Civil and Political Rights

ICO: Information Commissioner's Office

IGIS: Inspector General of Intelligence and Security (Australia)

IGIS Act: Inspector General of Intelligence and Security Act (Australia)

IMS: IP multimedia sub-system

IMSI: International Mobile Subscriber Identity

IOCA 1985: Interception of Communications Act 1985

IOCC: Interception of Communications Commissioner

IOCCO: Interception of Communications Commissioner's Office

IOT: Internet of Things

ISP: Internet service provider

IP: Internet Protocol

IP address: Internet Protocol address

IPT: Investigatory Powers Tribunal

ISA 1994: Intelligence Services Act 1994

ISA 2001: Intelligence Services Act 2001 (Australia)

ISC: Intelligence and Security Committee of Parliament

ISCommr: Intelligence Services Commissioner

ISIC: Independent Surveillance and Intelligence Commission

ISP: Internet Service Provider

IPT: Investigatory Powers Tribunal

JCDCDB: Joint Committee on the draft Communications Data Bill

JSA 2013: Justice and Security Act 2013

LGA: Local Government Association

LPP: Legal Professional Privilege

MI5: Security Service

MI6: Secret Intelligence Service

MLAT: Mutual Legal Assistance Treaty

MoD: Ministry of Defence

MPS: Metropolitan Police Service

MTIC: Multi-trader intra-community

NAFN: National Anti-Fraud Network

NCND: Neither confirm nor deny

NCA: National Crime Agency

NDA 1985: National Defence Act 1985 (Canada)

NGO: Non-governmental organisation

NSA: National Security Agency (USA)

NTAC: National Technical Assistance Centre

NZSIS: New Zealand Security and Intelligence Service

ONS: Office for National Statistics

OSC: Office of Surveillance Commissioners

OSCT: Office for Security and Counter-Terrorism

OSINT: Open Source Intelligence

OTT: Over The Top (providers)

PACE: Police and Criminal Evidence Act 1984

PCFOC 2014: Protecting Canadians from Online Crime Act 2014 (Canada)

PFA 2012: Protection of Freedoms Act 2012

PGP: Pretty Good Privacy

PIC: Priorities for Intelligence Collection

PRA: Pen Register Act (USA)

PSNI: Police Service of Northern Ireland

RIPA: Regulation of Investigatory Powers Act 2000

RIP(S)A: Regulation of Investigatory Powers (Scotland) Act 2000

RUSI: Royal United Services Institute

SCA: Stored Communications Act 1968 (USA)

SIGINT: Signals Intelligence

SIRC: Security Intelligence Review Committee (Canada)

SISA 1979: Security Intelligence Service Act 1969 (New Zealand)

SOCA: Serious Organised Crime Agency

SPoC: Single Point of Contact

SSA 1989: Security Service Act 1989

SSA 2012: Search and Surveillance Act 2012 (New Zealand)

TA 1984: Telecommunications Act 1984

TEU: Treaty on European Union

THS: Tor Hidden Services

TIA 1979: Telecommunications (Interception and Access) Act 1979 (Australia)

TICSA 2013: Telecommunications (Interception Capability and Security) Act 2013 (New Zealand)

Tor: The Onion Router

url: Uniform Resource Locator

VOIP: Voice Over Internet Protocol

VPN: Virtual Private Networks

WA 1968: Wiretap Act 1968

WGD: Warrant Granting Department

WTA 2006: Wireless Telegraphy Act 2006

Annex 2: DEFINED TERMS

Below are listed the terms defined for ease of reference and used in this Report.

1. **Acquisition Code** (Acquisition and Disclosure of Communications Data Code of Practice, March 2015).

2. **Belhadj IPT Case** (*Belhadj and others v the Security Service and others* (Case No IPT/13132-9/H)).

3. **Big Data** (very large data sets).

4. **Charles Farr Statement** (Charles Farr's witness statement of 2014 in the Liberty IPT Case).

5. **Content-derived metadata** (the technical and "less intrusive" elements of communications content)

6. **Covert Surveillance and Property Interference Code** (Covert Surveillance and Property Interference Code of Practice, December 2014).

7. **Data Protection Directive** (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

8. ***Digital Rights Ireland*** (Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger and others*, EU:C:2014:238).

9. **Draft Equipment Interference Code** (Draft Equipment Interference Code of Practice, February 2015).

10. **Draft Interception Code** (Draft Interception of Communications Code of Practice, February 2015).

11. **e-privacy Directive** (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector)

12. **EU Data Retention Directive** (Directive 2006/24/EC 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**).**

13. **Interception Code** (Interception of Communications Code of Practice).

14. **ISC Privacy and Security Report** (Intelligence and Security Committee, *Privacy and Security: A modern and transparent legal framework*, HC 1075, (March 2015)).

15. **ISC Rigby Report** (Intelligence and Security Committee, *Report on the Intelligence relating to the murder of Lee Rigby*, (November 2014)).

16. **JCDCDB Report** (Report of the Joint Committee on the Draft Communications Data

Bill, HL Paper 79 HC 479 (December 2012)).

17. **Liberty IPT Case** (*Liberty and others v The Secretary of State for Foreign and Commonwealth Affairs and others*, Case Nos. IPT/13/77/CH; 13/92/CH; 13/194/C and 13/204/CH, [2015] UKIPTrib 13_77-H).

18. **Liberty ECtHR Application** (*10 Human Rights Organisations v United Kingdom,* an application to the ECtHR filed on 10 April 2015).

19. **PI IPT Case** (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs and GCHQ and others*, Case No. IPT/14/85/CH).

20. **Retention Code** (Retention of Communications Data Code of Practice, March 2015).

21. **The RUSI Review** (Independent Surveillance Review of the Royal United Services Institute).

22. **Service providers** (used to refer to: (1) companies which offer communications services (Communications Service Providers properly so called), such as BT and Vodafone, (2) companies providing internet access (commonly referred to as Internet Service Providers), such as AOL, Virgin Media and Sky (collectively, technical readers will know these two categories as the four lower levels of the OSI 7-layer model), and (3) companies which operate "*over the top*" of an internet connection (commonly called OTT providers or Applications Services Providers), such as Facebook and Twitter).

23. **The Snowden Documents** (documents stolen from the US National Security Agency by the contractor Edward Snowden, and published since 2013, purporting to describe various surveillance capabilities and activities).

24. **SURVEILLE Report** (SURVEILLE, *Paper Assessing Surveillance in the Context of Preventing a Terrorist Act,* (May 2015)).

25. **Venice Commission Report** 5 (European Commission for Democracy Through Law (Venice Commission), *Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies*, Study No 719/2013 (April 2015)).

Annex 3: WRITTEN SUBMISSIONS RECEIVED

Access
All Party Parliamentary Group on Drones
Association of Chief Police Officers
The Bar Council
Dr Paul Bernal
Big Brother Watch
Bingham Centre for the Rule of Law
Birnberg Peirce and Partners
Caspar Bowden
BT
Center for Technology & Democracy
Jan Clements
Competition and Markets Authority
Paul Connolly
Dr Andrew Defty and Professor Hugh Bochel
Demos
DWP
Mark Dzięcielewski
EE
Equality and Human Rights Commission
Facebook/Google/Microsoft/Twitter/Yahoo
Faculty of Advocates
Gambling Commission
Peter Gill
Global Network Initiative
GCHQ
Richard Greenhill
Guardian Media Group
Morton Halperin
The Henry Jackson Society
HMRC
Home Office
Human Rights Watch
Interception of Communications Commissioner's Office
The Internet Services Providers' Association
The Internet Telephony Services Providers' Association
The Law Society
Liberty
Local Government Association
Ray McClure
Media Lawyers Association
Metropolitan Police Service
MI5
MI6
Gavin Millar QC
National Union of Journalists

NCA
The Newspaper Society
Ofcom
Sir David Omand
Open Rights Group
Police Scotland
PSNI
Charles Raab
Rights Watch (UK)
Roke Manor Research Ltd
Royal Mail
The Scottish Government
Graham Smith
The Society of Editors
Professor Peter Sommer
Talk Talk Group
Telefonica
Three
UCL
Virgin Media
Vodafone

Annex 4: MEETINGS

UNITED KINGDOM

Rt Hon Theresa May MP, Home Secretary
Rt Hon Yvette Cooper MP, Shadow Home Secretary
James Brokenshire MP, Security Minister
Office of Security and Counter-Terrorism, Home Office
Foreign and Commonwealth Office
Sir Nigel Sheinwald, Special Envoy on intelligence and law enforcement data sharing

MI5
MI6
GCHQ
National Technical Assistance Centre

US Embassy
Canadian High Commission
German Embassy

Alison Saunders, Director of Public Prosecutions
Crown Prosecution Service

National Crime Agency
Rob Wainwright, Director, Europol
National Policing Lead for Communications Data
Metropolitan Police Commissioner
MPS Assistant Commissioner for Specialist Crime and Operations
MPS Communications Intelligence Unit
MPS SO15 Communications Data Team
Senior National Coordinator, Counter-Terrorism
Data Communications Group Futures
Chief Constable and Deputy Chief Constable, Police Service of Northern Ireland
Gloucestershire Constabulary
Nottinghamshire Police
Local Government Association
Association of Chief Trading Standards Officers
Hampshire Trading Standards
Brighton City Council
National Anti-Fraud Network

Members of Intelligence and Security Committee, UK Parliament
Members of Joint Committee on Human Rights, UK Parliament

Sir Michael Burton, President, Investigatory Powers Tribunal
Charles Flint QC, Member, Investigatory Powers Tribunal
Rt Hon Sir Mark Waller, Intelligence Services Commissioner

Rt Hon Sir Paul Kennedy, Acting Interception of Communications Commissioner
Rt Hon Sir Anthony May, Interception of Communications Commissioner
Rt Hon Sir Christopher Rose, Chief Surveillance Commissioner
Rt Hon Lord Judge, Chief Surveillance Commissioner designate
Rt Hon Sir William Gage and Rt Hon Sir Scott Baker, Office of Surveillance Commissioners
Jo Cavan, Director, IOCCO
Sue Cobb, Chief of Staff to the Intelligence Services Commissioner
Dr Michael Maguire, Police Ombudsman for Northern Ireland

Royal United Services Institute
Open Society Justice Initiative
Jamie Bartlett and Carl Miller, Demos
Eric King, Privacy International
Alan Rusbridger and staff, The Guardian
Prof Ian Brown, University of Oxford
Dr Richard Clayton, University of Cambridge

Dinah Rose QC
Matthew Ryder QC
Martin Chamberlain QC
Jonathan Glasson QC
Tom Hickman
Ben Jaffey

Sir David Omand
Graham Smith
Morton Halperin

Apple
BT
Facebook
Google
Vodafone
Communications Data Strategy Group, CSP representatives

GERMANY

Federal Ministry of the Interior
Federal Ministry of Justice
Federal Chancellery
Federal Data Protection Authority
BND (foreign intelligence agency)
BfV (internal security service)
Federal Office for the Protection of the Constitution
G10 Commission
Bitkom (Federal Association for Information Technology)
Prof Christoph Moellers, Humboldt University of Berlin

Prof Hans-Georg Albrecht, Max Planck Institut

UNITED STATES

Office of the Director of National Intelligence
National Security Agency
Federal Bureau of Investigation
Department of Justice

Foreign Intelligence Surveillance Court

Yahoo
Google
Apple
LinkedIn
Dropbox
Twitter

Susan Friewald, University of San Francisco
David Medine and Prof Jim Dempsey, PCLOB
Prof David Cole and Alberto Bedoya, Georgetown University

Access
American Civil Liberties Union
Cato Institute
Center for Democracy and Technology
Center for National Security Studies
Electronic Frontier Foundation
Human Rights Watch
New America Foundation
Third Way

CANADA

Office of the Communications Security Establishment Commissioner
Security Intelligence Review Committee
Chief Justice and Justices of the Federal Court
Justice Canada
Royal Canadian Mounted Police
Public Prosecution Service of Canada
Professor Craig Forcese, University of Ottawa

BRUSSELS

Paul Nemitz, DG Justice, Director Fundamental Rights
Luigi Soreca, DG Home, Director Internal Security
Matthias Reute, DG Home, Director General
Gilles de Kerkhove, Counter-Terrorism Coordinator
Stefano Manservisi, Chef de Cabinet of High Representative Mogherini
Giovanni Buttarelli, European Data Protection Supervisor
Claude Moraes MEP, Chair of LIBE Committee
Timothy Kirkhope MEP
Axel Voss MEP
Marju Lauristin MEP

Not in that list are the Review team (1.23 above), the people with whom I enjoyed fruitful dialogues at various conferences, notably those organised by Wilton Park in October and November 2014, those referred to at 8.39 above whom I did not meet but who gave their assistance with the law of the Five Eyes countries, and those whose assistance came via email or twitter.

I am also grateful to Simon McKay for letting me see proofs of his *Covert policing: law and practice* (2nd edn. 2015), to Poppy Anderson for Viscount Falkland (2.20(a) above) and, as ever, to my special adviser Professor Clive Walker.

Annex 5: IMPACT OF ENCRYPTION AND ANONYMISATION

1. In this Annex the following key is used:

   (a) Eve: Agency.

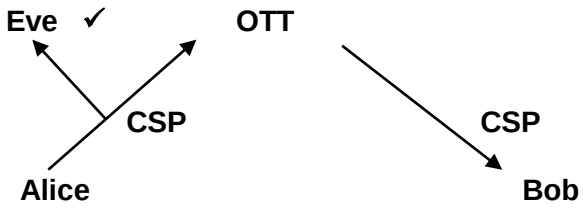
   (b) Alice: Sender of email.

   (c) Bob: Recipient of email.

