LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's response to the Investigatory Powers Commissioner's informal consultation on bulk powers

June 2018

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research. Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Corey Stoughton
Advocacy Director
Direct Line: 020 7378 3667
Email: coreys@libertyhumanrights.org.uk

Rachel Robinson
Advocacy and Policy Manager
Direct Line: 020 7378 3659
Email: rachelr@libertyhumanrights.org.uk

Gracie Bradley
Advocacy and Policy Officer
Direct Line: 020 7378 3654
Email: gracieb@libertyhumanrights.co.uk

Sam Grant
Advocacy and Policy Officer
Direct Line 020 7378 5258
Email: samg@libertyhumanrights.org.uk

Hannah Couchman
Advocacy and Policy Officer
Direct Line: 020 7378 3255
Email: hannahc@libertyhumanrights.co.uk

Zehrah Hassan
Advocacy Assistant
Direct Line: 020 7378 3662
Email: zehrahh@libertyhumanrights.org.uk

Introduction

Liberty advocates for the lawful, targeted and proportionate use of intrusive powers to detect and prevent serious crime. We believe that the mass speculative interception of communications, retention and acquisition of communications data, bulk hacking and bulk personal dataset (*"BPD"*) acquisition is unlawful, unnecessary and disproportionate.

There is no statutory definition of 'bulk'. The *Bulk Personal Dataset Factsheet* that was released alongside the original Investigatory Powers Bill described bulk powers as involving the availability of "information about a wide range of people, most of whom are not of interest to the security and intelligence agencies".[1]

The closest the Investigatory Powers Act (*"the Act"*) comes to defining bulk is contained in Part 7, where BPDs are defined as "*a set of information that includes personal information relating to a number of individuals where the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service."* [2]

The powers outlined under the Act licence surveillance on a disproportionate scale, placing those charged with issuing and reviewing warrants in the position of either impugning the fundamental aims of the legislative scheme, or accepting the highly dubious premise that routine, daily, surveillance of billions of communications can amount to a proportionate action. Liberty therefore believes that it is impossible for judicial commissioners to consider the conduct permitted under a bulk warrant as proportionate.

As technological capabilities continue to expand, so too do our ways of communicating. These developments, which see much of our communication take place electronically, undoubtedly make mass surveillance easier and more affordable – but it will never be proportionate in a democratic society during peacetime to mass collect, monitor or process innocent communications in order to find those that threaten our security.

Mass surveillance and rights

Mass surveillance represents an unjustified interference with Article 8 rights[3]. In a deeply alarming departure from established common law and human rights law principles, bulk warrants may be targeted at an entire telecommunications system or complete populations rather than specific, individual people. Bulk interception means that billions of communications are being intercepted each day without any requirement of suspicion, or even a discernible link to a particular operation or threat.

The Government has previously attempted to argue that bulk interception is not intrusive if it is carried out by machines rather than humans – an analysis which is profoundly concerning, and speaks to a lack of understanding of what it means for something to be kept private. Automated State interception of communications and the acquisition of communications data is not a passive or innocuous process. The State cannot physically intercept a communication in a way that doesn't interfere with privacy simply because it claims that human eyes may not see it.

[1] *Bulk Personal Dataset Factsheet* accompanying the Investigatory Powers Bill – Home Office, March 2016
[2] Investigatory Powers Bill 2016, Clause 182.
[3] Article 8 of the European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society".

Mass surveillance also engages the right to freedom of opinion and expression, the right to seek, receive and impart information and the right to peaceful assembly and association. For example, mass surveillance in the context of protest can lead to a chilling effect. Those with a legitimate and lawful interest in expressing dissent may feel watched or monitored to such an extent that they are deterred from attending protests and other gatherings, again emphasising the disproportionate impact of bulk powers.

Relevant Case Law

The European Court of Human Rights ("**ECtHR**") has made it clear that the principal test in relation to these matters and their compatibility with Article 8 is that *"powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures…"*[4]

In particular, the ECtHR's decisions in *Zakharov*[5] and *Szabó*[6] established that, for a surveillance law to be foreseeable (i.e. readily available and clear to citizens) and therefore compatible with Article 8, it must provide for individual targeting; in other words, an order or other act permitting surveillance must be limited to an identified individual or set of premises or, perhaps, single operation or investigation. Secondly, surveillance must be permitted only if there is a reasonable suspicion, on a sufficient factual basis, that the person about whom information is sough is engaging in acts that justify the imposition of surveillance (e.g. that he/she has or will engage in serious crime).

For obvious reasons, bulk surveillance fails to meet those requirements, enshrined in human rights law, that surveillance be individualised and based on reasonable suspicion, and as a result it is unlawful. The Judicial Commissioners cannot therefore authorise bulk warrants that will be compliant with human rights law.

Of particular relevance to the job of the Judicial Commissioners are the safeguards that are also laid out in *Zakharov* and *Szabó* in relation to the authorisation procedure for surveillance. In these cases, the ECtHR held that:

- in general, the authorisation procedure carried out by the Judicial Commissioners must be "capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration"[7]. However, the framework in which the Judicial Commissioners will carry out their review (i.e. applying only a judicial review standard, the system of urgent modifications which allows for them to be bypassed, the fact that warrants about the same persons/communications are not required to be combined, etc.) will not meet this standard. Liberty urges the Commissioners to apply a more rigorous standard of review, and for Ministers to avoid urgent modifications without approval. To the extent possible, Liberty would also urge that warrants concerning the same person/communications be combined for consideration, so that the totality of interference on an individual is assessed as necessary and proportionate;

[4] Kennedy v UK, Application no 26839/05, 2010, paragraph 153.
[5] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber)
[6] *Szabó and Vissy v Hungary* (App No 37138/14, 12 January 2016, Fourth Section)
[7] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [257].

- the reviewing authority (i.e. IPCO / the Judicial Commissioners) must be required to verify the existence of a reasonable suspicion (see above)[8] – while this is not required by the Act, the failure of the Judicial Commissioners to verify as such is contrary to human rights law;

- the request for authorisation must identify a specific person/premises to be placed under surveillance[9] – while this is not required by the Act, the failure of any warrant reviewed by the Judicial Commissioners to contain such an identification means that the warrant is unlawful and should not be authorised; and

- in conducting its review, and in particular deciding whether surveillance is necessary and proportionate, the reviewing authority must be provided with all the material before the original decision-maker[10] – the Judicial Commissioners must therefore have sight of the material that the Minister has seen.

