LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's submission to the Terrorism Reviewer's Review of Bulk Powers

July 2016

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 Policy

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

Bella Sankey
Director of Policy
Direct Line: 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sara Ogilvie
Policy Officer
Direct Line: 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Silkie Carlo
Policy Officer (Technology & Surveillance)
Direct Line: 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

Sam Hawke
Policy Assistant
Direct Line
Email: samuelh@liberty-human-rights.org.uk

Background

1. The Government has appointed David Anderson QC to review the 'operational case' for the powers contained in Parts 6 and 7 of the Investigatory Powers Bill, currently before the House of Lords. The establishment of a Review follows a recommendation by the Joint Committee charged with scrutinising the Draft Investigatory Powers Bill and pressure from the main Opposition parties and human rights campaigners, including Liberty.

2. The Review takes place against a fraught context for trust in the UK and US intelligence agencies, demonstrated most recently by the Chilcot Inquiry report which was highly critical of the culture and leadership of the agencies and their over-reliance on flawed intelligence.

3. Since the revelations of large-scale surveillance practices by Edward Snowden in 2013, the British Government has sought to claim the absolute necessity of 'bulk' surveillance practices both in the course of legal challenges to its practices, and in ex post facto legislative efforts. However, the necessity of 'bulk' powers, particularly in relation to signals intelligence, is often conflated with the necessity of technical infrastructures that can be used to gather information in either an indiscriminate bulk manner or on targets. Furthermore, justifications for bulk powers have been supported with scant operational case studies that are vague and fall far short of demonstrating necessity. In the attached Annexe to this submission, we reproduce and scrutinise each case study contained in the Government's 'Operational Case' document, with particular focus on whether they provide evidence of the strict necessity of bulk powers. We conclude that none of the case studies or examples provided has yet provided met this threshold. In the main body of this submission we explore the technical infrastructures used in signals intelligence and the necessity of the various technical options. We further address the 'operational case' of the remaining Part 6 and 7 powers.

Terms of reference

4. The terms of reference for the Review state that it will "examine the operational case for the investigatory powers contained in Parts 6 and 7 of the IP Bill including the 'Operational Case for Bulk Powers' document which was published alongside the Bill on the 1st March 2016."

5. From a public policy perspective, it is imperative that the Review measures the agencies' claims concerning bulk by whether the powers as presently drafted in the IP Bill are 'strictly necessary' in a democratic society. This is a both a legal and technical question. It is a legal question because the test derives from the UK's international human rights obligations which mandate that secret surveillance powers will only be lawful if they meet clear thresholds and include key safeguards. It is also a technical question because it involves (a) an analysis of the breadth of practice which falls under the term 'bulk' and an assessment of which practices, if any, are strictly necessary, and (b) an analysis of the alternative, targeted, powers that could equally serve the purposes of preventing and detecting serious crime and protecting national security. The central question for the Review is whether *but for* the scope of the powers, crucial information would not have been obtained that has resulted in serious offences being prevented or detected. This must include an assessment of whether the same information could have been accessed through a power drafted in a more targeted way.

6. A thorough review of the 'operational case' should also focus not only on the claimed successes of bulk powers, but review comprehensively the operation of bulk surveillance programmes including inspecting evidence of their failures.

The test: "*strictly necessary for the obtaining of vital intelligence in an individual operation*"

7. Over the past forty years, the European Court of Human Rights has considered numerous challenges to State interception laws and practices across the Council of Europe. It has developed a body of case law consisting of legal tests and safeguards to measure the lawfulness of member states' legislative systems. The Court has repeatedly stated its principal test 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…*"[1] (emphasis added).

8. In *Liberty v UK* (2008) which concerned the pre-RIPA external interception regime the Court found a violation of Article 8 on the grounds that the legal discretion granted to the Executive for the physical capture of '*such external communications as described in the warrant*' was '*virtually unfettered*' and the discretion governing which communications of the total volume captured were listened to or read was also too broad.

9. In *Szabo and Vissy v Hungary* (2016) the Court further refined its principal test, holding that "*A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration for safeguarding the democratic institutions and moreover if it is strictly necessary as a particular consideration, for the obtaining of vital intelligence in an individual operation*" (emphasis added).