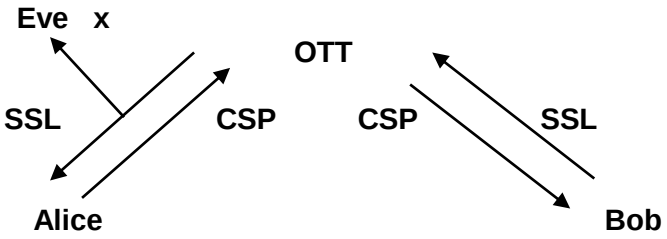
   (d) SSL: Secure Sockets Layer.

   (e) The communications data being discussed in the following examples is sender/recipient details.

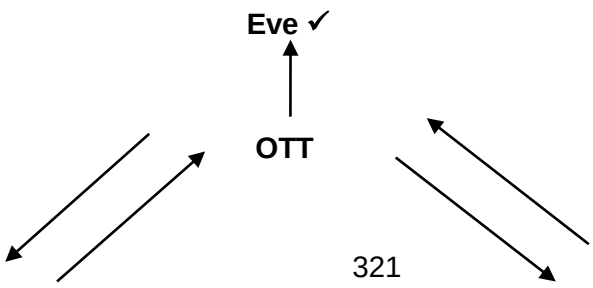
2. First example: there is no encryption in use. Eve can obtain access to the content and sender/recipient details of an email sent by Alice to Bob via the CSP.



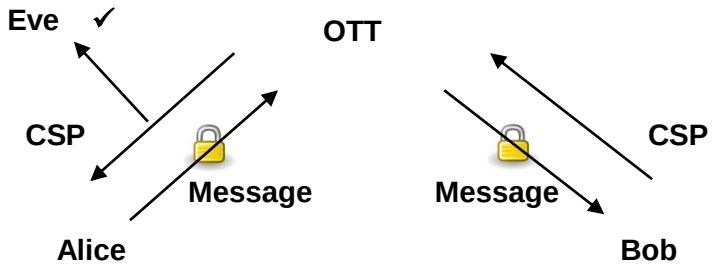
3. Second example: the OTT provider is using SSL, meaning that the content and sender/recipient details of an email sent by Alice to Bob are visible to the OTT. They are not visible to the CSP. The CSP is only able to see that the email is to be sent to the particular OTT provider.



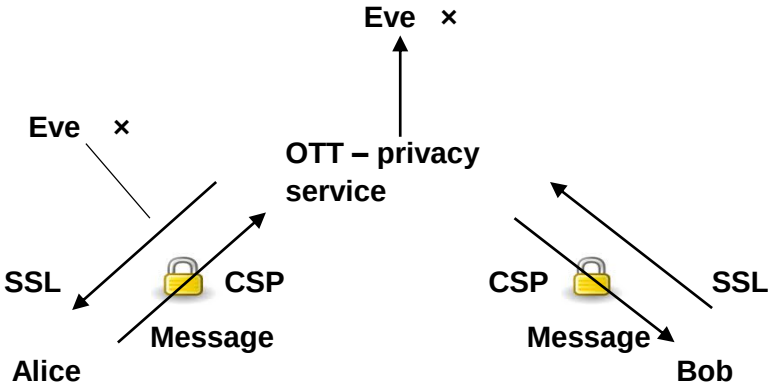
4. Third example: Eve can access the content and sender/recipient details from the OTT provider via a warrant or court order. If the OTT provider is based overseas, it may not cooperate with a UK court order.



5. Fourth example: the use of end-to-end encryption means that the content of the email is not visible to the CSP or the OTT provider. Sender/recipient details are visible to both.



6. Fifth example: the OTT provider is a privacy service. It does not retain data at all and so cannot provide data in response to a warrant or court order. If the OTT provider does collect data, Alice and Bob can hide sender/recipient details by using an anonymisation service such as Tor and end-to-end encryption will provide protection for the content. Content and sender/recipient details are not visible to a CSP because SSL and end-to-end encryption are used. The privacy service could be compromised overtly or covertly and so a user may use an anonymisation service before visiting the privacy service.



7. For the sake of completeness, it should be noted that the combined protection offered by SSL, end-to-end encryption and anonymisation services is not absolute. A user of all three is still vulnerable to CNE.

Annex 6: LIST OF BODIES WITH NON-RIPA POWERS

Department	Mechanisms (non-RIPA)	Section
Department for Business Innovation and Skills	Business Protection from Misleading Marketing Regulations 2008	21 (1) , 23(1)
	Companies Act 1985	434 (2); 444 (1); 447 (2) (3)
	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Consumer Protection Act 1987	18 (1), (2); 29(4)(5)(6)
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Copyright Design and Patents Act 1974	16(a)
	Copyright Design and Patents Act 1988	107A (2), 198A (2)
	Enterprise Act 2002	225-227
Competition & Markets Authority	Companies Act 1985	434 (2); 444 (1); 447 (2) (3)
	Competition Act 1998	
	Enterprise Act 2002 (Soon to be replaced by the Consumer Rights Bill)	225-227
	Consumer Credit Act 1974	
	Business Protection from Misleading Marketing Regulations 2008	21, 23
	Fair Trading Acts 1973, 1986	29(1)
Financial Conduct Authority	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Financial Services & Markets Act 2000	16(1)(2), 131E(1), 165, 165A, 171-175, 218A-221, 305
	Pensions Act 2004	75, 192
	Pensions (Northern Ireland) Order 2005	67,68 & 73
	Merchant Shipping (Accident Reporting and Investigative) Regulations 2005	12(?)
Ministry of Justice	Prison Rule 35	

Department for Work and Pensions	Pensions Act 2004	75, 192
	Pensions (Northern Ireland) Order 2005	67,68 & 73
	Social Security Administration Act 1992, as amended by the Social Security Fraud Act 2001	09B and 110A
	Social Security Administration Act 1992, as amended by the Social Security Fraud Act 2001 (Northern Ireland)	110(6)
	Child Support Act 1991	15(6)
Northern Ireland Department of Social Development	Child Support (Northern Ireland) Order 1991	16, 17
Northern Ireland Department of Agricultural and Rural Development	Animal Health Act 1981 amended by the Disease of Animals (Northern Ireland) Act 2010	36(i) (5)
DEFRA	Animal Health Act 1981	36(i) (5)
HMRC	Finance Act 1988	127
	Taxes Management Act 1970	20(1)
	Value Added Tax Acts 1983, 1994	Schedule 11 Section 4
Scottish Government	Adult Support & Protection (Scotland) Act 2007	10(1), 61
Welsh Government	Environmental Protection Act 1990	19(2), 71(2), 116(1)
Northern Ireland Department of Enterprise Trade & Investment	Business Protection from Misleading Marketing Regulations 2008	21(1), 23(1)
	Consumer Credit Acts 1974 and 1985	36B(1), 162, 174A
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Timeshare Act 1992	Schedule 2 s3(1)(2)
	Trade Marks Act 1994	93(2)
	Video Recordings Act 2010	17(2)
	Weights and Measures (Northern Ireland) Order 1981	41(2) Schedule 9(4)

	Control of Pollution Acts 1974, 1975	93(1)
	Environmental Protection Act 1990	19(2), 71(2), 116(1)
	Salmon & Freshwater Fisheries Act 1975	31(?)
General Dental Council	Dentists Act 1984 (Amendment) Order 2001 or 2005	50(3)
Police, National Crime Agency, Police Service of Northern Ireland	Dangerous Dogs Act 1991	5(2)
	Drug Trafficking Act 1985	55
	Police and Criminal Evidence Act 1984	19, 20
	Serious Organised Crime and Police Act 2005	66
	Video Recordings Act 1984, 2010	17(2)
	Terrorism Act 2006	33
Department for Transport (Marine Accident Investigation Boards)	Merchant Shipping Act 1995	257-259
Department for Transport (Maritime and Coastguard Agency)	Merchant Shipping Act 1995	257-259
	Merchant Shipping (Accident Reporting and Investigative) Regulations 2005	12(?)
Home Office (Border Force)	Immigration Act 1971	28D
	Immigration and Asylum Act 1999	127, 131
Ministry of Justice (National Offender Management Service)	Prison Rule 35	35
Scottish Criminal Casework Review Commission	Criminal Procedure (Scotland) Act 1995	194L
Gangmasters Licensing Authority	Gangmasters (Licensing) Act 2004	16
Information Commissioner's Office	Privacy and Electronic Communications Regulations 2003 (as amended 2011)	31A
	Enterprise Act 2002	225-227
	Data Protection Act 1998	29 (3), Schedule 9(1)(3)

Ofcom	Communications Act 2003	135
	Enterprise Act 2002	225-227
	Wireless Telegraphy Act 2006	89(4), 99(3)
	Postal Service Act 2011	55
Scottish Fire and Rescue	Fire Precautions Act 1971	19(1)
Northern Ireland Fire Authority	The Fire and Rescue Services (Northern Ireland) Order 2006	19(1)
England Fire Authority	Fire Precautions Act 1971	19(1)
Welsh Fire Authority	Fire Precautions Act 1971	19(1)
Northern Ireland Prison Service	Prison Rule 35	35
Local Authorities	Business Protection from Misleading Marketing Regulations 2008	21 (1) , 23(1)
	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Consumer Protection Act 1987	18 (1), (2); 29(4)(5)(6)
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Control of Pollution Acts 1974, 1975	93(1)
	Copyright Design and Patents Act 1974	16(a)
	Copyright Design and Patents Act 1988	107A (2), 198A (2)
	Dangerous Dogs Act 1991	5(2)
	Fire Precautions Act 1971	19(1)
	Food Safety Act 1990	32(5)(6)
	Local Government Act 1971, 1974 and 1982	141
	Package Travel, Package holiday and Tours Act 1992	Schedule 3 Section 3
	Property Misdescriptions Act 1991	Schedule s3(1)
	Timeshare Act 1992	Schedule 2 s3(1)(2)

	Trade Descriptions Act 1968	28(1)
	Trade Marks Act 1938, 1994	93(2)
	Weights and Measures Act 1985	39, 79(2), Schedule 8(4)
	Weights and Measures (Northern Ireland) Order 1981	41(2), Schedule 9(4)
Charity Commission	Charities Act 2011	47, 52
Charity Commission for Northern Ireland	Charities Act (Northern Ireland) 2008	22 (3), 23 (1)
Environment Agency (and regional equivalents)	Control of Pollution Acts 1974, 1975	93(1)
	Environmental Protection Act 1990	19(2), 71(2), 116(1)
	Salmon & Freshwater Fisheries Act 1975	31(?)
	Environment Act 1995	108(4)(k)
Food Standards Agency	Food Safety Act 1990	32(5)(6)
Health and Safety Executive	Regulatory Reform (Fire Safety) Order 2005 in England and Wales Fire (Scotland) Act 2005 (FSA) in Scotland	19(1)
	Health and Safety at Work Act 1974	20
	Working Time Regulations 1998	Reg. 28(7) and Schedule 3
	Food and Environment Protection Act 1985	Part III s19 and Schedule 2, para 2.
	Plant Protection Products Regulations 2011	Reg. 7 and Schedule 1, para 4
	Plant Protection Products (Sustainable Use) Regulations 2012	Reg. 20 and Schedule 3, para 4

	Environmental Protection Act 1990	115
	Regulatory Reform (Fire Safety) Order 2005	Article 26
	Fire (Scotland) Act 2005	62
	Electricity Act 1989	28, 30
	Electricity Safety, Quality and Continuity Regulations 2002 REACH Enforcement Regulations 2008	Reg. 30. Schedule 6
Pensions Regulator	Pensions Act 2004	75, 192
	Pensions (Northern Ireland) Order 2005	67,68 and 73
British Board of Film Classification	Video Recordings Act 1984, 2010	17(2)
General Optical Council	Opticians Act 1989	21(1), (3)
Child Support Agency	Child Support Act 1991	15(6)
UKBA (See Home Office)	Immigration and Asylum Act 1999	127, 131
General Pharmaceutical Council (for the Royal Pharmaceutical Society of Great Britain)	Pharmacy Order 2010	11
Intellectual Property Office	Copyright Design and Patents Act 1974, section	16(a)
	Copyright Design and Patents Act 1988, sections	107A (2); 198A (2)
Department for Culture, Media and Sport	Privacy and Electronic Communications Regulations 2003	

Trading Standards	Business Protection from Misleading Marketing Regulations 2008	21 (1) , 23(1)
	Companies Act 1985	434 (2); 444 (1); 447 (2) (3)
	Consumer Credit Acts 1974, 1985	36B (1), 162, 174A
	Consumer Protection Act 1987	18 (1), (2); 29(4)(5)(6)
	Consumer Protection from Unfair Trading Regulations 2008	21(1)(b)(d)
	Copyright Design and Patents Act 1974	16(a)
	Copyright Design and Patents Act 1988	107A (2), 198A (2)
	Enterprise Act 2002	225-227

Annex 7: THE SNOWDEN ALLEGATIONS

1. In this annex, I summarise some of the main allegations that emerge from the Snowden Documents unlawfully taken from the NSA in the United States and subsequently published by a number of newspapers.[1]

2. As emphasised at para 7.7 of the Report, this summary should not be taken as any endorsement by me of the truthfulness or representative nature of the practices alleged (all of which, save PRISM, are neither confirmed nor denied by the Government), nor of the conduct of Edward Snowden.

Bulk interception allegations

PRISM

3. The PRISM programme was said to involve the collection by the NSA of data from the servers of nine US internet companies (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple - "*the Prism Providers*"). Types of data collected included a range of digital information such as email, chat, videos, photos, stored data, VOIP, video conferencing and online social networking details. An automated system called PRINTAURA organised the data by category. Some providers had the capability to provide real-time notification of an email event by a target, such as a log-in.[2]

UPSTREAM

4. UPSTREAM data collection programmes such as BLARNEY, OAKSTAR, FAIRVIEW and STORMBREW, were said to involve the collection by the NSA of communications from the infrastructure which carries internet traffic, rather than from the servers of internet companies. A slide referring to UPSTREAM programmes is said to describe "*the collection of communications from fiber cables and infrastructure as data flows by*".[3]

TEMPORA

5. This programme was said to involve the interception by GCHQ of digital traffic flowing through the underwater fibre optic cables landing in the UK. It is described as providing analysts access to "*huge amounts of data*". "*All web, email, social, chat, EA, VPN, VOIP*" is said to be "*promote*" from the cables; "*high-volume, low value traffic*", such as peer-to-peer downloads is then filtered out. A buffering technique holds data in a "*repository*"; content for three days and metadata for up to 30 days "*to allow retrospective analysis and forwarding to other systems*". Search terms are applied to the promoted data and any hits are entered into TEMPORA. Data is also entered into TEMPORA based on "*technology type or IP subnet*". In 2012, GCHQ appeared to be managing to collect data from 46 cables in this way.[4]

---

1 References in this Annex are to on-line versions of the documents discussed.

2 https://www.eff.org/document/2013-06-06-wapo-prism.
https://www.eff.org/document/20140430-intercept-prism-olympics.