The lack of operational case

In Liberty's view, there is no operational case for agencies to collect, process and link personal data on the entire UK population. Current law allows data to be transferred across the private and public sector to further national security and the prevention and detection of crime. Such agencies therefore already have gateway powers to obtain information on those it identifies as being subjects of interest, which is a further factor to be weighed when considering necessity.

The Government has not attempted to make a robust operational case for bulk surveillance. The bulk powers have simply been presented *as "crucial to monitor known and high-priority threats"*[11] and also *as "a vital tool in discovering new targets and identifying emerging threats"*[12].

In his July report "*Guide to Powers"*[13] David Anderson QC, Independent Reviewer of Terrorism Legislation, offered six anecdotes provided by relevant agencies in an attempt to justify mass interception. However, with the vague and limited information provided, it is impossible to assess whether the security outcomes could have been achieved by using the wealth of targeted and operation-led intrusive surveillance powers at the agencies' disposal. In nearly all of the examples, reference is made to known terrorists or a specific "intelligence operation".

Liberty would encourage judicial commissioners to consider the fact that no case has been put forward to suggest that such data collection meet this threshold of necessity and proportionality relation to Article 8. The Intelligence and Security Committee reports that intelligence agencies think BPDs are an *"increasingly important investigative tool"* to *"enrich"* information obtained through other techniques and concludes that BPDs are *"relevant"* to national security investigations[14]. In Liberty's view, an intrusive surveillance warrant which is "enriching" and "relevant" does not meet the legal threshold for lawfulness and, as such, judicial commissioners are faced with an impossible task.

[8] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [260] – [261].
[9] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [257], [264] – [265].
[10] *Zakharov v Russia* (App No 47143/06, 4 December 2015, Grand Chamber) [260] – [261].
[11] Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism, (2016*), UN High Commissioner for Human Rights*, A/HRC/33/29
[12] Guide to powers, p.20 para. 33
[13] Guide to powers, p.20 para. 33
[14] Privacy and Security: a modern and transparent legal framework-Intelligence and Security Committee, March 2015, p.55 para.153

Efficacy

Any consideration of necessity and proportionality requires an assessment of the benefit afforded by bulk powers. As such, the efficacy of bulk powers becomes a key consideration.

The available evidence indicates that mass surveillance powers have not been effective in tackling serious crime, and particularly not terrorism. Rather, there is evidence that mass surveillance practices actively impede law enforcement efforts.

For example, bulk telephone data has not proved useful for counterterrorism in the US. The Privacy and Civil Liberties Oversight Board, an independent executive branch board in the U.S., found that the bulk telephone records program conducted under Section 215 of the USA Patriot Act not only raised constitutional and legal concerns, but had no material counterterrorism value*: "Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."*[15]

Similarly, the President's Review Group on Intelligence and Communications Technologies concluded in 2013 that *"the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."*[16]

Both panels advised that the bulk surveillance program should be shut down and section 215 was allowed to expire in May 2015. The USA Freedom Act followed, reducing the capacity of the NSA to undertake mass collection of Americans' phone records, requiring instead that a subset of data be requested pursuant to limits set out in the Act.[17]

A further example comes in the form of Denmark's Data Retention Law (*Logningsbekendtgørelsen*), which was put in place from 2007 until 2014. This law required internet providers to retain internet session logs for 12 months. These logs included client and server IP addresses, port numbers, transmission protocols and timestamps.[18] A report published by the Danish Ministry of Justice in December 2012 found that several years of collecting internet session data had not yielded any significant benefits for law enforcement - session data had played a minimal role in only one case.[19] To the contrary – members of staff reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[20] In June 2014, the Danish government repealed the obligation on operators to retain session data on the basis that it was "*questionable whether the rules on session logging can be considered suitable for achieving their purpose*".[21]

---

[15] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court –Privacy and Civil Liberties Oversight Board, 23 Jan 2014, p.11

[16] Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies –12 Dec 2013, p. 104

[17] USA Freedom Act 2015, available at: http://judiciary.house.gov/_cache/files/1cb59778-0a72-4c09-920d-0e22bf692bb4/fisa-01-xml.pdf.

[18] *Logningsbekendtgørelsen 2006* (https://www.retsinformation.dk/forms/r0710.aspx?id=2445). An English translation produced by the Ministry of Justice is available at https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf

[19] *Redegørelse om diverse spørgsmål vedrørende logningsreglerne* – Justitsministeriet, Dec 2012 (http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf). There is no English translation. The article "*In Denmark, Online Tracking of Citizens is an Unwieldy Failure*" - TechPresident, 22 May 2013, discusses the report (http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy).

[20] Ibid.

[21] *Justitsministeren ophæver reglerne om sessionslogning ("The Ministry of Justice repeals the rules about session logging*) – Justitsministeriet, 2 June 2014, http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning

Furthermore, scientists have rightly condemned "how little of the debate [on mass surveillance] has dealt with the likely success of these tactics (…)", arguing that "the efficacy of such surveillance programs must be clearly understood if a rational policy is to be developed".[22] The statistics journal Chance published a paper on the risk of automatic screening processes (such as those used for bulk interception, bulk data retention and upstream collection), which concluded that whilst a 99% accurate system would indeed report on 99% of the terrorists, the margin of error would also be responsible for producing hundreds of thousands, if not millions, of reports on innocent citizens.[23] This is partly the cause of "bulk data failure" that former intelligence professionals have described.[24]

In every major terror attack in Europe and the USA since and including the 9/11 attack on the World Trade Centre – including the Madrid bombings in 2004, the London 7/7 bombings in 2005, the murder of Lee Rigby in 2013, the Boston bombings in 2013, the Charlie Hebdo offices attack in January 2015 and the Paris attacks in November 2015 – some or all of the culprits have been known to the intelligence agencies. The failure to prioritise or action intelligence appropriately is commonly attributed to both human error and pressured resources – these reasons featured in the reports on the London 7/7 bombings[25] and the murder of Lee Rigby.[26]

No evidence has been provided to illustrate a unique or critical contribution of bulk powers in combatting serious crime or indeed terrorism. Whilst in some cases bulk powers may offer helpful contributions to intelligence gathering (which would not be necessary and proportionate) they have not, as far as is publicly known, proved critical in saving lives nor unique in providing intelligence that could be otherwise acquired through targeted methods. This adds further weight to the contention that bulk powers are unnecessary and disproportionate.