Bulk Surveillance Powers: Exploring the Technical Necessity and Technical Options

Defining 'bulk'

10. 'Bulk' powers were only first officially acknowledged in March 2015 in a report published by the ISC which revealed two hitherto unconfirmed 'bulk' surveillance practices. The report referred first to 'bulk' interception of external communications conducted under the auspices of section 8(4) of the Regulation of Investigatory Powers Act 2000 and second to the practice of acquiring bulk personal datasets (BPDs), a capability it described as being "*not defined in legislation*".[2] "Two further 'bulk' practices were eventually officially acknowledged alongside the publication of the Draft IP Bill in November 2015: the acquisition and processing of UK-scale communications data[3] and 'bulk' equipment interference.

11. There is no statutory definition of 'bulk', although bulk powers are often described 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".[4] The 'Operational Case' document provides the circular explanation that "*it is inevitable that much of the data acquired using any of the bulk capabilities will not be of intelligence interest, because it is impossible to determine at the time of acquisition whether a particular piece of information will have intelligence value*." The closest the IP Bill comes to defining bulk is contained in Part 7 where BPDs are defined by reference to their nature

[1] Kennedy v UK, Application no 26839/05, 2010, paragraph 153.
[2] Ibid, para 157.
[3] On the day that the draft Bill was published, the Home Secretary announced that the Agencies have been acquiring the communications data of the UK population in bulk under the vaguely worded section 94 of the *Telecommunications Act 1984* since 2005. This had never previously been publicly admitted by the Executive and was apparently only known by a handful of Cabinet ministers.
[4] *Bulk Personal Dataset Factsheet* accompanying the Investigatory Powers Bill – Home Office, March 2016

2 Ibid, para 157.
3 On the day that the draft Bill was published, the Home Secretary announced that the Agencies have been acquiring the communications data of the UK population in bulk under the vaguely worded section 94 of the *Telecommunications Act 1984* since 2005. This had never previously been publicly admitted by the Executive and was apparently only known by a handful of Cabinet ministers.

"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."* [5]A general rule is that "**if a significant portion of the data collected is not associated with current targets, it is bulk collection**; otherwise, it is targeted".[6] This rule will be used as a working definition of bulk collection for this report.

Bulk Interception

12. Documents revealed by NSA whistle-blower Edward Snowden show that bulk interception powers have been used by GCHQ to collect images and conduct facial recognition via millions of innocent people's webcams[7], harvest details of the use of search engines, online maps, and social media[8], and to create web browsing profiles at a global population level.[9] Bulk interception takes place at such scale that billions of communications are being intercepted each day. Liberty understands that the Agencies are currently handling 50 billion communications per day. The ISC reported that at the end of 2014, there were just 20 section 8(4) warrants in place authorising the vast volume of interception under this power.

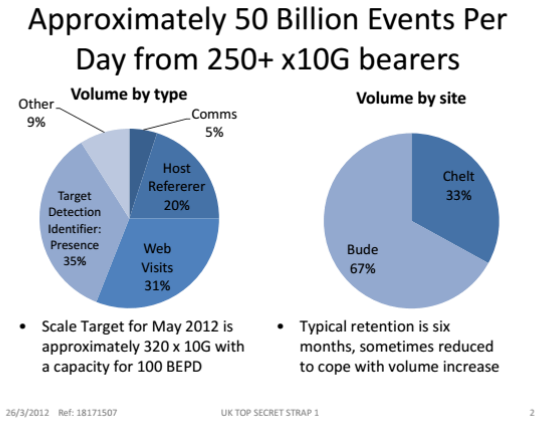
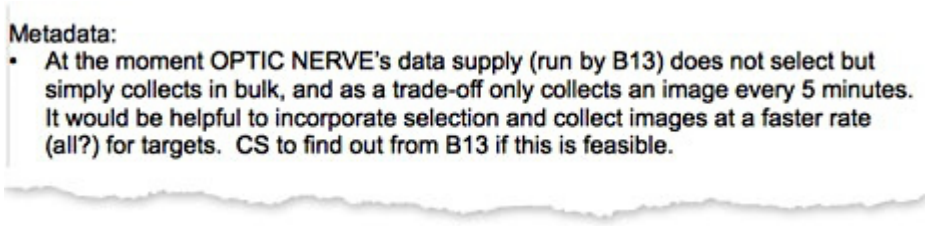


FIGURE 1: GCHQ's bulk interception ('*GCHQ Analytic Cloud Challenges*', GCHQ)


Metadata:

- At the moment OPTIC NERVE's data supply (run by B13) does not select but simply collects in bulk, and as a trade-off only collects an image every 5 minutes. It would be helpful to incorporate selection and collect images at a faster rate (all?) for targets. CS to find out from B13 if this is feasible.