3 https://www.eff.org/document/2013-06-08-guard-prism.

4 https://www.eff.org/document/20140618-der-spiegel-gchq-report-technical-abilities-tempora.

MUSCULAR

6. The MUSCULAR programme was said to be a joint GCHQ and NSA project which intercepted internal fibre optic cables used by Google and Yahoo, to transmit unencrypted data between their data centres.[5] During a 30-day period in 2012-2013 it was said that 181 million records were sent from a British collection point back to the USA via this programme.[6]

DISHFIRE

7. Slides relating to this programme describe the collection of almost 200 million text messages per day in 2011 by NSA from around the world. Slide 5 describes why SMS is regarded as so useful**;** they contain metadata and "*metacontent*" (content derived metadata), the latter includes such "*gems*" as notifications relating to credit card transactions and flight plans which can enhance analytics.[7]

OPTIC NERVE

8. Under this programme Yahoo webcam images were said to be intercepted by GCHQ. In one 6 month period in 2008 images were collected from 1.8 million Yahoo user accounts globally. The programme saved one image every five seconds and users were "*unselected",* i.e., the collection was in bulk rather than targeted. Between 3% and 11% of images were said to involve "*undesirable nudity*". This programme was also used to trial facial recognition technology.[8]

MYSTIC and RETRO

9. The NSA programme referred to as MYSTIC was described as a voice interception programme which used buffering to record an entire country's telephone calls and enable access for a month after the call took place. The RETRO tool, short for *retrospective retrieval*, was said to enable the retrieval of calls up to thirty days in the past.[9]

Bulk Processing tools

10. Under the FASCIA programme the NSA was said to track the movements of mobile phones by collecting location data as people move around. Almost 5 billion mobile phone location records were logged per day.

11. A data sorting tool called CO-TRAVELER was said to look for unknown associates of known intelligence targets by tracking people whose movements intersect.[10]

12. PREFER was said to be the analytic tool used to carry out analysis of the text messages collected via the DISHFIRE programme outlined above. It was able to

---

5 https://www.eff.org/document/2013-10-30-wapo-muscular-smiley
https://www.eff.org/document/2013-10-30-wapo-muscular.

6 https://www.eff.org/document/2013-11-04-wapo-windstop.
https://www.eff.org/document/2013-11-04-wapo-sso-overview.

7 https://www.eff.org/document/20140116-guard-dishfire-presentation.

8 https://www.eff.org/document/20140227-guard-gchq-optic-nerve.

9 https://www.eff.org/document/20140318-wapo-description-data-collection-under-mystic.
https://www.eff.org/document/20140318-wapo-adding-another-country-mystic-program.

10 https://www.eff.org/document/20131210-wapo-cotraveler-overview.

extract information from missed call alerts or texts with international roaming charges. Missed call alerts could allow contact chaining, i.e., working out someone's social network. Border crossings could be worked out from roaming charges texts and names could be extracted from electronic business cards.

13. The XKEYSCORE system was said to be developed by the NSA, to allow analysts to carry out a search, using a single search term, such as an email address, or telephone number, across three days worth of raw data collected via a number of programmes such as PRISM and UPSTREAM. According to documents relating to OPTIC NERVE, the webcam material collected via this programme was fed into XKEYSCORE. XKEYSCORE indexed data sources including email addresses, IP addresses, port numbers, file names, cookies and buddy-lists. Monitoring of Facebook chats was said to be possible simply by entering a Facebook user name and date range. A slide labelled "*future"* listed VOIP as a target. Another slide described how 300 terrorists were captured using intelligence generated from XKEYSCORE.[11]

14. DEEP DIVE was said to have a greater capability than traditional XKEYSCORE which handles low rates of data and ingests all of it. DEEP DIVE could handle 10 gigabytes of data. It "*promoted"* data that has a "*potential intelligence value"* and only that is ingested into XKEYSCORE. Data "*that is not allowed to be in the system – UK-UK"* is blocked. DEEP DIVE XKEYSCORE was said to be used by the TEMPORA programme though this was not the only way in which data was promoted to TEMPORA. Promotion also took place based simply on technology type or IP subnet.[12]

Computer Network Exploitation

15. Documents referred to a number of programmes aimed at "*Active SIGINT*" or CNE. They were said to involve implanting malware (software designed to disrupt a computer) directly onto a user's computer. Examples in the documents describing the use of this technique by GCHQ included a programme called NOSEY SMURF which involved implanting malware to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, TRACKER SMURF which had the capability to provide the location of a target's smart phone with high-precision, and PARANOID SMURF which ensured malware remained hidden.[13]

16. It was also said that a GCHQ project called OPERATION SOCIALIST used technology called QUANTUMINSERT to direct staff at Belgacom, without their knowledge, to fake websites in order to plant malware on their computers.[14] GCHQ was also said to have gained access via CNE to the entire network of a company called Gemalto, which produces SIM cards, including their encryption keys.[15]

17. Documents also said that implants of malware can take place in bulk. An automated system called TURBINE, allows "*the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by*

11 https://www.eff.org/document/2013-07-31-guard-xkeyscore-training-slides.
12 *Ibid.*
13 https://www.eff.org/document/20140128-guard-leaky-phone-apps.
14 https://www.eff.org/document/2013-09-20-spiegel-belgacom.
15 https://www.eff.org/document/20150219-intercept-sim-card-encryption-key-theft-and-mobile-network-access.

groups instead of individually."[16]

18. OPERATION MULLENIZE was said to involve a technique called User Agent Staining to write a unique mark or "*stain*" onto a target machine. The unique marker enabled all the events from the machine to be pieced together to "*recreate a browsing session."* The catalyst for the operation was said to be the sharing of an IP address by many users at one time, which made it difficult to identify users. It was said that a method has been devised to enable "*staining"* on a "*large-scale*".[17]

16 https://www.eff.org/document/20140315-intercept-turbine-intelligence-command-and-control.
17 https://www.eff.org/document/20131004-wapo-gchq-mullenize.

Annex 8: INTERCEPTION CASE STUDIES

Case 1

1. A criminal investigation into a UK-based organised crime group involved in the importation of Class A drugs from South America.

2. Interception assisted in identifying the command and control structure of the group and their associates in other European countries. It identified individuals responsible for facilitating the supply of drugs and also those involved in establishing front companies for importing legal goods. Intercept provided intelligence on the modus operandi employed by the group, the dates and location of the importation, and the storage place of a series of drug shipments.

3. This resulted in the arrest of UK-based members of the group and their co- conspirators overseas, as well as the seizure of significant quantities of Class 'A' drugs, foreign currency, firearms and ammunition. Intercept material provided key intelligence which was pivotal in building an evidential case and ended in the successful prosecution of the defendants. It also served to enhance the Serious Organised Crime Agency **[SOCA]**[18]'s working relationships with overseas partners involved in the investigation.

Case 2

4. A criminal investigation into an organised crime group based in the south east of England involved in acquiring, supplying, and storing firearms in the UK.

5. Interception provided intelligence on the structure of the organised crime group, its methods of working, and the types of crime it was involved in. It helped to identify the types of firearm and the locations where the weapons and ammunition were stored. This led to the seizure of weaponry which ranged from handguns to automatic weapons, as well as significant quantities of ammunition. It also provided intelligence on turf wars with other groups operating in the area, which was critical to operational planning.

6. The intelligence provided by intercept was developed further and helped to identify those responsible for the wholesale supply of firearms in Europe. It also revealed changes to the structure of the group and its weaknesses, enabling SOCA to re- focus the investigation.

7. The result was the successful prosecution of a significant number of gang members involved in the supply and distribution of firearms.

Case 3

8. A criminal investigation into a pattern of escalating violence between a number of rival organised crime groups, including street gangs linked to the London drug economy, operating across the capital.

---

18 Now replaced by the NCA.

9. Intelligence derived from interception indicated a conflict between organised crime groups as each sought to control a greater section of the drugs market. The intelligence suggested the use of firearms by the groups. This prompted immediate steps to tackle the group, with the intention of dismantling the network, disrupting the supply of Class A drugs, preventing further loss of life and arresting those involved. The operation also targeted individuals directly involved in gun possession and crime whilst disrupting other criminal activities such as small-scale drug dealing, acquisitive crime and serious assaults.

10. Intercepted material identified the individual co-ordinating the sale of significant amounts of Class A drugs, led to the location of his safe storage premises, and identified senior gang members involved in the supply chain. It also enabled junior gang members to be identified as couriers of the drugs to numerous locations across London, the Home Counties and beyond, including the method and timing transport. Interception also revealed that the head of the organised crime group was conspiring with others to shoot a rival. This led to an armed stop of the target whilst he was *en route* to the hit location. He was found to be in possession of a loaded firearm and arrested.

11. The primary operation led to the collapse of the network operating across London and the Home Counties. During the course of the operation, intelligence from interception led to the seizure of over 40 firearms, in excess of 200kg of Class A drugs, the seizure of over £500,000 of cash and over 100 arrests.

Case 4

12. A criminal investigation into a London-based money laundering network, linked to several organised crime groups that were responsible for a major share of criminal activity across London.

13. An operation was launched in partnership with HMRC to identify the proceeds linked to the groups' criminal activities and to deny them funds. The police had identified that a considerable quantity of cash was being laundered on a regular basis by a relatively small group of criminals. Launderers were identified as working for multiple crime networks and making significant profits. However, traditional policing methods were unable to provide details of how the network ran their business.

14. Intercepted material indicated the method by which the laundering network was moving funds between accounts. This led to the covert interception of high value cash transactions, depriving the organised crime groups of their profits and diminishing their ability to complete criminal transactions.

15. During the operation, cash in excess of £3 million was seized. Intercept intelligence indicated that a number of criminal enterprises had collapsed and a number of targets had been forced to cease their activities due to a lack of funding.

Case 5

16. Multi-trader intra-community **[MTIC]** fraud is estimated to cost the exchequer approximately £750 million annually. The fraud typically comprises a scheme involving a number of participants which is set up with the sole purpose of defrauding the public purse. For example, an organised crime group acquires a VAT registration number in the UK for the purposes of purchasing goods free from VAT in another EU member state. The goods are imported into the UK and sold at a VAT inclusive price. The UK company selling the goods will then "*go missing*" without paying the output tax due to HMRC. The criminally obtained funds will be laundered through a complex network of financial transactions involving bank transfers and cash movements in the UK and overseas. In practice, MTIC fraud will involve complex layers of companies performing different functions in an effort to conceal the fraud and to thwart investigation and compliance activity.

17. In one particular operation, supported by interception, a total of £3.2 billion in VAT repayments was withheld from criminal groups fraudulently trading in mobile telephones and computer chips. Interception was also critical in identifying the bank of first choice for laundering the proceeds of the crimes. Working with international partners, HMRC was able to prevent the distribution of assets to the criminal gangs. The scale of the criminal conspiracy and related laundering operation is illustrated by the fact that over $200 million of MTIC funds have been frozen and are the subject of criminal and civil action.

18. Since HMRC started using interception to support investigations into MTIC fraud, the level of attempted fraud has reduced substantially from an estimated high of £5 billion in 2005/2006 to an estimated current figure of £750 million.

Annex 9: BULK DATA CASE STUDIES

Case Study 1

1. Since HMRC started using interception to support investigations into MTIC fraud, the level of attempted fraud has reduced substantially from an estimated high of £5 billion in 2005/2006 to an estimated current figure of £750 million.

2. In the late 2000s, bulk data enabled GCHQ to trigger a manhunt for a known terrorist linked to previous attacks on UK citizens. At a time when other intelligence sources had gone cold, GCHQ was able to pick up the trail by identifying patterns of activity online believed to be unique to the suspect. Follow-up searches of bulk data provided further leads for the investigation. This work in turn highlighted links to extremists in the UK. Through a series of arrests, the network was successfully disrupted before any attack could place.

Case study 2

3. In 2010 GCHQ analysts identified an airline worker in the UK with links to al-Qaida. Working with the police, agencies investigated the man, who it transpired had offered to use his access to the airport to launch a terrorist attack from the UK, and pieced together the evidence needed to successfully convict him. This individual had taken great care to ensure that his extremist views and plans were totally concealed in his offline behaviour, meaning that this investigation and conviction would have been highly unlikely without access to bulk data.

Case study 3

4. Sometimes, because of the international nature of al-Qaida inspired terrorism, bulk data is the first and last line of defence. In 2010, an intelligence operation identified a plot which came right from the top of al-Qaida: to send out waves of operatives to Europe to act as sleeper cells and prepare waves of attacks. The intelligence specified unique and distinctive communications methods that would be used by these operatives. GCHQ, in partnership with many other countries, was able to identify operatives by querying bulk data collection for these distinctive patterns. This international effort led, over a period of months, to the arrest of operatives in several European countries at various stages of attack preparation – including one group literally *en route* to conducting a murderous attack.

Case study 4

5. In April 2011, GCHQ intelligence uncovered a network of extremists in the UK who had travelled to Pakistan for extremist training. Whilst the targets were abroad, GCHQ analysis revealed that the group had made contact with al-Qaida. When the group returned to the UK, intelligence suggested that they aspired to conduct an attack, possibly using Improvised Explosive Devices (IEDs). In April 2012, the group was arrested and later charged (in April 2013) under Terrorism Act 2006 s5, for which they received sentences ranging from 5-16 years in prison.