Re-identification

Identifiers for a target, such as their phone number, email address or internet service provider, may change – especially if a target is seeking to evade detection. In these circumstances, the "relocation" of a target can be achieved through other known identifiers (i.e. banking records will reveal a mobile phone purchase, and it may be possible for this device to be tracked). It is also possible to – in extremis – deploy targeted equipment interference. Of course, once the personal identity of the target is known, there are a wide range of methods for establishing new communications identifiers.

Analysts can also use the target's social networks to locate alternate identifiers for the target. Where the threshold of necessity and proportionality is met, other people in contact with the target can have their communications data analysed to discover any new contact that appears in the network. As such, bulk powers are not necessary.

[22] Until proven guilty: False positives and the war on terror –Howard Wainer & Sam Savage, Chance, March 2008, 21(1), pp.59-62, https://www.researchgate.net/publication/242713602_Until_proven_guilty_False_positives_and_the_war_on_terror
[23] Ibid.
[24] See, for example, Written evidence –William Binney, 9 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocuent/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/25753.htm
[25] Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005 –Intelligence and Security Committee, 8 July 2008
[26] Report on the intelligence relating to the murder of Fusilier Lee Rigby –Intelligence and Security Committee, 25 Nov 2014

Discovery

The Home Office's *"Operational Case for Bulk Powers"* argues that bulk data mining has led to the discovery of a "*previously unknown individual*" – however, this is qualified by adding that the discovered target was in contact with "*a Daesh-affiliated extremist in Syria"*.[27] This plainly does not justify the broad bulk interception power currently provided for in the Act. On the basis of this example, a targeted SIGINT interception regime which filtered out those who were not being uniquely targeted would have yielded the same result. Targeted interception of known targets, such as the Daesh-affiliated extremist, would provide for rapid and accurate target discovery, such as the discovery of this "*previously unknown individual*".

However, targeted interception can, if dictated by policy and permitted by law, extend beyond individuals under suspicion to sites under suspicion. For example, targeted surveillance of websites, or areas of websites, hosting illegal content can reliably lead to the discovery of new suspects. Such sites or webpages can be indexed and authorised for surveillance, on the basis of reasonable suspicion, and thus used as a unique identifier to add to the signals filtering process. Again, bulk powers are not necessary.

"The Dark Web"

The Home Office's *"Operational Case for Bulk Powers"* makes the claim that 'the use of bulk data' is *"among the few effective methods available to counter the illicit use of the dark web"*.[28] The Home Office claims that data 'obtained through bulk interception' is used to identify anonymous users. However, this same information could be obtained through the targeted model of signals intelligence described above.

The infrastructure of the Tor network is such that bulk data powers – whether bulk interception, bulk CD access or proposed internet connection records – do not assist in the identification of users, whose traffic is distributed through Tor relays around the world. The only foreseeable application of bulk powers to law enforcement in this context would be an indiscriminate surveillance exercise (i.e. identifying all Tor uses), which could be both undemocratic and unnecessary. The FBI's takedown of the dark web marketplace Silk Road;[29] the prolific operation to takedown the 'Playpen' paedophilia site and identify over 1,000 of its anonymous visitors;[30] and the Australian Taskforce Argos' operation against the paedophile network 'The Love Zone', each involved the targeting of the website, the arrest and subsequent impersonation of its key facilitator, and the hacking of visitors to the site as well as other traditional investigative methods to uncover targets' real identities.

As such, the operational case for use of bulk powers in this context has not been made. Identifying all users of anonymising technologies is absolutely not necessary to deal with criminals who operate online, and would certainly not be proportionate.

[27] Supplementary written evidence to the Joint Committee on the draft Investigatory Powers Bill (IPB0165) – Theresa May, December 2015, p.8
[28] Paragraph 3.13
[29] *The Dark Web Dilemma: Tor, Anonymity and Online Policing* – Eric Jardine, Sept 2015, Global Commission on Internet Governance, p.8
[30] *FBI crack Tor and catch 1,500 visitors to biggest child pornography website on the dark web* – Mary-Ann Russon, 6 Jan 2016, IB Times, http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417

Storage

The key argument put forward in support of bulk storage is that it provides a retrospective record of activity for a person, or group of people, who are not under suspicion at the time of collection but later fall to be so.

This argument fails to acknowledge that the target themselves will hold an enormous amount of information relating to their previous communications – and an analyst will be able to access call records (which phone providers store for their own business purposes), retrieve messages or emails (which are stored on communications providers' servers), access content that is stored locally on a target's device and obtain banking and travel records.

It is, of course, the case that obtaining such information from communications service providers is not always possible – but this leaves available, in extremis, the option of targeted equipment interference.

Other options include a suspicion-led algorithm, which can recognise contacts shared by other targets as being within a zone of suspicion. It has been noted that "*if targeted collection can be done quickly and well enough, bulk information about past events may not be needed*".[31]

Confidential and privileged communications

Liberty would also advocate extreme caution around the interception of bulk data and the inevitable breach of legal professional privilege and access of material relating to journalism and so on. Bulk surveillance removes the possibility of safeguarding such communications.

As a result of proceedings brought by Liberty and others, the Investigatory Powers Tribunal disclosed in June 2015 that GCHQ had unlawfully intercepted and examined private communications of the Egyptian Initiative for Personal Rights (EIPR) and Legal Resources Centre (LRC) in South Africa.174[32] It later amended its ruling to clarify that the agency had unlawfully intercepted and examined Amnesty International's communications rather than those of EIPR.