[5] Investigatory Powers Bill 2016, Clause 182.
[6] *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.2
[7] *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ* – Spencer Ackerman and James Ball, The Guardian, 28 February 2014. https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo
[8] MEMORY HOLE, MARBLED GECKO, and SOCIAL ANTHROPOID respectively. See https://theintercept.com/gchq-appendix/
[9] KARMA POLICE: See *Profiled – From Radio to Porn, British Spies Track Web Users' Online Identities* – Ryan Gallagher, The Intercept, 25 September 2015. https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/

FIGURE 2: OPTIC NERVE, a GCHQ bulk interception program which targeted 1.8million Yahoo webcam users in a six-month period, collecting images including of which approximately 7% were intimate and explicit (‘*Potentially Undesirable Images’,* GCHQ*).*

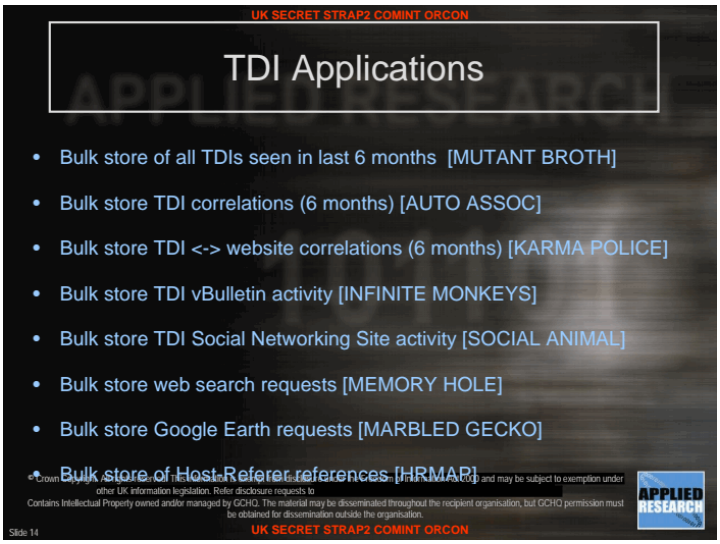


FIGURE 3: A list of some of GCHQ’s bulk stores from bulk interception, including people’s web searches, use of online maps, and social media activity, which can be searched for target detection identifiers (TDIs, ‘*Target Detection Identifiers’,* GCHQ).

TOP SECRET STRAP1

THQ/1202THQ/1900/0058
29 February 2008

popular PRIME TIME. looks for cross-media timing chains, e.g. a telephone call triggers a chat event.

ACTION: Ran out of time for discussion – to be brought back for next PSTG session.

- **KARMA POLICE** - submitted at TRL 4.

KARMA POLICE aims to correlate every user visible to passive SIGINT with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet.

For more details, refer to high-level overview document B/6760BA/5001/1.

Initial work with INOC shows high analyst usage of technique.

ACTION: To be progressed as a Better Analysis theme based requirement for explore.
- noted that the legalities with respect to ‘content’ need to be cleared.

FIGURE 4: KARMA POLICE, a GCHQ bulk interception program aiming to provide a “web browsing profile for every visible user on the internet” (*‘PullThrough Steering Group Meeting #16’*, GCHQ).

13. The Home Office describes bulk interception as a “vital tool” used to “obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK”.[10] However, what is currently described as ‘bulk’ interception covers many technical processes and lends itself to diverse and highly controversial further practices.

[10] *Bulk Interception Factsheet* accompanying the Investigatory Powers Bill – Home Office, March 2016

Signals Intelligence, or SIGINT

14. GCHQ conducts signals intelligence (SIGINT) by intercepting signals involved in communications and extracting information. GCHQ intercepts signals by extracting data flowing through a channel (e.g. fibre optic cable), filtering the data, and storing it. The stored data than then be queried to produce a subset of data in response to a question, which can be analysed and refined. The resulting information may provide or contribute to intelligence that is disseminated among analysts and policy makers.