Case study 5

6. GCHQ used analysis of bulk data to track down two men overseas who had been harnessing the vulnerabilities of the web to blackmail hundreds of children across the world, including the UK, into exposing themselves online – causing them huge trauma. Some of the victims self-harmed and considered suicide. It was the vital work of GCHQ analysts that brought this abuse to an end: they were able to confirm the suspects' names and locations, and to identify an accomplice. After liaison between law enforcement agencies, the two men were arrested and jailed in their home country.

Case study 6

7. 2014 bulk data analysis of known ISIL extremists in Syria highlighted links to an unidentified individual whose contacts, locations and attempts to hide his internet activity raised analysts' suspicions. This analysis of bulk data provided the trigger for an investigation involving many different agencies across several countries. This investigation quickly led to the suspect's arrest and prevented a bomb plot in mainland Europe which was materially ready to proceed.

Annex 10: UK RETAINED COMMUNICATIONS DATA USE CASES

Case 1

1. In September 2009 the body of taxi driver Stuart Ludlam was discovered with two gunshot wounds to the head in the boot of his taxi outside the train station in Derbyshire Police carried out checks on the mobiles Ludlam was carrying at the time of his murder in order to help identify his killer. His work telephone had been stolen but data on communications using that device were identified through subscriber checks which revealed that Ludlam had received diverted calls from the main taxi office number. Incoming and outgoing call data with cell site locations were requested to trace Ludlam's movements on that day. Call data was of no use at this time as it only showed the taxi number on divert calling. Police then applied for call data for the taxi landline number to identify the last number to have contacted Ludlam and any other numbers that might be of interest to the investigation, in order to establish how he might have been lured to the murder scene. The last number to have called the taxi company was attributed to a pre-paid SIM card for which there were no subscriber details. Using the telephone data police were able to identify the place where the telephone had been purchased and where the last top-up before the murder had been purchased, which was at a supermarket petrol station a few days beforehand. The petrol station did not have in-store CCTV but police requested the till records which revealed another transaction of 20 GBP of petrol at the same time as the purchasing of the mobile telephone top-up. Officers now knew the time the top-up was purchased, and so examined all CCTV tapes from locations in the vicinity of the supermarket, which showed a male purchasing a mobile telephone in a nearby shop. This male was identified as Colin Cheetham, who after further investigation was convicted of Ludlam's murder and jailed for 30 years. Without access to relevant traffic data Cheetham might never have been identified.

Case 2

2. A 14-year old female from the Fife area was reported missing in November 2009. She had a history of self-harm and multiple suicide attempts. She had left a note for her parents in which she claimed to have been *"hearing voices"*. A trace to find the live location of the victim's telephone was carried out but it had been switched off. Historical call data was examined to ascertain with whom she had been in contact prior to her going missing. The call data identified a mobile telephone whose subscription was attached to an individual unknown to the girl's parents. Checks at the registered address of the subscriber revealed that the missing girl was in the company of a 36-year-old man whom she had met in an internet chat room. The man was charged with sexual offences.

Case 3

3. UK authorities received intelligence from US authorities that an individual using email had sent a movie file of a woman sexually abusing a four-month-old girl. The log-on IP address for this account was found to be registered to a male from Northampton. Further enquiries established that a girlfriend of the individual had three children all

less than four years old. After investigation both were convicted of the serious sexual abuse of the children. The children had been found in conditions of neglect, described by an officer as filthy, unsanitary and unfit for human residence.

Case 4

4. Internet data were used in an investigation into the grooming of a 13-year-old girl on an internet chat service. Examination of the victim's computer by the authorities revealed the email address of a man who had coerced the girl into sending naked photographs of herself and exposing herself during webcam chat. Police officers made enquiries about the e-mail address which revealed the IP address belonged to an address in Wales. Further investigation resulted in the man being charged preventing potentially more serious sexual offences taking place.

Case 5

5. In 2010/ 2011 police used data from thousands of calls over the previous 12 months between more than a dozen mobile phones to dismantle a nationwide cocaine trafficking ring. Two gang members found to be in possession of 3.58 kg of cocaine (valued 165,000 EUR) were arrested and their mobile phones seized. Detectives then spent months examining communications data to identify links between the other members of the group. This resulted in conviction of six gang members who were sentenced for a total of 53 years imprisonment and the confiscation of 61,000 EUR in cash which is being used to fund police operations targeting other drug dealers.

Case 6

6. Operation Frant was a detailed investigation into a number of drug dealers who were flooding London and the UK with high grade heroin from Afghanistan. The aim was to target the individuals who were masterminding this organised crime network, and as they were not 'hands on' the only possible method of detection was detailed investigation of communications data. The first part of the operation targeted the 'runners' with their consignments. In December 2007 Ghaffor Hussein was arrested in possession of a kilogramme of heroin and in January 2008 Christian Bailey was arrested in possession of 8 kilos of heroin. In April 2008 Harminder Chana and Patrick Kuster (a Dutch national) were arrested in possession of 356 kilos of heroin, having been under surveillance when the exchange took place. One of the ringleaders, Atif Khan, was also arrested later that day on the basis of telephone data and additional surveillance evidence linking him and Chana. Upon arrest all suspects' telephones were seized enabling investigators to obtain the cell site data and establish who orchestrated the deals. Mobile telephone call logs revealed that a certain telephone number had been used to call Khan's telephone 26 times, along with several texts, in a 45-minute period after Khan's arrest. This so-called "*dirty telephone"* was attributed to one Abdul Rob by cell site analysis which showed two mobile phones always in the same place at the same time. The telephone evidence was crucial in the case against Rob as there was no previous surveillance evidence of association with the other members of the network. Four members of the network were convicted for conspiracy to supply heroin and sentenced for total 81.5 years imprisonment.

Case 7

7. In January 2008 customs officers at Birmingham airport discovered over 16 kilos of heroine concealed with straws which had been threaded through rugs imported from Afghanistan, they alerted SOCA. SOCA substituted the drugs rugs with dummies, replaced the original packaging, and began a surveillance operation when the gang came to collect them. After the gang's hire car was abandoned for the second time, SOCA investigators decided to switch from traditional surveillance and to focus instead on their other main lead – a single unregistered mobile telephone number used by the gang to contact the courier company. Analysis of telephone data ultimately led to the identification of five men involved in the plot. All five gang members pleaded guilty on the strength of the telephone evidence. The four main players were sentenced at Birmingham Crown Court in June 2009 to between 10 years 8 months and 14 years 8 months and 14 years 5 months for conspiracy to import Class A drugs.

Case 8

8. Police investigated (Operation Backfill) a series of armed robberies where high value cars were advertised on a website for sale for *"strictly cash only"*. Persons interested in buying the cars went to meet the supposed traders and were robbed at gun point. Police examined internet data and identified the laptop and premises from where the suspects had logged onto the internet when posting the advertisements, leading to a number of arrests.

Case 9

9. In October 2004 a large criminal network conspired to steal £229 million from a bank in the City of London by transferring funds to bank accounts opened in seven different countries. Landline and mobile telephone communication data was critical to establishing those involved in this crime and understanding how it happened. The network members used landline, mobile, and kiosk phones in the UK and across multiple countries. Three defendants were extradited to the UK for trial. Billing data, call data and cell-site location data were all used as evidence in the trial which took place in March 2009. Three defendants were convicted of conspiracy to steal and two were convicted of money laundering.

Annex 11: CRIME TYPES FOR WHICH COMMUNICATIONS DATA IS USED

CRIME TYPE	% FOR WHICH COMMUNICATIONS DATA IS USED (OUT OF TOTAL)
Sexual offences	9%
Vulnerable or missing persons	6%
Harassment or stalking	7%
Drugs offences	25%
Homicide, attempted murder & threats to kill	8%
Financial offences	10%
Terrorism	1%
Firearms and explosives	5%
Offences against the person	11%
Offences against property	11%
Other offences	7%

Annex 12: URGENCY OF REQUIREMENTS FOR COMMUNICATIONS DATA

The Acquisition Code (footnote 52) explains that the CDSG has adopted a grading scheme to indicate the appropriate timeliness of the response to requirements for disclosure of communications data.

GRADES	% OF USE DURING 2012 SURVEY
Grade 1 – an immediate threat to life	6%
Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security	18%
Grade 3 – matters that are routine but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime.	76%

Annex 13: LOCAL AUTHORITY USE OF COMMUNICATIONS DATA

1. This annex contains case studies illustrating how councils make use of communications data to stop criminal activity and bring perpetrators to justice.

Operation Magpie – Cambridgeshire County Council

2. Operation Magpie concerned an investigation into an organised crime group who defrauded elderly and vulnerable people. The criminals exploited their victims to the extent that one person was evicted from their home, as well as laundering cheques to the value of £700,000.

3. The ringleader of the gang received a prison sentence of 7 years with two co-conspirators receiving sentences of 5 years each. 16 other offenders were also convicted of money laundering offences serving prison sentences of up to 30 months.

4. Malcolm Taylor from Trading Standards at Cambridgeshire County Council said "*Without access to communications data, we would not have been in a position to connect the conspirators and detect the level of criminality that extended to over 100 vulnerable and elderly victims, some of whom have since died*".

Operation Troy – Suffolk County Council

5. Operation Troy was a long running advanced fee fraud case that was investigated and prosecuted by Suffolk's trading standards service. The fraud operated between 2007 and 2010, involved at least £7.5 million of consumer detriment affecting well over 16,000 consumers and involved two distinct frauds;

6. An escort/companion fraud in which consumers were offered guaranteed work as escorts and companions in return for a registration fee, however no work was subsequently provided.

7. A debt elimination fraud in which consumers paid an advanced fee to receive a debt elimination service but little or no service was ever provided.

8. The fraud was complex and well organised, operating from call centres in Spain. UK customers made contact with the call centres using free phone numbers that appeared to be UK based after viewing various escort websites offering work. During calls with escort agency staff, false promises would be made regarding the immediate availability of work and potential earnings available. Many consumers complained of similar experiences and provided similar accounts of last minute cancelled work appointments after they had paid their fees.

9. The escort websites and telephone numbers changed frequently to confuse consumers and make it difficult for enforcement bodies to track the source of the fraud. By using RIPA powers and obtaining communications data for the telephone numbers used for the fraud, the following links were established:

(a) The multiple telephone numbers were owned and operated by only two individuals. One of those individuals, who held the majority of the numbers, had been identified as being involved in operating multiple UK bank accounts used for money laundering aspects of the fraud and the creation of shell companies.

(b) All the UK free phone numbers were being redirected to Spanish based numbers that were linked to a small number of call centres operating from the Malaga area of Spain. These call centres were all owned by one man who was known to have a previous history of fraudulent trading.

(c) The link provided by this communications data provided evidence that what appeared outwardly to be over 12 different separate escort website/agencies were in fact all one fraud perpetrated by one set of linked individuals.

10. In June 2012 European Arrests warrants were applied for in respect of Antoni Muldoon, the man at the helm of the fraud, and two other members of the gang, Geraldine French and Bradley Rogers. All three were returned to the UK. Following extradition in September 2012 Muldoon pleaded guilty to conspiracy to defraud at Ipswich Crown Court.

11. Following Muldoon's plea, and after a series of trials at Ipswich Crown Court including a ten week trial involving five of the defendants that concluded in June 2013, seven further members of the gang were found guilty of offences including conspiracy to defraud and money laundering offences. The sentences handed down totalled 36 years overall, with Muldoon receiving 7.5 years for his role and Mark Bell of Ipswich, Muldoon's right hand man in the UK, receiving 6.5 years.

12. Confiscation proceedings followed the sentencing and to date £315,000 has been awarded in confiscation and costs, which Suffolk Trading Standards has used to repay victims of the fraud. Confiscation proceedings are continuing against Antoni Muldoon who is known to have benefited to the largest extent from this fraud and the amount of confiscation possible from him is expected to be substantial. Confiscation hearings for Muldoon are set to take place in January 2015.

13. In July 2014 four of the defendants appealed their convictions and sentences at the Court of Appeal in London and in front of three sitting High Court Judges all appeals were turned down.

14. Steve Greenfield, Suffolk's Head of Trading Standards and Community Safety commented that "*RIPA powers were essential to the successful outcome of this case*".

Counterfeit goods case study 1

15. Two internet traders based in Slough were selling counterfeit trainers on e-bay for £35.00. The only intelligence the trading standards service had was the e-mail address and mobile phone numbers that the complainants used to make the purchase. The actual retail price of these trainers was £135 a pair. By obtaining the data from the mobile phones and the IP address the council were able to pinpoint the address being

used by the perpetrators. A test purchase had been made prior to a warrant being sought. A sting operation resulted in a seizure of trainers with a street value of £325,000 and both offenders received a custodial sentence. Without the communications data this would not have been possible.

Counterfeit goods case study 2

16. Officers seized some potentially counterfeit mirrors from a shop. By the time the mirrors were confirmed as being counterfeit the trader had disappeared after failing to attend for interview. The contact details he provided proved to be false. However, officers obtained a mobile number for the trader and the subscriber details identified his home address in Swansea. This enabled officers to contact him. He subsequently pleaded guilty to 3 offences under the Trade Marks Act 1994. Without the access to the communications data officers would not have been able to find the new address to which he had moved and so the investigation would not have been able to proceed.

Barnet council – rent deposit scheme fraud

17. A man and woman were jailed following a Barnet Council investigation to crack a highly organised plot to obtain fraudulent payments from the authority by using a complex web of false identities to open a string of bank accounts which were then activated to receive thousands of pounds in fraudulent rent deposit scheme payments. The rent deposit scheme is used by the council to provide people in need of housing with initial financial support to help secure a tenancy for private rented accommodation.