GCHQ's activity was only deemed unlawful because the agency had breached its own internal guidance in a technical manner. The judgment provided no explanation as to why human rights NGOs had been bulk intercepted and individually examined and perversely did not find this action to amount to a breach of the ECHR.

This Act clearly permits the routine bulk interception and examination of human rights NGOs, lawyers, journalists, elected representatives and others – and, in Liberty's view, the bulk collection systems are not capable of providing sufficient protection in these situations.

Case studies and examples

The Home Office report *"Operational Case for Bulk Powers"* included anecdotal examples of the use of bulk powers in a range of contexts. One such example, as outlined above, related to a "previously unknown individual" being in contact with "a Daesh-affiliated extremist in Syria".

[31] *Bulk Collection of Signals Intelligence*: Technical Options – Committee on Responding to Section 5(d) of Presidential Policy Directive 28, 2015 (The National Academies Press), p.10

[32] The Tribunal did not make determinations concerning whether the other eight organisations had been intercepted.

This example clearly does not justify bulk interception. Robust targeted surveillance of known targets, such as Daesh-affiliated extremists, should provide for the most efficient and accurate target discovery, such as the discovery of this “previously unknown individual”.

A further example given in the same publication is the discovery that a paedophile (who was already on the Sex Offenders Register) was using illegal websites to pay for images of extreme child sex abuse. Again, robust targeted surveillance of known paedophile networks and known websites hosting illegal content reliably leads to the discovery of new suspects. Again, this scenario does not justify bulk interception of communication and emphasis the utility of targeted surveillance.

Liberty analysed a variety of case studies, provided by the Home Office in the same report, in our response to the *Terrorism Reviewer’s Review of Bulk Powers*. Each of these case studies, along with Liberty’s analysis, can be found below at Appendix A.

Conclusion

In Liberty’s view, bulk powers and the ability to collect enormous quantities if information about people who are of no interest to law enforcement or intelligence agencies is not strictly necessary for the obtaining of vital intelligence in individual operations.

ANNEX A

Taken from Liberty's submission to the Terrorism Reviewer's Review of Bulk Powers (2016)[33]

An Analysis of the Government's 'Operational Case for Bulk Powers'

The Home Office published a 47-page 'Operational Case for Bulk Powers' on 1 March 2016 as an accompanying document to the Investigatory Powers Bill. For that reason, the Act is referred to as a Bill throughout.

The document presents 'a series of examples and case studies to illustrate the value of (bulk) powers' to the security and intelligence agencies.

Upon examination, Liberty would conclude that none of these case studies provide evidence to meet the requisite threshold of necessity and proportionality.

Bulk Interception

Case Study: Counter-Terrorism
The security and intelligence agencies' analysis of bulk data uncovered a previously unknown individual in 2014, in contact with a Daesh-affiliated extremist in Syria, who was suspected of involvement in attack planning against the West. As this individual was based overseas, it is very unlikely that any other intelligence capabilities would have discovered him. Despite his attempts to conceal his activities, the agencies were able to use bulk data to identify that he had recently travelled to a European country. Meanwhile, separate intelligence suggested he was progressing with attack planning. The information was then passed by the agencies to the relevant national authorities. They disrupted the terrorists' plans and several improvised-explosive devices were seized.

Analysis
This case study describes the use of bulk interception for target discovery, and the subsequent discovery of the target's recent travel to Europe.

Targets can be discovered by contact chaining - using a 'seed' identifier belonging to a known target to map their social network and discover further subjects of interest. This case study describes the 'previously unknown individual' as discovered to be 'in contact with a Daesh-affiliated extremist in Syria'. Using the Daesh-affiliated extremist as a seed, further valuable targets can be discovered – however, this does not necessitate bulk interception.

Maintaining a rich store of targeted data, analysts can build social networks based on relationships in a variety of metadata such as phone numbers, email addresses, credit cards, money transfers, travel arrangements, and so on. Such networks can grow around targets without also collecting data on entirely unrelated individuals of whom there is no suspicion - bulk collection is *not* necessary for contact chaining. Targeted interception can be conducted within the framework of covert signals intelligence – it does not necessarily require the co-operation of overseas telecommunications operators. Contact chaining through such targeted interception leads to the discovery of valuable targets and the rapid onset of further collection on newly discovered targets.

[33] Accessed at: https://www.libertyhumanrights.org.uk/sites/default/files/campaigns/resources/Liberty%27s%20submission%20to%20the%20Terrorism%20Reviewer%27s%20Review%20of%20Bulk%20Powers.pdf

This case study does not provide evidence of the necessity of bulk interception, as the intelligence aims are equally met by targeted interception.

Case Study: Disrupting Child Sexual Exploitation

In 2013, the agencies carried out analysis of bulk data to identify patterns of behaviour used by paedophiles on-line. They identified a UK national visiting a website that sold images of child sexual exploitation. The website was hosted in a country that rarely cooperated with UK law enforcement and without the analysis of bulk data the individual's use of the website would have escaped detection. The individual had previously held a position that provided him with access to children, and he was already on the UK Violent and Sexual Offenders register. Due to the security and intelligence agencies' work he was prosecuted for his actions, sentenced to three years' imprisonment and made subject to a Sexual Offenders Harm Order for life.

Analysis

This case study describes the use of bulk interception for the disruption of a sex offender's online activity.

A claim is made that, 'without the analysis of bulk data the individual's use of the website would have escaped detection'. However, targeted interception can be used to collect information on the use of websites that are under suspicion, to promote target discovery. The targeted surveillance of websites or areas of websites that sell images of child sexual exploitation, or host illegal content, leads to the discovery of targets. Such sites or webpages can be indexed and authorised for surveillance, on the basis of reasonable suspicion, and thus used as a unique identifier to add to the signals filtering process.

This case study does not provide evidence of the necessity of bulk interception, as the intelligence aims are equally met by targeted interception.