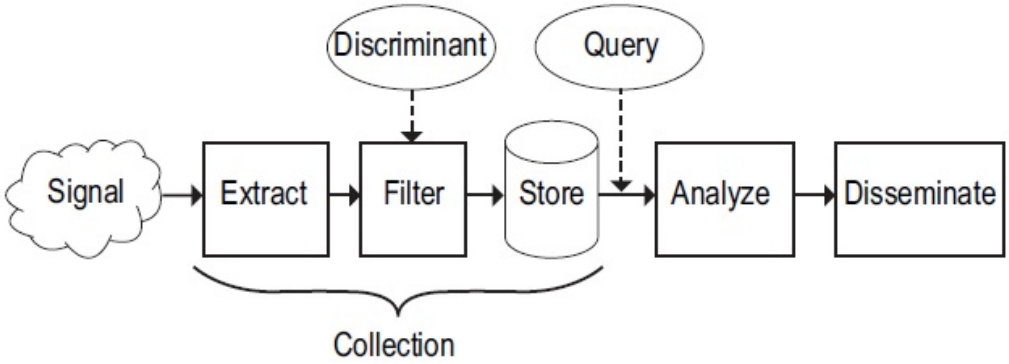


FIGURE 5: A conceptual model of the signals intelligence process[11]

15. *Extract*: The signal is obtained from a source and converted into a digital stream that can be reconstructed into sessionised data.

16. *Filter*: Data is selected for retention according to 'discriminants' applied, which describe the properties of items that should be retained. Data flowing by can be selected according to detailed instructions specifying selectors and identifiers. For example, a discriminant could be "all telephone calls from 12-34567-891234", or "all telephone calls from 12-34567-891234 to Syria". Alternatively, a filter can simply block high-volume low-traffic data, and thus select all meaningful data and person-to-person communications flowing by for retention.

If discriminants are deployed during filtering that limit collection to targets, the collection is **targeted**.

If discriminants are deployed to select a quantity of data unrelated to targets, and/or result in the collection of data disproportionately exceeding data related to targets, the collection is **bulk**.

17. *Store*: Filtered items are retained in a database. It is at this point that intercepted data is accessible, and 'collection' occurs.[12]

If filtering related to targets, this will be a rich store of **targeted** data.

If filtering does not relate to targets but involves broad discriminants this will be a very large store of **bulk** data.

[11] *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.5

[12] "*Reflecting this reality, the committee's definition of 'collection' says that SIGINT data is collected only when it is stored,* not *when it is extracted": 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.29

Interception is the access to or interference with a system or its operation to make contents of communication available during transmission to someone other than the sender or intended recipient.[13] Whilst interception describes the whole process, the store/collection phase may be considered the point at which 'interception' has occurred, or at least is complete, as it is at this point that data is available to a third party for the desired period of time. The previous steps are fleeting.

18. *Query:* An analyst searches the store of collected data according to detailed instructions.

    For example, a query could be as specific as "emails sent from seriouscriminal@outlook.com to othercriminal@gmail.fr between February 10 2016 to May 10 2016, and containing the word 'jihad'".

    However, a query could in theory be as broad as "all emails containing the word 'jihad'".

    The volume and relevance of results returned varies greatly depending on whether a targeted or bulk store has been queried, and the specificity of a query.

19. *Analyse:* An analyst can analyse the results returned by the query for any significant items.

20. *Disseminate:* Analysts may disseminate the intelligence within the Agency or beyond to law enforcement or policy makers.

Is 'bulk interception' necessary?

Extraction

21. Extracting signals from bearers of bulk data constitutes an invasion of privacy, as it involves unauthorised 'access' (although the packets of data are not necessarily intelligible until the point of storage) to vast amounts of information. However, extraction is a near real-time technical process that is required in order to filter the stream, sessionise/reconstruct packets of data, and store the selected information.

22. Clearly, the communications of targets cannot be covertly obtained with the co-operation of the targets themselves, and the communications of overseas targets cannot currently *always* be entirely obtained from third parties such as communications providers. Therefore, this mode of data acquisition provides an alternative route to communications of intelligence value.

Filter

23. Filtering is a crucial element of signals intelligence, which determines whether the interception is targeted or bulk.

24. Applying a discriminant per se does not necessarily result in targeted collection. Under the program *Tempora,* GCHQ applied a broad discriminant to eliminate only high-volume low-value traffic (peer-to-peer downloads, TV and film streaming, etc.). This is therefore a bulk interception program – a broad discriminant was applied that did not relate to targets, subjects of interest or

[13] RIPA, 2000, clause 2. Also in the Investigatory Powers Bill, 2016, clause 2.

even zones of suspicion, so the collection was bulk, leading to the storage of billions of communications of no legitimate intelligence value.