18. The investigation by the council's Corporate Anti-Fraud Team **[CAFT]** was launched after uncovering irregularities with a number of rent deposit payments. Investigators went on to identify 41 fraudulent payments worth £132,629 which had been paid to different bank accounts. During the course of the investigation a further 12 fraudulent payments worth more than £31,600 were intercepted and blocked by CAFT.

19. CAFT worked with NAFN to obtain mobile phone records, under RIPA, which provided significant evidence to show that the accused were in regular contact on the days when substantial withdrawals and deposits were made. The powers also enabled the investigators to identify the real owners of the false identities by obtaining the mobile phone service providers records which identified names and addresses where these suspects could be found. The legislation also allowed information of redirected post from credit card companies, banks and online purchase deliveries which also assisted in tracing addresses that the suspects used which were then the subjects of police / CAFT raids. Without access to this information the investigation would not have proceeded to a useful outcome.

Landfill tax fraud

20. A council was alerted to a skip hire company who were disposing of waste in an unauthorised manner, including avoiding payment of landfill tax estimated at £1.3 million. Enquiries made by the council identified three suspects but there was no evidence to link them to the offences. Subscriber and itemised billing data provided by NAFN proved that there were regular communications between the individuals

during periods in question. Without this information, it would have been impossible to pursue a prosecution.

Fraudulent car trader

21. A car trader was convicted of multiple offences contrary to the Fraud Act 2006 in relation to the sale of misdescribed and clocked cars. Vehicles were purchased at auction with higher mileage and advertised online via AutoTrader. The trader claimed a third party was responsible and he simply allowed the third party to use his account at auction to obtain vehicles more easily. However, SIM cards found in possession of the car trader were confirmed, using communications data, as being associated with unregistered pay as you go telephone numbers used in adverts for vehicles. During the course of the investigation, the trader sold his house and moved location; a second set of communications data (forwarding address details from Royal Mail helped to locate him for the purposes of arrest, entry warrants and interview. The penalty was 12 months imprisonment and a Proceeds of Crime Act 2002 confiscation order in excess of £58,000.

Annex 14: LOCAL AUTHORITY RIPA COMMUNICATIONS DATA REQUESTS VIA NAFN

	2012	2013	2014	2015
January	247	190	81	158
February	328	204	106	190
March	341	313	146	
April	270	230	78	
May	383	136	83	
June	233	208	71	
July	292	335	1563[19]	
August	338	246	166	
September	292	129	110	
October	496	337	119	
November	150	201	62	
December	198	175	91	
Total	**3568**	**2704**	**2676**	

[19] The July 2014 one-off surge involved a criminal investigation by one local authority in relation to a suspected £multi-million conspiracy to defraud. The application included approximately 1300 requests for subscriber checks and itemised billing.

Annex 15: THE LAW OF THE FIVE EYES

Australia

1. The primary statute governing access to intercept and communications data in Australia is the TIA 1979.[20] It is long and complex.

2. It distinguishes between "*interception*" of communications that are passing through a telecommunications system and "*access*" to stored communications on a carrier's equipment, although both are only lawful when carried out pursuant to a warrant. Interception is narrowly confined to "*real time*" communications: "*listening to or recording by any means, such a communication in its passage … without the knowledge of the person making the communication*."[21] Once a communication has become accessible to the recipient, it is no longer passing over a telecommunications system and must be accessed via a stored communications warrant.[22]

Interception

Australian Security Intelligence Organisation

3. The TIA 1979 Part 2-2 sets out the mechanism by which ASIO (the Australian equivalent of MI5, governed by the Australian Security Intelligence Organisation Act 1979) might be issued with a warrant to intercept communications. ASIO cooperates with the Australian Secret Intelligence Service **[ASIS]**, the Australian Signals Directorate and the Australian Geospatial-Intelligence Organisation.

4. ASIO may apply for, three types of warrant to intercept communications in order to access the communications of a person who is reasonably suspected of being engaged in or likely to engage in activities prejudicial to security.[23] Each of those warrants may be issued by the Attorney-General on request by the Director-General of Security:

   (a) A warrant that specifies the telecommunications service likely to be used by a person engaged in activities prejudicial to security;[24]

   (b) A named person warrant that grants authority to intercept the various communications methods employed by an individual (all their mobile phone numbers or email addresses);[25]

   (c) A B-party warrant, which enables the interception of a service that will be used by a non-suspect to communicate with a suspect.[26]

---

20 The Surveillances Devices Act 2004 and the Telecommunications Act 1997 contain further relevant provisions.
21 TIA 1979 s6(1).
22 TIA 1979 s5F(1). If only the telecommunications data is required, then stored material may be accessed without a warrant under s 178 and 179 of TIA.
23 TIA 1979 s9(1).
24 TIA 1979 s9(1).
25 TIA 1979 s9A.
26 TIA 1979 s9(1)(a)(ia).

5. Accordingly, national security warrants may only be obtained for quite narrow purposes; they do not provide a basis for bulk interception. Section 10 sets out a mechanism for the issuing of emergency warrants, when the Director General of Security considers it appropriate, for no longer than 48 hours.

6. A separate regime governs the grant of warrants where ASIO wishes to intercept "*foreign intelligence"*. In each case, the Attorney-General must be satisfied, on the basis of advice from the Minister of Defence or Foreign Affairs, that obtaining the foreign intelligence set out in the notice is in the interests of Australia's national security, foreign relations or economic well-being. Once again, three types of warrant may be issued:

   (a) A warrant authorising interception on quite a general level to a particular "*telecommunications service*." Where known, the name and address, occupation and number of the subscriber should be set out in the request.[27]

   (b) A named person warrant, for which the application must specify the telecommunications service that is being used by a person or foreign organisation and the foreign intelligence information that will be obtained.[28]

   (c) A "*foreign communications*" warrant for the interception of foreign communications only, (those sent or received outside of Australia.[29]

7. The Director-General must not request the issue of a foreign intelligence warrant under s 11A, 11B or 11C for the purpose of collecting information concerning an Australian citizen or permanent resident.[30]

Law Enforcement Authorities

8. The TIA 1979 Part 2-5 sets out the circumstances in which law enforcement bodies may intercept telecommunications. They may apply for a warrant to an eligible Judge or a nominated member of the Administrative Appeals Tribunal **[AAT]**. A range of agencies can apply, at both the state and federal level, including the Independent Broad-based Anti-Corruption Commission and various Crime Commissions.[31]

9. The application must be supported by an affidavit setting out the facts and other grounds on which it is based. Two types of warrant may be issued:

   (a) A telecommunications service warrant, which authorises the interception of a particular telecommunications service that may be used by an identified individual. It must set out the number of previous applications (if any) related to the service or that person and the use made by the agency of information obtained by interceptions under those warrants.

27 TIA 1979 s11A(1).
28 TIA 1979 s11B.
29 TIA 1979 s11C.
30 TIA 1979 s11D(5).
31 TIA 1979 s39.

(b) A named person warrant, which must set out the name of the person and details sufficient to identify the telecommunications service they are using, details of previous applications and use made of the material obtained.[32]

10. The Judge or AAT member must be satisfied that there are reasonable grounds for suspecting that a particular person is using or is likely to use the service and the information that would be likely to be obtained would be likely to assist in connection with the investigation by the agency of a serious offence.

11. The Judge or AAT member should have regard to:

(a) How much the privacy of any person or persons would be interfered with;

(b) The gravity of the conduct constituting the offence;

(c) The value of the information obtained;

(d) The extent to which other methods have been used, would be likely to assist, or might prejudice the investigation.

12. They must be satisfied that all other practicable methods of accessing the communications have been exhausted.[33]

13. Warrants may be sought and obtained, in urgent circumstances, via telephone.[34]

Stored Communications

14. The TIA 1979 Part 3 contains a separate regime governing access to stored communications. In broad terms, both ASIO and criminal law enforcement agencies are entitled to issue preservation notices, requiring a carrier to preserve all stored communications specified in the notice.[35] The notice may only specify one person or telecommunications service.[36] The TIA 1979 distinguishes between a domestic preservation notice and a foreign preservation notice. A foreign preservation notice is issued when a foreign country intends to request the Attorney-General to secure access to telecommunications. In that sense, they reflect the UK's MLAT regime.[37]

15. ASIO does not have to apply for a preservation notice before seeking access to material on the basis of a warrant. It may apply for a warrant in any case where it reasonable grounds for suspecting that a particular carrier holds stored communications that is likely to assist in connection with the investigation of a serious contravention (a crime of sufficient seriousness).[38] Furthermore, ASIO does not normally have to apply for a separate stored communications warrant. An interception warrant will also entitle them

32 TIA 1979 ss42 and 46A.
33 TIA 1979 ss46 and 46A.
34 TIA 1979 ss43 and 50.
35 Recent changes have added a new TIA 1979 s110A that has restricted the power to access stored telecommunications data to "*criminal law enforcement agencies*", rather than the broader law enforcement agencies described above.
36 TIA 1979 s107H(3).
37 TIA 1979 s107N.
38 TIA 1979 s106(c).

to access stored communications if the warrant would have authorised interception if it were still in passage.[39] However, a criminal law enforcement agency will need to apply for a stored communications warrant.

16. TIA 1979 contains a number of provisions relating to the destruction of material obtained via warrants.

Telecommunications data

17. TIA 1979 Part 4 sets out the circumstances in which bodies may obtain access to telecommunications data. Telecommunications data is not formally defined, although it does not include the contents or substance of a communication.[40] A new mandatory data retention regime specifies categories of information that must be kept by service providers for a period of two years.[41] These categories include the subscriber of a relevant service and the source, time, date, and location of a communication.[42]

18. Sections 174-6 provide for three types of disclosure of telecommunications data to ASIO. Firstly, on a voluntary basis by a service provider "*if the disclosure is in connection with the performance by* [ASIO] *of its functions*." Secondly, an authorisation for access to existing information or documents (which may be granted by the Director General of Security, Deputy Director General of Security and an officer of ASIO approved by the Director General). Thirdly, a slightly wider body of individuals may authorise access to prospective information (anybody above a certain level of seniority within ASIO may grant permission), for not longer than 90 days.[43] In the case of an authorised disclosure, the authorising individual must be satisfied that the disclosure would be "*in connection with the performance by* [ASIO] *of its functions*".

19. Sections 177-180 set out the framework governing the disclosure of existing telecommunications data to enforcement agencies (which includes any criminal law enforcement agency). An enforcement agency may authorise the disclosure of telecommunications data where reasonably necessary to enforce the criminal law, locate missing persons, enforce a law imposing a pecuniary penalty or protect the public revenue. Accordingly, bodies that have the power to levy a fine may seek access to telecommunications data.[44] The disclosure of prospective telecommunications data may be authorised for a limited period where reasonably necessary for the investigation of a serious offence.[45]

20. Sections 180A and 180E allow authorised officers of the Australian Federal Police to obtain access to telecommunications data for the purpose of further disclosing that material to a foreign authority. The procedure, as with intercepted material, is similar to the UK's MLAT process.

---

39 TIA 1979 s109.
40 TIA 1979 s172.
41 TIA 1979 s187C.
42 TIA 1979 s187A.
43 TIA 1979 ss175-6.
44 As long as they are defined as an enforcement agency in the newly amended TIA (see s110A).
45 TIA 1979 s180.

21. Before any authorisation is made (on any of the bases set out above) the authorised officer considering making the authorisation must be satisfied on reasonable grounds that any interference with privacy is justifiable and proportionate.[46]

22. An authorisation, the notification of that authorisation, revocation and notification of the revocation must be in written or electronic form, and must contain:

    (a) The identity of the eligible person and the basis on which they are eligible to make the authorisation;

    (b) The person or company from whom the disclosure is sought;

    (c) Details of the information or documents to be disclosed;

    (d) A statement that the eligible person considers that to be in connection with ASIO's functions; and

    (e) The date of the authorisation. [47]

23. Authorisations made on behalf of an enforcement agency must set out certain additional material. The rules are very detailed and vary, depending on whether the material is historic or prospective and on behalf of a foreign government or not.

24. Each year, the head of an enforcement agency must give the Minister a written report that sets out the number of authorisations made and the number of disclosures to foreign countries and names of those countries. The minister consolidates that material and lays before Parliament a report that sets out the consolidated material.[48]

The Australian Secret Intelligence Service

25. Different provisions apply to the activities of ASIS (the equivalent of MI6), which are controlled by the Intelligence Services Act 2001 **[ISA 2001]**.

26. ASIS may gather intelligence about an Australian person or class of Australian persons outside Australia, as long as this is authorised by the Minister for Foreign Affairs.[49] The Minister must be satisfied that gathering the intelligence is necessary for the proper performance of one of ASIS's statutory functions, and the person or class of persons is involved in one of a list of specified activities (such as acting for a foreign power, or other activities that pose a threat to Australia's security).[50] ISA 2001 s14 waives any liability for ASIS in respect of acts committed overseas that would be unlawful if done pursuant to a proper function of the agency. That waiver does not extend to activities inside Australia that ASIO could not carry out without a warrant, but it may well include interceptions overseas.

---

46 TIA 1979 s180F.

47 The Telecommunications (Interception and Access) (Requirements for Authorisations, Notifications and Revocations) Determination 2012, drafted by the Communications Access Co-ordinator.

48 TIA 1979 s186.

49 TIA 1979 s9.

50 ISA 2001 s9.

Oversight

27. Oversight of the interception process is provided in Australia by three mechanisms. Firstly, the Parliamentary Joint Committee on Intelligence and Security oversees the administration and expenditure of the Australian intelligence community, including ASIO. It is made up of members of both houses of Parliament nominated by the governing party, in consultation with all the parties in Parliament, although with a majority made up of the party currently in government. It reports to Parliament once a year, and will also review any amendments to include new agencies in the list of those which may authorise the disclosure of metadata.[51]

28. Secondly, the Inspector General of Intelligence and Security **[IGIS]** is established by the Inspector General of Intelligence and Security Act 1986 **[IGIS Act]**. It is a largely investigatory role, appointed for five years. He carries out broad-ranging investigations into the actions of the agencies at his own initiative or pursuant to a complaint or a request from the public or from ministers, including the Prime Minister.[52] He must seek the approval of the Prime Minister or a responsible Minister before investigating actions that took place outside of Australia.[53]

29. The IGIS is appointed by the Governor-General on the advice of the Prime Minister. The office is accountable to the Prime Minister but does not take directions from him. IGIS provides an annual report to the Prime Minister, who may redact that report before laying it before Parliament, although an unredacted version must be made available to the leader of the opposition.