Case Study: Protecting the UK from cyber attack

The security and intelligence agencies routinely use bulk interception to detect cyber-attacks against the UK, including large scale thefts of data and serious fraud by cyber criminals, and operations by hostile intelligence services and potential terrorists. Using electronic 'signatures', which operate in a similar way to electronic fingerprints, the agencies scan the technical detail of internet communications for evidence of incoming attacks to the UK. This approach can both identify known forms of computer malware and discover new forms of cyberattack that the agencies have not previously encountered. Cyberspace is so large, and technical change so rapid, that bulk interception is the only way for the agencies to monitor for such attacks as they occur: targeted approaches would be highly likely to miss an attack. The resulting intelligence is typically shared with industry partners, who in turn use it to protect UK citizens and businesses.

Analysis

Given the extremely vague nature of this example, it is not possible to analyse it in any detail. However, the case study manifestly fails to justify the necessity of bulk interception of communications. The nation's cybersecurity relies on the robust defence of networks involved in our critical national infrastructure; secure online platforms protected by strong encryption; the promotion of industry-wide security standards; trust in UK software, internet and communications service providers; public education in online safety; and effective law enforcement concerning criminals who operate online.

Protecting the nation's cybersecurity relies largely on the protection of critical networks rather than limitless bulk surveillance of communications. The case study describes how 'the agencies scan the technical detail of internet communications for evidence of incoming attacks to the UK'. Even if such an approach is adopted, 'scanning' (filtering) data flowing

through intercepted bearers for information of which there is reasonable suspicion of serious crime or threats to national security results in *targeted* interception – not bulk interception which involves more indiscriminate 'scanning' and the collection of bulk data, the majority of which is unrelated to serious crime.

Bulk Equipment Interference

Example: Protecting Against a Terrorist Attack
A group of terrorists are at a training camp in a remote location overseas. The security and intelligence agencies have successfully deployed targeted EI against the devices the group are using and know that they are planning an attack on Western tourists in a major town in the same country, but not when the attack is planned for. One day, all of the existing devices suddenly stop being used. This is probably an indication that the group has acquired new devices and gone to the town to prepare for the attack. It is not known what devices the terrorists are now using. The security and intelligence agencies would use bulk EI techniques to acquire data from devices located in the town in order to try to identify the new devices that are being used by the group. If it is possible to identify those devices quickly enough, it may be possible to disrupt the attack. Without bulk EI powers, it is very unlikely that this would be achievable.

Analysis
This hypothetical case study aims to demonstrate the necessity of bulk equipment interference in an overseas counter-terror operation. A hypothetical case study does not constitute evidence or an operational case. It certainly doesn't meet the factual and legal test of strict necessity.

The targets in this scenario are known as they are under intrusive surveillance with the use of targeted equipment interference. Depending on the device, this could allow investigators to discover the identities of the individuals, track their location and locations visited (allowing further intelligence and potentially CCTV gathering), listen in to their conversations and/or capture images either by intercepting calls or remotely activating the microphone and/or camera, retrieve other identifiers relating to the targets such as phone numbers, email addresses, other device identifiers etc., access all communications, contacts, images and stored data on the device, map the user's communication network, access any registered address and bank details associated with the device.

The investigators are aware that the cell is planning an attack on Western tourists. Given the certainty of that assessment, and the risk that the attack could occur at any time, there would be good cause to dispatch physical surveillance or otherwise urge law enforcement to intervene immediately. In the event that the surveilled devices cease being used before the opportunity to urgently intervene, the investigators would need to identify the new devices – the example suggests that intelligence agencies would do so by using bulk equipment interference, i.e. by hacking all the devices in the town. However, the question remains how investigators would identify the new devices. This is not a new problem. Intelligence agencies identify the new phones of a suspect who uses burner phones by using the tracked device and data gathered from it as a seed: for example, by tracking proximal devices to the target device (which may be the new phone); or by investigating any contact to the target's network from new numbers or devices; even using algorithms to scan social networks within the zone of suspicion for similar call patterns to that associated with the target device when it is 'dropped'.[34] These methods do not involve bulk equipment interference.

[34] See NSA programs PROTON and CRISSCROSS, https://theintercept.com/document/2014/08/25/crisscross-proton-point-paper/

This hypothetical example does not provide evidence of the necessity of bulk equipment interference. It is clear that, in this dramatic scenario, human life would be best protected by intervention upon discovery that a group of terrorists are at a training camp and that the cell is planning to attack Western tourists at any time. Failing timely intervention at the point at which sufficient evidence would exist both to prevent an attack and pursue a prosecution, a range of targeted methods would be at the agencies' disposal in order to allow them to rediscover targets that they have previously gained a wealth of information about.

Example: Countering Biological Weapons Proliferation
A hypothetical totalitarian state has an indigenous email system which is mandated for use by the general population, but also by scientists working on the state's biological weapons programme who are involved in the proliferation of weapons technology. This means it is used by many thousands of people within that country. The security and intelligence agencies can only obtain limited data from interception which means it is not possible to identify particular accounts which belong to individuals of intelligence interest working on the biological weapons programme. Bulk EI techniques would be needed to access a limited amount of data relating to a very large number of users of the service – potentially even all its users. This would enable the security and intelligence agencies to filter out those who were not of intelligence interest, and focus on those who were associated with the biological weapons programme in order to use targeted EI techniques against them to support the UK's aim of disrupting their proliferation of biological weapons.

Analysis
This hypothetical scenario claims that bulk equipment interference compromising the security of an entire population's email communications would be the necessary and proportionate action to identify suspected scientists.

In this hypothetical scenario, it may be appropriate to gather further intelligence through targeted techniques and human sources but it is plainly not strictly necessary to deploy equipment interference powers at such an extraordinary scale. It is highly unlikely that such population-level intrusion could be justified as strictly necessary against another sovereign state with which we are not at war – intelligence should at the very least narrow the investigation to equipment in a specified location, in which case a targeted equipment interference warrant may be deemed necessary and proportionate to meet the legitimate aim of curtailing an identified threat to life or protecting national security.

This hypothetical scenario does not provide evidence of a proportionate or necessary use of equipment interference powers, and does not support the case for bulk equipment interference powers.