- TEMPORA is the codeword for GCHQs internet buffer business capability as a whole – which is the ability to loosely promote a % of traffic across GCHQs SSE access into a repository which will keep the content (and its associated metadata) for periods of time (approximately 3 days for content and up to 30 days for metadata) to allow retrospective analysis and forwarding to follow on systems.
- TEMPORA as a capability is *agnostic* of the technologies used to promote that traffic and to store that traffic and so should not be used as a codeword for the individual components (e.g XKS, MVR etc).
- At the moment the components include, amongst others, GCHQ SSE Access, POKERFACE sanitisation, XKS (in various configurations) and it will include MVR in the very near future.
- TEMPORA also covers the management of the rules used to promote traffic into the internet buffer capability.
- TEMPORA is not processing centre specific. At the moment there are instances of TEMPORA at all xPC (Namely CPC, OPC and RPC1). These should be referred to, when required, as OPC/CPC/RPC1 TEMPORA

[edit] A bit more detail

TEMPORA are GCHQ's large-scale, Deep Dive deployments on Special Source access (SSE). Deep Dive XKeyscores work by promoting loose categories of traffic (e.g., all web, email, social, chat, EA, VPN, VoIP...) from the bearers feeding the system and block all the high-volume, low value traffic (e.g., P2P downloads). This usually equates to ~30% of the traffic on the bearer. We keep the full sessions for 3 working days and the metadata for 30 days for you to query, using all the functionality that Keyscore offers to slice and dice the data. The aim is to put the best 7.5% of our access into TEMPORA's, comprising a mix of Deep Dive Keyscores and promotion of data based on IP subnet or technology type from across the entire MVR. At the moment, users are able to access 46x10Gs of data via existing Internet Buffers.. This is a lot of data! Not only that, but the long-running TINT program and our initial 3-month operational trial of the CPC Internet Buffer (the first operational Internet Buffer to be deployed) show that every area of ops can get real benefit from this capability, especially for target discovery and target development. Internet Buffers are different from TINT in that the latter is purely an experimental, research environment whereas Internet Buffers can be used operationally for EPR, Effects, enabling CNE etc.

For a more detailed depiction of how TEMPORA and TINT differs please see here.

FIGURE 6: A description of GCHQ's bulk interception program TEMPORA in which 'all web, email, social, chat' etc. was stored in a buffer for 3 (content) to 30 (metadata) days, before being transferred to another storage system or discarded ('*TEMPORA'*, GCHQ).

25. It has been argued that bulk interception has greater utility than targeted interception for several reasons – whether these reasons meet the necessity threshold is discussed below.

Contact chaining

26. Analysts may query a database by using a 'seed' identifier – an identifier belonging to a known target or subject of interest, which can be used to map the individual's patterns of behaviour and social network. Analysts can map contacts with the seed, highlighting those that are also suspicious because they are targets in their own right. If both the seed and another suspicious contact share a third unknown contact, that contact could be investigated too.

27. It has been argued that restricting interception to targets might obscure such ability, and frustrate efforts to map and understand networks. However, in a targeted interception model this is

not the case. Algorithms can flag contacts with a seed that are also suspicious – whether targets in their own right, or subjects of interest. If both the seed and another suspicious contact share a third contact, a suspicion-led algorithm can recognise that contact as being within a zone of suspicion too, and thus discover a new target. Algorithms can, in near real-time, output a new command for storage of data belonging to the new contact (such rules could be pre-approved by a judge). The Committee tasked with examining the bulk collection of Signals Intelligence in the US concluded that, "*If targeted collection can be done quickly and well enough, bulk information about past events may not be needed*".[14]

28. 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. Bulk collection is not necessary for effective contact chaining. Evidently, contact chaining through targeted collection provides insight to the structure and composition of important networks, and the appropriate prioritisation of targets.

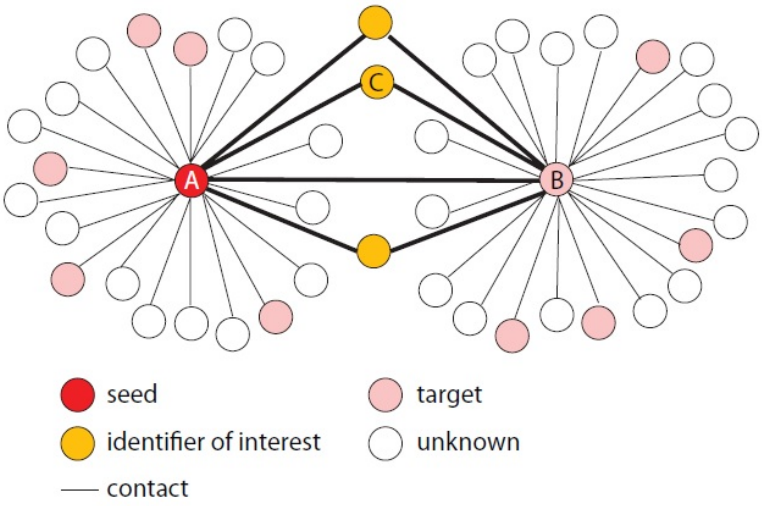


FIGURE 7: Contact chaining [15]