30. As part of his role, IGIS also conducts regular inspections and investigations. Amongst those inspections are regular reviews of the documents that ASIO has relied on as providing the basis for its interception warrants.

31. Thirdly, the Commonwealth Ombudsman investigates the use of interception powers by law enforcement agencies, including through regular inspections of their records.[54] The office does not have jurisdiction over the intelligence agencies.[55] The Ombudsman must also inspect the records of enforcement agencies to determine their compliance with the new metadata regime.[56]

Canada

32. Canadian law provides a separate authorisation mechanism for the police and the security services to collect data.

Criminal law enforcement

33. Part VI of the Criminal Code, added pursuant to the Protection of Privacy Act 1974, provides for the grant of judicial warrants to intercept private communications. Private

51 TIS 1979 ss110A(11) and 176A(11).
52 IGIS Act s8.
53 IGIS Act s9AA.
54 Ombudsman Act 1976 s5.
55 Ombudsman Regulations 1977 sch. 1.
56 TIA 1979 s186B.

communications are defined as "*any oral communication or any telecommunication that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.*"

34. In order to obtain an interception warrant, the police must make an application to a judge of a superior court of criminal jurisdiction that is signed by the Attorney General of the province in which it is made (or an agent specified for this purpose by the Government). It must be accompanied by an affidavit setting out (s185):

> "... (c) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence;
>
> (d) the type of private communication proposed to be intercepted;
>
> (e) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used;
>
> (f) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made;
>
> (g) the period for which the authorization is requested; and
>
> (h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[57]

35. The application is made *ex parte* and is heard confidentially. However, targets of interceptions must be given notice of that fact they have been subject to surveillance, within 90 days of the authorisation having expired. A confidentiality extension may be granted up to three years after the investigation has come to a close (s196) in terrorism offence cases, where the judge is persuaded that it is in the "*interests of justice*". There are special provisions for obtaining an urgent authorisation from the judge (s188).

36. Stored communications, for example in cloud storage or on a personal computer, may also be accessed via a production order or search warrant. A search warrant may be granted by a judge who is satisfied that there are reasonable grounds to believe that there is "*anything on or in respect of which any offence"* has been or is suspected to

[57] Subsection (h) does not apply to some serious crimes and terrorism offences.

be committed, or evidence as to commission of an offence or the whereabouts of a person who is believed to have committed an offence.[58] A judge may also order a person, other than a person under investigation for an offence, to produce documents or prepare a document based on data already in existence and produce it.[59]

37. There is some confusion within Canadian law concerning whether emails that have already been sent should be governed by intercept or search warrants. In *R v Telus* (2013) SCC 16, the Supreme Court interpreted "*interception*" purposively, holding held that a warrant requiring a service provider to prospectively provide access to text messages was invalid: the police were seeking an "*interception*," as the service provider stored text messages on their servers as part of the communication and transmission process. Thus it is likely that the Royal Canadian Mounted Police should use their intercept powers, not those for search warrants, when seeking prospective access to email.

38. In late 2014, the Canadian Parliament passed the PCFOC 2014 that amended certain aspects of the Criminal Code. It provided for a clearer and more comprehensive framework for access to metadata by judicial warrant or court order, on a "*reasonable grounds to suspect*" standard (one that is lower than the more traditional reasonable grounds to believe threshold).[60]

Access for the Security Services

39. The CSIS are regulated by the CSIS Act 1984, which distinguishes between "*security intelligence*" and "*foreign intelligence."* The former relates to national security threats; the latter to the political or economic activities of foreign states. Save in relation to the s16 exception set out below, CSIS's role relates to the collection and analysis of security intelligence, and it is broadly the equivalent of MI5.

40. The CSIS Act 1984 s12 provides, where relevant:

> "The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

41. The s16 exception provides that the service may collect information or intelligence in relation to any foreign state as long as that information does not relate to a Canadian citizen, permanent resident or Canadian corporation and is done in Canada.

42. Warrant applications are made to a special bank of 14 specially selected and security cleared Federal Court judges, who meet up twice a year to ensure consistency. They largely hear warrant applications alone but may sit in larger numbers to hear an application and to hear submissions from CSIS on a topic of wider interest, although in

---

58 Section 487.1.

59 Section 487.12. A separate provision concerns provision of financial data of those suspected of Terrorist Financing or Money Laundering (487.13).

60 Criminal Code 417.014-018.

such cases the substantive decision is still taken by a single presiding judge. They are entitled to appoint an *amicus* advocate to make submissions in respect of the privacy issues raised by the application. I was told, in the course of my meeting with several judges of the Court, that they frequently appoint *amicus* counsel when novel warrants are sought that deploy new technology or propose new applications of old technology. The members of the Court were of the view that those counsel provided them with real assistance. I was told that warrant applicants can be made, heard and determined within 24 hours, and dealt with even faster in an emergency. The ordinary time lag is around 3 days.

43. The applicants are subject to a high duty of candour and may not omit relevant or important information. They will be criticised for failing to do so, as they were in *X(Re)* (2013) FC 1275, when Judge Mosley concluded they had deliberately suppressed their intention to monitor Canadian terror suspects outside of Canada (via cooperation with other Five Eyes members).[61]

44. In addition to the judges (who sit on rotation), the Designated Proceedings Registry employs eight full time staff and one full time senior counsel. The Registry's annual budget (excluding infrastructure and some IT costs) was $826,000 last year (*circa* £430,000). During 2013-14 the Federal Court dealt with 85 new warrant applications and 178 renewal applications.

45. A warrant must be supported by an affidavit, which I am told are ordinarily between 35 and 200 pages long. They set out (amongst other things):

    (a) Why the applicant believes "*on reasonable grounds*" that the warrant is necessary for the Service to carry out its role;

    (b) Other procedures have been tried and failed or are unlikely to succeed;

    (c) The type of communication to be intercepted or information, records, documents or things to be obtained;

    (d) The identity of the person whose communication is proposed to be intercepted (if known); and

    (e) Any previous applications in respect of that person.

46. A warrant may not be issued for longer than 60 days, where it is issued to enable the Service to investigate "*threats to the security of Canada*", or one year in any other case.

47. Thus, this warrant process involves a two-stage review process: by the Minister and also by the court. The judicial element was introduced following a series of reports into abuses carried out by the Canadian police Security Services in the 1970s.

48. In 2008 in *Re CSIS*, the Federal Court held that the CSIS had no power to carry out activities beyond Canadian borders because the CSIS Act is not extraterritorial in scope, or at least did not authorize overseas conduct that was not in compliance with

[61] The judgment was upheld by the Court of Appeal (*Re(X)* 2014 FCA 249)

foreign laws (and thus violated foreign sovereignty). As a practical result, the power to covertly collect information (pursuant to a s21 warrant) relating to foreign affairs is restricted to the right to take steps within Canada itself. The effects of that decision were reversed by PCFOC 2014 which provided that CSIS may perform its duties and functions outside of Canada. It expressly authorises a judge to issue a warrant for overseas investigations, even if those investigations may be violation of foreign or other laws.

49. Sections 34 and onwards of the Act establish the SIRC, composed of members of the Canadian Privy Council. Those who sit on SIRC are not ordinarily members of the Senate or House of Commons. The Governor in Council (in practice, the Canadian federal cabinet) appoints the members of the Committee in consultation with the Prime Minister, Leader of the Opposition and the leader of each party with at least 12 Members of the House of Commons. The individuals appointed play an important but comparatively limited role in the operations of SIRC. They retain other obligations and ordinarily only meet a small number of times per year. The day-to-day operations of SIRC are carried out by its full time staff of 18 individuals.

50. The Committee is required to review the Service in general, although the statute does not specify that it should review the warrantry process. However, in practice SIRC reviews a random sample of all warrant applications in any given year (around 5%). That review involves an examination of the underlying documents that led to the warrant application, that were not provided to the court in the application. Their reports are provided to the Minister and the Director of the Service. SIRC also prepares an annual report recounting its operations and summarising its findings and recommendations.

51. Any individual may complain of the Service's activities to the Committee, which is entitled to investigate and make recommendations. .[62] SIRC has no powers to enforce its holdings. It is competent only to make recommendations.

52. The National Defence Act 1985 **[NDA 1985]** recognised the existence of what is now the CSE, a signals intelligence agency and the Canadian equivalent of GCHQ. NDA 1985 defined CSE's mandate as:

> "(a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."[63]

62 Section 37.
63 273.64(1).

53. In conducting its mandate (a) and (b) functions, CSE may not direct its activities at Canadians or any person in Canada and their activities are subject to measures to protect the privacy of Canadians in the use and retention of intercepted material. When CSE performs its mandate (c) function providing assistance to federal law enforcement and security services, it is sheltered by those bodies' lawful authority (e.g., a Part VI authorization or CSIS Act warrant).

54. When CSE collects foreign intelligence, this is generally an internal decision with no legislated oversight requirements. However, in the course of collecting foreign intelligence through signals intelligence operations, CSE may sweep up incidental "*private communications*" – that is communications involving Canadians or persons in Canada. To prevent this from being a violation of the Criminal Code's Part VI prohibition on unlawful intercepts, the NDA 1985 puts in place a special authorization regime, involving the Minister of National Defence. Unlike CSIS, CSE may be authorised by the Minister to obtain foreign intelligence that may involve private communications without reference to the courts. The Minister must be satisfied that the interception will be directed at foreign entities outside Canada, the information could not be obtained by other means, the value of the material justifies the interception and that satisfactory measures are in place to protect the privacy of Canadians and to ensure that the material will only be used or retained if they are essential to international affairs, defence or security. These broad powers stand in some contrast to the focused and specific warrantry process for CSIS.

55. While CSE has historically adopted the position that a ministerial authorisation was not required before it obtained access to metadata, following *Telus* and *Spencer*, and the changes introduced by PCFOC 2014, that position is no longer arguable.

56. NDA 1985 requires the appointment of a supernumerary (retired) judge as a Commissioner of CSE to review its activities and investigate any complaints (section 273.63). The current Commissioner is supported by 11 staff members. His operation costs a little under $2 million Canadian dollars per year.[64] Among other things, the Commissioner reviews any new ministerial authorisations relating to private communication on a provisional basis and then addresses them in more detail in his annual review. His staff are also given access to the data analysis engineers within CSE and may confirm the processes and uses that it is subjected to.

57. The Commissioner's reports have been an important source of information concerning what mechanisms are employed by CSE and also how it interprets its obligations. In particular, the 2012 Commissioner's report disclosed CSE's policy concerning the private communications of Canadian citizens that are the 'bycatch' of a foreign intelligence collection:

    (a) They must be destroyed, save where the material is foreign intelligence or material essential to protect the lives or safety of individuals of any nationality, or where it contains information on serious criminal activity relating to the

64 http://www.ocsec-bccst.gc.ca/ann-rpt/2013-2014/ann-rpt_e.pdf p. 13.

security of Canada or is essential to identify, isolate or prevent harm to the Canadian Government's computer systems.

(b) At the expiry of an authorisation, CSE must report to the Ministry of National Defence explaining what Canadian communications were retained and on what basis.[65]

(c) When CSE shares information with its global partners, the names of any Canadian are redacted and only reinstated at the specific request of a partner country and after CSE has satisfied itself that the requesting government department has proper authority and justification to make the request.[66]

New Zealand

The Security and Intelligence Service

58. NZSIS is New Zealand's equivalent of MI5, and is governed by the New Zealand Security Intelligence Service Act 1969 **[SISA 1979]**.

59. Like Canada, America (and to some extent Australia), New Zealand provides for judicial oversight of the warrant process at the point of authorisation. However, unlike those countries, that oversight is provided by a retired High Court Judge, the Commissioner of Security Warrants. The Commissioner is a creature of statute, created in 1999.[67]

60. Domestic warrant applications are jointly signed off by both the Minister and the Commissioner. The applicant must provide sworn witness evidence that the interception is necessary for the detection of activities prejudicial to security or for the purpose of gathering foreign intelligence information essential to security. They must also provide evidence that any communication sought to be intercepted is not privileged and that the information is not be obtained by any other means.[68]

61. Foreign intelligence warrants operate differently. Firstly, the Commissioner is not involved in their authorisation. Secondly, as well as satisfying the conditions above, NZSIS must demonstrate that that there are reasonable grounds for believing that no New Zealand citizen or permanent resident is to be identified by the proposed warrant as a person who is to be subject to the warrant and that any place to be specified in the proposed warrant is occupied by a foreign organisation or a foreign person.

62. Whether internal or foreign, intelligence warrants must specify the type of communication to be intercepted, the identity of the persons (if known) whose communications are sought to be intercepted and (if not known) the place or facility in respect of which communications may be intercepted.[69] Given the restrictive nature of those requirements, it is unlikely that NZSIS has any power to carry out bulk interception.

---

65 *Ibid.,* p. 14-15.
66 *Ibid*., p. 27.
67 SISA 1979 s5A.
68 SISA 1979 s4A.
69 SISA 1979 s4B.

63. SISA 1979 also contains provisions relating to destruction of irrelevant data.

The Government Communications Security Bureau

64. The GCSB was originally a branch of the Ministry of Defence. It bears some resemblance to GCHQ in the United Kingdom. The Director of GCSB may apply in writing to the Minister for an interception warrant authorising the interception of:[70]

(a) Communications made or received by one or more persons or classes of persons specified in the authorisation or made and received in one or more places or classes of places specified in the authorisation;

(b) Communications sent from, or being sent to an overseas country; or

(c) The accessing of one of more specified information infrastructures or classes of information infrastructures that the Bureau cannot otherwise lawfully access.