Example: Cyber Defence
A state controlled agent provides the infrastructure to several other state controlled malicious Computer Network Exploitation (CNE) programmes. These programmes are responsible for espionage against the Government and UK industry at massive scale. The security and intelligence agencies' ultimate aim would be to identify that agent and any others supplying infrastructure to the programmes in order to find any of the new computer equipment before it is used. In order to do this the security and intelligence agencies would need to use bulk EI to survey a location from where they believe the infrastructure is being procured, in order to identify activity characteristic of the procurers. In order to find these individuals, the security and intelligence agencies would need to acquire a large amount of data from which to identify likely candidates, who would then be subject to more targeted intelligence investigation.

Analysis

There is too little detail in this hypothetical example to either take it as evidence of the necessity of bulk equipment interference, or indeed to analyse it in great detail.

The example describes counter-espionage and cyber defence efforts. Bulk equipment interference would allegedly be needed to 'survey a location from where they believe the infrastructure is being procured'. It is unclear how bulk equipment interference would support the agencies in such a vaguely described activity as 'surveying a location'.

Reporting on the draft Investigatory Powers Bill, the Intelligence and Security Committee recalled that in oral evidence "*the Director of GCHQ suggested that, hypothetically, a Targeted EI warrant could cover a target as broad as an entire hostile foreign intelligence service".*[35] Therefore, it would appear that a targeted equipment interference warrant would serve the purpose of such state level, counter-espionage operations. This hypothetical case study does not provide evidence of the necessity of bulk equipment interference powers.

Bulk acquisition

Case Study: Protecting Northern Ireland
Within the last three years, a group of terrorists were planning an attack in Northern Ireland. It was suspected that they had already obtained explosives for the attack and were escalating their activity. Increased activity often indicates that an attack is close, but in this case the exact date was not known and the group's attention to security made it extremely difficult to discover more. Bulk communications data provided the breakthrough. Through interrogation of the data, the security and intelligence agencies found previously unknown members of the network and were able to increase their coverage of this expanded group. As a result they became aware of a sudden further increase in activity from analysis of the group's communications activity. This led to police action and the recovery of an improvised explosive device. It was clear that the device was ready for use and the increased activity was most likely late-stage preparation for the attack. The security and intelligence agencies' work, built upon analysis of bulk communications data, provided sufficient grounds for the police to arrest a key figure in the plot, who was subsequently charged and convicted with terrorism offences.

Analysis
This case study describes the use of bulk acquisition of communications data in target discovery.

Targets can be discovered by contact chaining - using a 'seed' identifier belonging to a known target to map their social network and discover further subjects of interest.
Maintaining a rich store of targeted data, analysts can build social networks based on relationships in communications data. Such networks can grow around targets without also acquiring data on entirely unrelated individuals of whom there is no suspicion - bulk acquisition is *not* necessary for contact chaining through communications data.

An alternative approach would involve the Intelligence agencies issuing requests for targeted retention and access to the suspects' CD . Through 'interrogation of the data', as described in the case study, further subjects of interest can be discovered and additional data acquisition warrants for data relating to those individuals can be issued. However, this results in a store of targeted communications data - it is not necessary to retain or acquire the communications data of all the citizens of a nation in order to discover members of one terrorist cell.

[35] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; para. 14.

This case study does not provide evidence of the necessity of bulk acquisition, as the intelligence aims are met by the targeted acquisition of communications data.

Case Study: Preventing bombings in the UK
In 2010, a group of terrorists were plotting bombings at several symbolic locations in the UK, including the London Stock Exchange. Following an intensive investigation, in which analysis of bulk communications data played a key role, not least as the network was spread across multiple locations, the group were all identified and their plot uncovered. The investigation required the complex analysis of large volumes of data in order to identify the attackers and to understand the links between them; it would not have been possible to do this at speed by relying on requests for targeted communications data. The security and intelligence agencies were then able to work with police to disrupt them in time and the group were charged with terrorism offences, including conspiracy to cause an explosion. All entered a guilty plea and were sentenced to prison terms of up to 18 years.

Analysis
This case study describes the use of bulk acquisition of communications data in target discovery and the rapid mapping of a social network.

In this case study, it is claimed that 'it would not have been possible to do this at speed by relying on requests for targeted communications data'. Yet, targeted CD retention notices and access requests can ensure that relevant data is received in an urgent manner. Judicial warrants are not currently required, but even if they were - as Liberty advocates- in a fast moving counter-terror operation such as this there may be little time to seek warrants for individuals' communications data from selected communications service providers and so in such instances, urgent warrants – such as those available for targeted interception - would be appropriate. In this case it is essential to map the targets' social networks, so a series of warrants or urgent warrants would need to be sought, as contacts with the seeds, particularly those shared by the seeds, will rapidly become of interest.

In a priority counter-terror investigation such as this, it is highly likely that targeted interception would be an appropriate measure, in addition to accessing communications data. In addition to content, targeted interception provides a rich set of communications data that can be used for contact chaining in order to 'identify the attackers and to understand the links between them', as described in the case study. This is described at length in our report, *Bulk Surveillance Powers: Exploring the Technical Necessity and Technical Options.*
This case study does not provide evidence of the necessity of bulk acquisition, as the intelligence aims are met by targeted interception, and could be combined with the urgent acquisition of targeted communications data.

Case Study: Thwarting mass casualty attacks against aviation
In 2006 a group of terrorists based in more than one part of the UK plotted to bring down multiple aircraft using homemade bombs (improvised explosive devices). If successful, their plan would have been the largest terrorist attack ever to take place in the UK, with a death toll similar to the 9/11 attacks in the United States. The security and intelligence agencies used bulk communications data to find these terrorists and disrupt their plan. This required the complex analysis of large volumes of data in order to identify the attackers and to understand the links between them; it would not have been possible to do this at speed by relying on requests for targeted communications data. Those planning the attack were arrested, tried and sentenced to life imprisonment.

Analysis
This case study reports that the agencies 'used bulk communications data to find these terrorists and disrupt their plan'.

It is unclear how bulk communications data was used to identify the cell, as no information is given about the source of the seed. However, we know that contact chaining and identifying social networks works in the same way with a targeted approach to communications data as a bulk approach, as a rich subset of relevant communications data is required.