65. As under SISA 1979, any application for a warrant or access authorisation must be made jointly to the Minister and the Commissioner of Security Warrants, if anything done under the warrant is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident.[71] If the warrant or authorisation is not sought for the purpose of intercepting the private communications of a person who is a New Zealand citizen or permanent resident, only the Minister needs to agree it.[72]

66. The Minister and Commissioner may grant the interception warrant if satisfied that it is for the purpose of performing the Bureau's functions; the outcome justifies the interception; it cannot be achieved by other means; there are satisfactory arrangements to ensure that nothing will be done in reliance on the warrant that goes beyond what is necessary; and anything done will be reasonable, having regard to the purposes of the warrant itself.[73] As with SISA 1979, no warrant may be issued for the purpose of intercepting privileged communications.

67. Interception without a warrant may take place in certain narrow circumstances, when the interception does not involve physically connecting an interception device to any information infrastructure or installing an interception device in a place; any access to information infrastructure is "*limited to access to one or more communication links between computers or to remote terminals*" and it is carried out in pursuance of either advising or cooperating with public authorities in terms of protecting communications and infrastructures, or regarding foreign intelligence.[74]

Police Surveillance

68. The Search and Surveillance Act 2012 **[SSA 2012]** sets out a comprehensive regime governing all species of warrant, including warrants for entry, warrants to set up road blocks and interception under a warrant. A warrant is necessary if an enforcement

70 GCSB Act s15A(1).
71 GCSB Act s15B.
72 GCSB Act s14.
73 GCSB Act ss15A(2).
74 GCSB Act s16.

officer wishes to use an interception device to intercept a private communication (as well as various other forms of surveillance).[75]

69. An application for a surveillance device warrant (which includes a warrant to use an interception device) must be made in writing and set out in "*reasonable detail*": the name of the applicant, the provision that authorises the application, the grounds on which it is made, the suspected offence in relation to which authorisation is sought, the type of device, the name address or other description of the person, place, vehicle or thing that is the object of surveillance, what material it is hoped to obtain and the period for which the warrant is sought.[76] If the person, place, thing or vehicle cannot be identified, the application must at least define the parameters of and objectives of the operation. An application may only be made by a constable or an enforcement officer that has been approved by an Order in Council.[77]

70. Other law enforcement bodies than the police may only undertake interception if they have been designated by an Order in Council made by the Governor-General.[78]

71. The application should be made to a Judge, who must be satisfied that there are reasonable grounds to suspect that an offence has been or is being or will be committed and that that offence falls within a list of sufficiently serious crimes, set out in the Schedule to the Act.[79] The Judge must also be convinced that the interception will obtain evidential material.

72. There are mechanisms for obtaining a warrant in an emergency, where there is insufficient time to secure access to a Judge.[80]

Access to Metadata

73. The law concerning access to communications data, or metadata, was unclear until recently. In 2013 it was disclosed that GCSB had taken the view that metadata was not a communication and so could be obtained without a warrant (or indeed any other formal authorisation mechanism).[81] TICSA 2013 has set the position out on a statutory footing. It defines "*call associated data*" as information generated as a result of making a telecommunication that includes the number from which it originates, the number to which it was sent, if it is diverted then the number at which it was received, the time at which it was sent, its duration, if it was from a mobile phone the point at which it first entered the network.[82]

74. Public telecommunications service providers are required to be capable of obtaining call associated data (other than telecommunications that are not authorised to be intercepted under the warrant or lawful authority).[83] That information should be

75 SSA 2012 s46.
76 SSA 2012 s49(1).
77 SSA 2012 s49(5).
78 SSA 2012 s50(1).
79 SSA 2012 s51(1).
80 SSA s48.
81 Kitteridge Report on GCSB Compliance, available online at: http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf para 23.
82 TICSA 2013 s3.
83 TICSA 2013 s10.

provided, on presentation of a proper warrant, to GCSB, SIS or the New Zealand Police.

75. A fresh round of Snowden disclosures in 2014 suggested that GCSB had developed a mass metadata collection program known as SPEARGUN. The basic premise of the alleged program was to insert metadata probes into the Southern Cross Cable, which carries much of New Zealand's telecommunications. Prime Minister John Key admitted that the project had been initiated but denied that it had become operational because he had vetoed it. The controversy arose, in part, as the broad powers under GCSB Act ss15 and 15A were not in place during 2012, when the project was allegedly begun.[84]

Oversight

76. The New Zealand security services are overseen via a number of statutory mechanisms. First, the Intelligence and Security Committee is a Parliamentary body, established in statute, which is made up of five persons including the Prime Minister, Leader of the Opposition and 3 other Members of Parliament.[85] It examines the policies and administration of the Security Intelligence Service and GCSB and consider other questions with intelligence or security implications that are referred to it by the Prime Minister.

77. Second, the Inspector-General of Intelligence and Security, is an individual appointed by the Governor General, on the recommendation of the Prime Minister.[86] The Inspector-General enquires into the Services' compliance with its legal obligations and complaints about its activities. They are specifically required to review, at least once every 12 months, the compliance with the governing legislation in relation to the issue and execution of warrants and authorisations.[87] The Inspector-General reports annually to the Prime Minister and a redacted version of that report is laid before Parliament.

78. Third, as set out above, the Commissioner of Security Warrants is engaged in agreeing to any warrant granted to the security service that will collect the communications of New Zealand citizens or residents.

The United States of America

79. The US law concerning investigatory powers is divided between two separate statutory frameworks. The WA 1968, the Stored Communications Act **[SCA]** and Pen Register Act **[PRA]** govern the use of investigatory powers in conventional criminal law enforcement.[88] A separate regime, the Foreign Intelligence Services Act 1978 **[FISA 1978]**, governs the collection and analysis of foreign intelligence. Both frameworks have been extensively amended since their introduction.

84 https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/
85 Intelligence and Security Committee Act 1996.
86 Inspector-General of Intelligence and Security Act 1996 **[IGISA]** s. 5.
87 IGISA s11(d).
88 US Civil Code Title 18 Chapter 119. SCA and PRA were introduced under the Electronic Communications Privacy Act 1986, which substantially amended the WA 1968.

Criminal law enforcement

80. The WA 1968 governs interception of wireless, oral and electronic communications within the United States. It defines intercept as "*the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.*"[89] Access to information that is not in the course of transmission, is governed by the SCA.[90]

81. All interceptions under the WA 1968 must be authorised by a court and are subject to careful review. US Code s2516 of Title 18 sets out the basis on which law enforcement staff, inside the United States, may be given authority to intercept communications. Various senior officials within federal law enforcement agencies (such as the FBI or the Attorney General's office) may authorise an application to a Federal Judge of competent jurisdiction for an interception warrant.[91] The application must be in writing, on oath and set out the facts and circumstances in some detail. I was told by law enforcement agencies that these applications are frequently substantial documents. An application may only be made in order to provide evidence (from the wiretap) that will be relevant to certain serious federal felonies. If the application is for an extension, it must set out the results obtained thus far or a reasonable explanation for the failure to obtain results under the previous warrant.[92]

82. The court must be satisfied that there is "*probable cause for belief*" that:[93]

    (a) An offence has been or is about to be committed;

    (b) Communications confirming the commission of the offence will be obtained;

    (c) Normal investigative procedures have been tried and failed or are unlikely to succeed;

    (d) The communications method is or will be used in connection with the commission of the offense.

83. The third of those criteria is not required for other types of investigatory warrant, such as a search warrant. As a result, interception warrants are sometimes referred to as "*super warrants*". The warrant shall not continue for longer than is necessary and may not be issued for more than 30 days.[94] In an emergency situation an interception may begin without an application to the court, if an application is made within 48 hours.[95]

84. The ordinary position under the WA 1968 is that an inventory of the fact of interception, dates and whether anything was intercepted is provided to the persons named in the order within 90 days of termination unless the authority can show "*good cause*" to

89 18 U.S.C § 2510(4).
90 As is the case in the United Kingdom, the precise boundary between data that is "*in the course of transmission*" and communications data is a complex area of some uncertainty.
91 18 U.S.C. § 2516 (1).
92 18 U.S.C. § 2518 (1)(f).
93 *Ibid*. at (3).
94 *Ibid*. at (5).
95 *Ibid*. at (7).

withhold that information at an *ex parte* hearing.[96] I was told, during my trip to the United States, that disclosure to the subject ordinarily occurs in the context of a criminal procedure. Those individuals who receive notification that they have had their communications intercepted but are not party to any criminal trial, rarely bring proceedings seeking damages. Such damages are capped in any event.

85. US Code Chapter 21 of Title 18, commonly referred to as the SCA, provides access for law enforcement to both contents and metadata that are stored on a Remote Computing Service. This provides computer storage or processing services to the public by means of an electronic communications system,[97] such as cloud storage. Access to the content of stored communications, without notice, is granted on the basis of a search warrant.[98] Access to stored material that does not include the content of communications may be granted on a similar basis.[99]

86. However, and importantly, a specified subset of non-content may be accessed by administrative subpoena without the scrutiny or authorisation of a court. Those data are: name, address, call records, length of service, types of service used, number used including temporarily assigned IP address, means and source of payment.[100] As a result, much of the most important metadata may be obtained without the permission of a court.

87. Furthermore, the SCA provides for access to metadata records, without judicial authorisation, where the Director of the FBI (or his designee) certifies that they are relevant to an authorised investigation to protect against international terrorism or clandestine intelligence activities. Those requests are known as "*National Security Letters*". The Director of the FBI may request, and a telecoms provider is required to provide, name, address, length of service and local and long distance toll billing records on that basis.[101]

88. An important distinction between US and UK law (as it currently stands) is that there is no requirement for service providers in the United States to store data beyond their own business needs. I was informed during my trip to the US that it was highly unlikely that Congress would consider legislation requiring service providers to retain or create data that they did not themselves need for business purposes (such as billing). However, telecommunications providers are required to retain data that they already produce and create such as: name, address, telephone number of the caller, telephone number called, date, time and length of a call.[102] If law enforcement agencies want access to material beyond that, or want access to other metadata, they are empowered to request that material is preserved, pending an application for access to that data.[103]

---

96 *Ibid*. at (8)(d).

97 18 U.S.C. § 2711(2).

98 If the data owner is put on notice, it may also be accessed via a court order, administrative subpoena or grand jury or trial subpoena 18 U.S.C. § 2703.

99 Search warrant, telemarketing fraud request or court order. It is important to note that for non-content subscriber records, no notice has to be given to the subscriber.

100 18 U.S.C. § 2703 (2).

101 18 U.S.C. § 2709 (b).

102 17 C.F.R. § 42.6.

103 E.g. 18 U.S.C. § 2704.

89. Finally PRA grants both federal and state law enforcement the right to make records of outgoing numbers from (pen register) and incoming calls (trap and trace) to a particular phone number pursuant to a court order.[104] The definition of a "*pen register*" was widened by the USA PATRIOT Act in 2001. It now includes a device which records "*signalling information"* that can record access to the internet and other network analysis devices.[105] The procedure for obtaining a court order is less onerous than the procedure for obtaining a warrant, both in terms of the standard of proof to be met and the level of detail that is ordinarily provided.[106] Court orders under the PRA last for up to 60 days. They do not provide a basis for gaining access to the contents of communications.

Gathering of foreign intelligence

90. FISA 1978 (as amended) authorises the electronic surveillance of foreign powers overseas - including groups engaged in international terrorism - and agents of foreign powers. Much of the material collected under FISA 1978 is gathered overseas or concerns the activities of non-US citizens in the mainland United States. However, a US person may also be an agent of a foreign power,[107] to the extent that they knowingly gather intelligence for a foreign power or engage in sabotage or terrorism on behalf of a foreign power.

91. FISA 1978 authorises broadly three kinds of data collection. First the traditional FISA 1978 process requires a Federal officer, with the approval of the Attorney General, to apply to the FISC, a bespoke federal court made up of eleven district court judges set up following reports of abuse by the intelligence agencies in the United States, for an interception warrant. Those eleven judges sit part time, at the court for one week stints on duty, where they read or hear warrant applications under FISA 1978. The Court has 10 full time staff members: five counsel to the Court and five administrative staff.[108]

92. The majority of applications are dealt with on the papers though I was informed that around 10% are dealt with following an oral hearing.[109] The judges can and do request that the individual who swore an affidavit in support of the application appears before them so that they can be asked questions by the judge. No special advocate can appear to make submissions in defence of the privacy interests in issue. The court has recently accepted an amicus brief from the Centre for National Security Studies on the question of bulk metadata production.[110] However, I am not aware of amicus counsel being instructed to make submissions in specific cases. Historically very few judgements of the FISC have been published. However, there has been a trend towards publication in recent years. A telecommunications provider, that is ordered to provide access to material, or a government body that has applied for a warrant may

104 18 U.S.C. § 3121.
105 18 U.S.C. § 3127 (3).
106 18 U.S.C. § 3122.
107 Defined as a citizen of the US, an alien with lawful permanent residence or a US corporation or unincorporated association.
108 The court does not publish details of its costs but the District Court Judges are not paid any additional salary for their FISC work.
109 In the calendar year 2013, the FISC received 1,655 applications under s 702, 178 applications for "*tangible things*" under s215 and the FBI applied for 14,219 National Security Letters.
110 http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Order-1.pdf.

appeal a decision of the FISC to the United States Foreign Intelligence Surveillance Court of Review. In practice, such appeals are rare.

93. An application for a FISA 1978 warrant must specify the identity (if known) or a description of the specific target of the electronic surveillance. It must set out the facts and circumstances to support the belief that the target is a foreign power or agent of a foreign power and that the targeted facilities will be used by them.[111] The application must also set out the minimisation procedures in place to ensure that the correspondence of United States persons is not acquired, retained or distributed.[112]

94. The judge of the FISC must be satisfied that there is probable cause to believe that the elements above are satisfied (including that the target is a foreign power or agent of a foreign power). An order may be granted for up to 90 days.[113] FISA 1978 orders may be granted that authorise the interception of the communications of US citizens, to the extent that the FISC judge is satisfied that there is probable cause to find that that individual is an agent of a foreign power.