In this case study, it is again noted that 'it would not have been possible to do this at speed by relying on requests for targeted communications data'. Again, multiple, targeted, retention notices and requests for communications data can be executed in an urgent manner - even if a requirement for prior judicial authorisation was introduced, urgent warrants would be appropriate here, or indeed targeted interception of SIGINT to rapidly map metadata and gain further insight to the group.

As with the previous case study, this does not provide evidence of the necessity of bulk acquisition of communications data, as the intelligence aims could be met by targeted interception and combined with the urgent acquisition of targeted communications data if necessary.

Case Study: Preventing a kidnap
The security and intelligence agencies uncovered a plot by known terrorists to stage a kidnap. This plan was still in the early stages, which meant that immediate efforts to arrest the plotters risked not having sufficient evidence to convict them successfully. On the other hand, if the police and intelligence agencies had acted too late, the group might have been able to carry out their plan. A solution was therefore required which balanced these two risks.
The security and intelligence agencies were able to use communications data to analyse patterns of communications between members of the group. This enabled them to assess the risks, so that appropriate action could be taken to ensure the safety of the potential victim and their family, who were relocated while the investigation continued. The group were prevented from carrying out their plan and those who had been targeted were able to return home.

Analysis
This case study does not attempt to justify the acquisition of bulk communications data, but demonstrates the utility of targeted communications data. The agencies 'uncovered a plot by known terrorists' and 'were able to use communication data to analyse patterns of communications between members of the group'.

This case study does not support the necessity of bulk communications data.

Catching and prosecuting attackers
Example 1: Following a failed terrorist attack in London in 2007, the security and intelligence agencies were able to confirm that the perpetrators were the same as a group who had carried out another attack shortly afterwards. This was achieved in a matter of hours through the analysis of bulk communications data, and was vital in understanding the scale of the threat posed in a fast-moving post-incident investigation, because of the ability to identify connections at speed; it would not have been possible to do this at speed by relying on requests for targeted communications data.
Through further analysis of communications data, the investigation went on to identify people who had had extensive contact with telephones used in the London attack. This enabled the security and intelligence agencies and police to establish at speed, that no further attacks were planned. The operation led to a successful prosecution.

Example 2: A group of terrorists were planning to kidnap and murder a British Muslim solider in the UK in 2007. They intended to video the soldier's death and send the film to their

terrorist contacts abroad for public release. Bulk communications data allowed the security and intelligence agencies to identify the group from patterns of communication activity. This paved the way to the police searching their properties, where a number of items were recovered which confirmed they had indeed been planning a kidnap and murder. This resulted in successful convictions. Bulk communication data was critical to this outcome. As the group was unknown at the outset of the investigation, relying on targeted data would have required the security and intelligence agencies to proceed much more slowly in order to identify potential members of the group and to discount others from their investigations. The ability to analyse bulk data meant that this process was faster and more effective.

Analysis
Example 1: Again, this case study does not justify the acquisition of bulk communications data, but demonstrates the utility of targeted communications data and contact chaining. Given the rapid development of the investigation, urgent targeted CD retention notices and access requests would be appropriate, or indeed targeted interception of SIGINT to rapidly map metadata and gain further insight to the group and its network.

Example 2: This example is too vague to analyse in any detail or to consider as evidence of the necessity of bulk communications data acquisition – no information is given as to how the group was identified from bulk communications data. The need for rapid analysis is used as justification for bulk communications data again here – although, as established, urgent targeted CD retention notices and access requests and targeted use of SIGINT supports rapid target discovery and network mapping.

Bulk Personal Datasets (BPDs)

Case Study: Focusing investigative resources
Intelligence indicated that a partially identified associate of a known subject of interest aspired to travel to Syria for extremist purposes. Using BPD, agency analysts were quickly able to identify the associate, enabling rapid focus of investigative effort on the one individual of concern and discounting hundreds of other potential candidates. Without access to BPD, a resource intensive and more intrusive process would have been needed to identify the individual from the hundreds of potential candidates, incurring collateral intrusion into individuals of no intelligence interest and with significant risk of failing to identify the individual prior to travel.

Analysis
There is too little detail in this example to either take it as evidence relating to the necessity of bulk personal datasets, or indeed to analyse it in any detail. It is difficult to know in what circumstances intelligence could be held that a partially identified associate of a known subject of interest 'aspires' to travel to Syria for extremism purposes, and yet completion of their identity would involve intrusion into hundreds of potential candidates without BPDs. It should also be noted that the collection, retention, processing and searching of BPDs is also an incredibly intrusive exercise that could involve the data of millions of people. The assertion in the example that the use of potentially population level databases is a lesser collateral intrusion than targeted methods to complete the identification of one subject of interest is questionable, certainly in the context of the inadequate explanation provided.

This case study does not provide evidence of the necessity to acquire bulk personal datasets.

Case Study: Identifying foreign fighters
Timely access to travel data has provided advance notice of the unexpected return to the UK of people judged to pose a potential threat to UK security. This helps the security and intelligence agencies to prepare a tailored response prior to their arrival to better mitigate the

threat they pose to national security. Information derived from travel data has also been critical to the ability of the security and intelligence agencies and their international partners to identify individuals travelling to join Daesh in Syria and Iraq and then disrupt their activities, including when they return to the UK radicalised.

Analysis
Our intelligence agencies may wish to know the travel movements of people judged to pose a threat to UK security – particularly when they are returning to the UK. This is important for the protection of national security. However, this function – which is already undertaken via the e-borders scheme - does not necessitate BPDs, which are almost limitless and present an intrusion to millions of people's private lives. Travel data is legitimately held and shared between countries without the need for broad BPD powers.

Case Study: Identifying subjects of interest
The name of an individual reported to be storing a weapon used in a terrorist attack was identified by the security and intelligence agencies. A combination of BPD were used to fully identify this person from hundreds of possible candidates. This resulted in the recovery of the weapon, and aided in the subsequent conviction of the individuals involved in the terrorist attack, who are now serving lengthy prison sentences.