95. The second, more controversial, aspect of FISA 1978 arises out of a series of amendments to the Act introduced in 2008 (the FISA Amendment Act 2008 Section 702 allows the targeting of individuals "*reasonably believed to be located outside the United States to acquire foreign intelligence information*" without the same degree of judicial scrutiny.[114] Under s702, the Attorney General and the Director of National Intelligence may jointly authorise that targeting for a period of up to one year. Acquisition of data via this route may not intentionally target:

(a) Any person known to be located in the United States;

(b) A person outside of the United States in order to target a person reasonably believed to be in the United States;

(c) A United States person reasonably believed to be outside the United States; or

(d) Any communication as to which the sender and recipients are all known to be inside the United States.

96. The basic mechanics of s702 are:

(a) The Attorney General and Director of National Intelligence draw up a certificate identifying categories of foreign intelligence that they wish to collect (for example email addresses of suspected terrorists overseas). Those certifications do not contain the level of specificity as to the individual targeted that is required under a normal FISA 1978 order;

(b) The certification must set out the targeting procedures that will be used. They must be "*reasonably designed"* to ensure that the material acquired is "*limited to targeting persons reasonably believed to be located outside the United*

111 50 U.S.C. § 1804 (a).
112 See: 50 U.S.C. § 1801.
113 50 U.S.C. § 1805.
114 50 U.S.C § 1881a.

States." The certification must also attest that the Attorney General has adopted Guidelines to ensure compliance with the s702 framework.

(c) A judge of the FISC reviews the minimisation and targeting provisions of those certifications before they are implemented. They must be satisfied that the targeting procedures are "*reasonably designed*" to meet the objectives set out above.[115] The presiding judge writes an opinion setting out why he or she considers that the procedures meet that standard and also why they comply with the First Amendment right to free speech.

(d) However, the judge does not have to approve the targeting decisions: they do not have to satisfy themselves that the target (or targets) are a foreign power or agents of a foreign power.[116]

(e) The NSA have published a fact sheet on their minimisation procedures, which provides that inadvertently acquired communication of or concerning a US person must be promptly destroyed if it is neither relevant to the authorised purpose or evidence of a crime.[117]

97. The Inspector General assesses compliance with the procedural requirements and reports on them on an annual basis to Congress. The Attorney General also submits a report to Congress each year setting out the number of applications and extensions of s702 surveillance certificates and the number of those orders or extensions granted, modified or denied.[118] He also submits a semi-annual assessment to three Congressional select committees concerning all electronic surveillance under s702.[119]

98. Section 702 provided the basis for the US Government to carry out its PRISM and Upstream collection programs (described more fully at Annex 7 to this Report).

99. A third, and equally controversial, aspect of FISA 1978 is Subchapter IV: Access to Certain Business Records for Foreign Intelligence Purposes (known as s215). It provides that the Director of the FBI, or a designee, may make an application for an order requiring the production of any "*tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities*."[120]

100. An application under s215 should be made to the FISC and include a statement of facts showing that there are reasonable grounds to believe that the things sought are relevant to an authorised investigation.[121] If the court is satisfied that that is the case, it will issue an order that describes the tangible things that must be provided "*with sufficient particularity to permit them to be fairly identified*."

115 50 U.S.C. § 1881a (i) (2)(B)(i)
116 50 USC § 1881a (g).
117 https://www.fas.org/irp/news/2013/06/nsa-sect702.pdf.
118 50 U.S.C. § 1807.
119 50 U.S.C. § 1808.
120 50 U.S.C. § 1861(1).
121 *Ibid*. 1861(1) (b).

101. Section 215 has become controversial in the light of the disclosures in the Snowden Documents, when it became clear that the FBI had applied, on behalf of the NSA, for orders authorising the collection of nearly all call information generated by certain telephone companies in the USA. The NSA had then queried the database of information that resulted by enquiring for all calls to or from telephone numbers in respect of which there was a "*Reasonable Articulable Suspicion*" that it was associated with terrorism (the seed number). The NSA then operated a system known as contact chaining whereby all persons in contact with the seed number - the first hop - all numbers directly in contact with the first hop numbers (the second hop) and all numbers in contact with those second hop numbers as well (the third hop) could be accessed and stored.[122] The judges of the FISC had authorised that program pursuant to a series of 90 day orders.

102. Finally, EO 12333 provides an extra-statutory basis for the intelligence services to carry out interception of communications. It was first issued in 1981 and has been amended on three occasions since. Part 1 of EO 12333 sets out the various roles of the intelligence bodies in the United States. Part 2 includes a broad power to collect information. Comparatively little is known about the use of those powers. If it is relied upon as a basis for carrying out interception, the intelligence agencies may do so without judicial authorisation.

Oversight

103. The intelligence services in the United States are subject to multiple forms of oversight. In 2007 Congress established a Privacy and Civil Liberties Oversight Board to review and oversee civil liberties in the context of national security. The Board has published two report. Its first, in January 2014 concerned the "*section 215 program*" and held that it did not comply with the statute itself. In particular, the Board held that the program had been authorised by reference to counter-terrorism investigations in general, and not a specific authorised investigation (as required). They also expressed their serious reservations about whether or not it complied with the Constitution.[123] A second report in July 2014, concerning s702 concluded that certain historical programs "*push the program close to the line of constitutional reasonableness."*[124] However, they concluded that the program was, in broad terms, lawful. Both Houses of Congress also provide legislative oversight in the form of a permanent select committee on intelligence.

104. A separate President's Intelligence Oversight Board reports directly to the President on potential violations of the law committed by the Agencies. Many of the Agencies themselves also contain an Office of Inspector General, with a remit to review compliance internally.[125]

---

122 Following a change in 2014 the FISC now has to approve RAS determinations before contact chaining may be carried out.

123 http://www.fas.org/irp/offdocs/pclob-215.pdf. That was a view shared by the President's Review Group on Intelligence and Communications Technologies, p. 85. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

124 http://www.pclob.gov/library.html page 9.

125 17th Report of Session 2013-14, HC231 (May 2014), p. 92.

Annex 16: POTENTIAL USE OF TRAFFIC DATA BY LOCAL AUTHORITIES

1. The information in this Annex derives from evidence to the Review from Hampshire County Council officers, March 2015.

Cold calling fraud

2. In April 2012 Mr V was arrested at a house where a consumer had been defrauded of a considerable amount of money. Other persons ran away and could not be identified.

3. From itemised billing checks on Mr V's telephone number, it was established that Mr V had been in regular contact with a Mr A. Itemised billing for Mr A's phone number showed a pattern of contacts with Mr V.

4. Some time later Mr A was arrested, but on interview he denied being present at the address and he claimed that someone else had asked him to cash a cheque that had been written by the consumer. Nothing could be proved to the contrary.

5. Only Mr V was able to be prosecuted for the fraud offences and he was eventually given a suspended sentence of 15 months imprisonment plus community service. He was also given a 7 year Criminal Anti Social Behaviour Order [**CRASBO**] banning him from being involved in cold calling anywhere in England and Wales.

6. All that could be proved against Mr A was a money laundering offence and he was just given a sentence of 140 hours community service. The local authority was unable to apply for a CRASBO against him, as they could not place him at the scene.

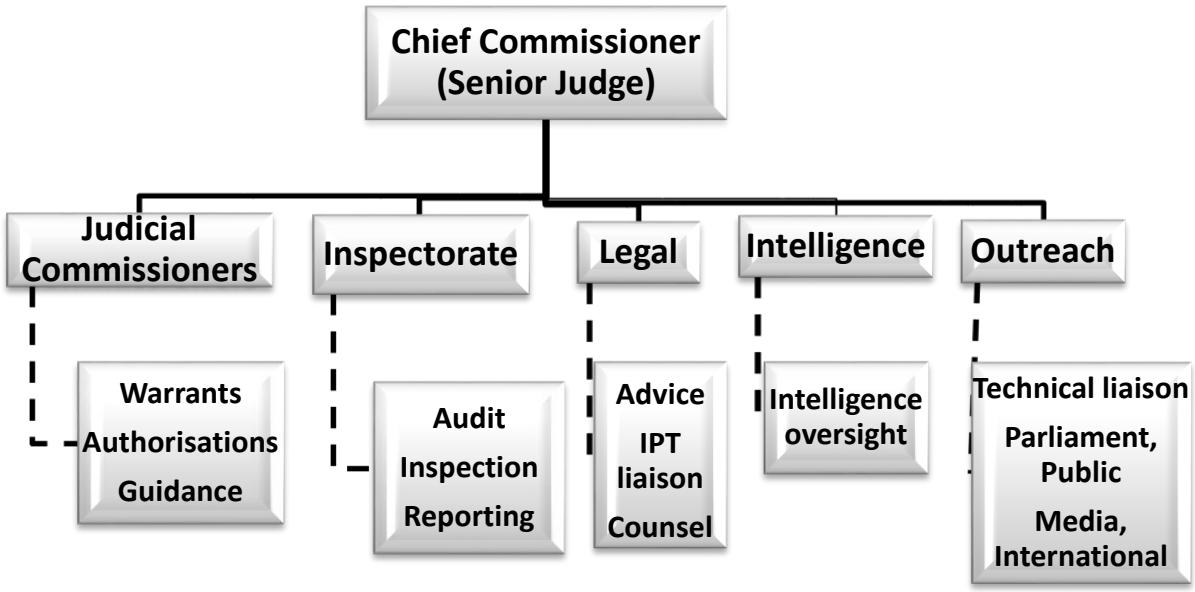
7. Had the local authority been able to access traffic data they would have checked location data for Mr A's phone, which would have been likely to show he had been in the vicinity at the consumer's house at the time of the offences. If this had been established this would have enabled them to prosecute him for the fraud offence and quite possibly to have used a conspiracy charge involving both men. If there had been a successful fraud prosecution, this would have resulted in a CRASBO being obtained against Mr. A. The CRASBO would have protected vulnerable consumers in general, since he would be liable to arrest if he was caught cold calling anywhere, even if no fraud was provable.

Counterfeit goods

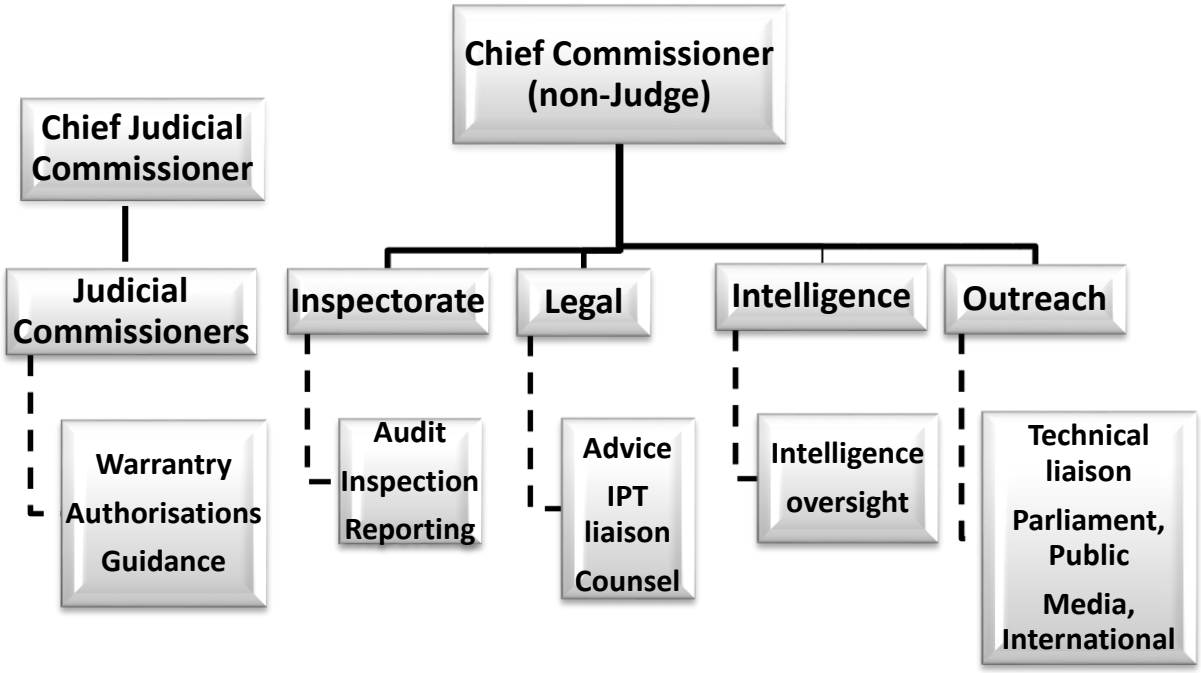
8. In a number of cases, a local authority has seized counterfeit goods from persons who are selling them locally, but appear to be obtaining them from other persons further up the distribution chain. The defendants have claimed not to know the name or phone number of their supplier, because he just rings them when he is about to deliver more stock. Consequently the local authority is usually only able to prosecute the person from whom the items were seized. If they were able to access traffic data they could use this to obtain incoming calls data for the defendant's phone to try to identify the supplier. This would otherwise not be possible as the defendant was not making phone calls to the supplier. Rather than just prosecuting the persons at the bottom of the

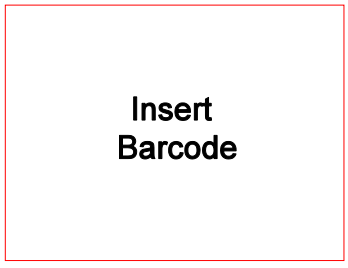
distribution chain, they would be able to prosecute the distributors who would also be supplying counterfeit goods to other persons in the locality and making greater profits.

Annex 17: Independent Surveillance and Intelligence Commission (ISIC) Model A



Annex 18: Independent Surveillance and Intelligence Commission (ISIC) Model B




Insert
Barcode