Analysis
This case study seeks to justify BPD powers for the purpose of fully identifying a named suspect. It is unspecified what 'combination of BPD' was used so there is too little information to constitute evidence of strict necessity either for the particular BPDs in question or the BPD powers in general. Depending on which country this investigation took place, it is very possible that local intelligence agencies or law enforcement would be able to assist in further identifying the named individual. It is also possible that the agencies would be able to complete the identification using open source intelligence or indeed human intelligence, as they had the suspect's name. This case study does not provide evidence that the extremely broad, almost limitless BPD powers in the Investigatory Powers Bill are necessary.

Case Study: Preventing terrorist access to firearms
The risks of terrorist access to firearms have been highlighted by tragic events in Mumbai, Copenhagen and more recently Paris. To help manage the risk of UK based subjects of interest accessing firearms, the security and intelligence agencies match data about individuals assessed to have access to firearms with records of known terrorists. To achieve this, the security and intelligence agencies acquired multiple datasets that contained the details of individuals who may have access to firearms, even though the majority will not be involved in terrorism and therefore will not be of security concern. This allows the matching to be undertaken at scale and pace, and more comprehensively than individual requests could ever achieve. This in turn has enables the security and intelligence agencies to manage the associated risks to the public.

Analysis
It is important that the security and intelligence agencies have information of which individuals have access to firearms in the UK. Firearms in the UK are held only on license, and the Home Office holds datasets of firearms licensees and certificate holders.

Keeping records of who has access to firearms does not necessitate the power to collect BPDs as it is currently so broadly drafted - an almost unlimited power involving far more expansive and intrusive, yet entirely secret, databases of integrated information on millions of people, potentially at the population-level. This case study does not provide evidence of the necessity to acquire bulk personal datasets for the purpose of preventing terrorist access

to firearms, as the relevant data is already legitimately required by law to be held by the Home Office without the need for broad BPD powers.

Case Study: Identifying human intelligence agents
The security and intelligence agencies were tasked by the UK's Joint Intelligence Committee to produce intelligence on a specific country threatening the UK's national security. They identified an individual with access to the required intelligence, but were unable to approach the individual directly due to the risk the individual would face from his country's own internal security service. Intelligence reporting showed that the individual was in contact with another person that the UK agencies might be able to approach with lower risk. The reporting, however, did not fully identify who this contact was. The security and intelligence agencies used BPD to identify that contact conclusively, enabling them to determine that they could safely approach the contact and seek support. The contact has been successfully recruited as an agent to help collect intelligence and protect the UK's national security.

Analysis
This case study describes the use of bulk personal datasets to help identify an individual for the agencies to approach as a potential informant.

Firstly, the use of intrusive surveillance powers, involving mass interference with the right to privacy, for the agencies' speculative recruitment effort is deeply controversial and likely unlawful. The use of intrusive surveillance powers for informant recruitment to further general intelligence gathering, in circumstances completely divorced from any immediate threat to life or suspicion of serious criminal offence is unnecessary, disproportionate and - as the misguided case-study reveals – can carry the risk of a heightened security threat to the individual concerned.

Even leaving legal necessity and proportionality aside, the case study does not provide evidence of factual necessity. The agencies discovered that the potential informant was in contact with another individual with access to intelligence who they had identified – however, it is not explained how or why the potential informant was unable to be identified through contact chaining and a continuation of the targeted approach. Nor is it clear how BPDs were uniquely able to complete the identification of the potential informant. This case study does not provide evidence of the necessity of BPDs. It does however provide evidence of the potential for abuse of broad surveillance powers and the deeply counter-productive impact that such abuses bring.

Protection of major events
When significant events take place – such as the NATO Summit in Wales in 2014 or the London Olympics in 2012 – the security and intelligence agencies work to ensure they occur safely. This includes tracing the details of individuals with access to venues so as to mitigate the risk that subjects of national security interest might gain access to these events. The majority of individuals in such datasets will not be of direct intelligence interest and this data is therefore treated as BPD. Without using this information, it would be far harder, more costly and intrusive for the police and agencies to put in place alternative measures to provide security assurance.

Analysis
It is understandable that certain events taking place in a high threat context may necessitate access controls, and knowledge of who has access to certain venues. It may be that a condition of working at such events requires staff to consent to public authorities retaining knowledge of their identity and access privileges, or even undergoing a vetting process. Approximately half a million people were screened in advance of the London Olympics in 2012, including potential Games workers, security guards, athletes, coaches, international

officials and volunteers.[36] However, this does not constitute evidence that incredibly broad non-consensual bulk personal dataset powers are required as these specific datasets can be, and have been, legitimately acquired.

Case Study: Stopping Al Qaeda (AQ) terrorist plots

Intelligence received by the security and intelligence agencies indicated that a member of AQ was facilitating suicide bombers in the UK. The security and intelligence agencies had a broad description for the AQ member but no name. Potential contact information was received, but didn't immediately identify the individual. Using BPD analysts were able to identify possible matches and quickly narrow this down to one strong match. At this point the necessity and proportionality case was robust enough to deploy other, more intrusive methods to cross-check the information and positively identify that the match was the suspected AQ member.

Analysis

This case study describes a situation in which intelligence and contact information only partly identified a terror suspect, and BPDs were used to 'identify possible matches'. There is too little information to analyse this case study in detail, or for it to constitute evidence of the necessity of BPDs. It is unclear what information was, or indeed could be, given in the intelligence that would fail to identify the suspect, make it impossible to identify the suspect using usual investigative tools, but yet would lead to a match in a dataset of predominantly innocent individuals. The case study says that the contact information received didn't 'immediately' identify the individual suggesting that it may have been capable of doing so with resort to targeted investigatory techniques at the outset. Reference to the use of more intrusive techniques once the 'necessity and proportionality case was robust' highlights the self-governing and self-serving nature of both the powers claimed and case studies provided. Necessity and proportionality are legal tests but currently reduced to subjective and circular determination by the agencies and ministers. Given that the vast majority of individuals in a bulk personal data are not of intelligence interest, this case study touches on one of the concerning ways in which BPDs are used – to 'identify possible matches'.

[36] *London 2012 Olympics: huge security vetting rejects 100 applications* – Andrew Hough, The Telegraph, 6 June 2012 http://www.telegraph.co.uk/sport/olympics/news/9312522/London-2012-Olympics-huge-security-vetting-rejects-100-applications.html