A retrospective record

29. An argument in favour of bulk storage is that, upon discovery of a new target, there exists a retrospective record of the individual's activities. It has been argued that, restricted only to forward-looking information, a trail may go cold, a target may change contact details, and vital information pre-dating the discovery of a target could be missed – particularly a concern in fast-moving, high-risk scenarios. These concerns can be mitigated so as to be eliminated. It is also an important point of principle and law, that a power cannot be justified on the basis of retrospectivity.

30. First, although the Agencies may not hold retrospective data themselves, the target's devices, and third parties such as the communications services they use, do. Once a target has been identified, if it is deemed necessary to obtain retrospective information, an analyst can seek the target's call records, which phone providers store for their own business purposes; retrieve

[14] *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
[15] *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.43

messages or emails, which are stored on communications providers' servers; access content that is stored locally on a target's device, which can be accessed in extremis through targeted equipment interference; and obtain banking and travel records. Much of this work can be conducted very rapidly, and increasing the ability to swiftly receive targeted information from communications service providers is a priority area for the Agencies. However, recognising that obtaining such information from communications service providers is not always possible, targeted equipment interference is another method which can provide a particularly high yield of intelligence.

31. Secondly, as discussed above, a suspicion-led algorithm can recognise contacts shared by other targets as being within a zone of suspicion, and thus discover and surveil new targets in near real-time. Thus, the onset of interception means the risk of missing of critical information is minimal: "*If targeted collection can be done quickly and well enough, bulk information about past events may not be needed*".[16]

32. Thirdly, and critically, all the statistically comprehensive and independent analyses of retrospective bulk data conducted to date, including the US President's Review Group on Intelligence and Communications Technologies (2013) and The US Privacy and Civil Liberties Oversight Board (2014), found that the availability of bulk retrospective metadata has no unique value for counter-terrorism aims.

33. 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.*[17]

34. Similarly, the President's Review Group on Intelligence and Communications Technologies concluded in 2013:

> *"Our review suggests 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."*[18]

35. Similarly, a self-evaluation report into Denmark's Data Retention Law (*Logningsbekendtgørelsen*), effective 2007-2014, which required internet providers to retain internet session logs for 12 months including client and server IP addresses, port numbers, transmission protocols and timestamps,[19] published by the Danish Ministry of Justice in December

---

[16] *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

[17] *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

[18] *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

[19] *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

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.[20] In fact, Ministry staffers reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[21] In 2013, approximately 3,500 billion telecommunication records were retained in Denmark, averaging 620,000 records per citizen.[22] 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*".[23]

36. Retrospective data from new targets can be sought from individuals' accounts, devices, and CSPs. Holding retrospective records at a population, and even international, level is clearly not *necessary* for any legitimate intelligence purpose – that it ever would be necessary is inconceivable.

Alternate identifiers

37. Identifiers for a target may change – for example, a target may change telephone number, email address or internet provider, possibly as an attempt to evade detection. It has been argued that bulk collection of communications data is necessary to discover 'alternate identifiers' – i.e. a target's new communications channel. However, this is neither necessary, nor the most efficient means of re-discovering a target.

38. Other targeted methods include, for example, targeted surveillance of other known identifiers of the target such as banking records to see if the target has purchased a new device, which it may be possible to acquire details of and track; deploying targeted equipment interference to a device in extremis, for example to overcome changes of internet providers, email addresses and online identities; or seeking information from a communications provider relating to the target. Furthermore, it is highly likely that a target identifier will, with the Agency's effort, lead to personal identification of the target. Once the personal identity of the target is known, there are a myriad of means by which alternate communications identifiers can be discovered.

39. Analysts can also use the target's social networks to locate alternate identifiers for the target – this is 'reverse targeting'. If the relevant necessity and proportionality thresholds are met, other people that were in contact with the target can have their communications data analysed to discover any new contact that appears in the network.

Target discovery

40. It is argued that bulk data is useful for 'target discovery' – the discovery of new targets and subjects of interest who may warrant further investigation. In a reversal of the long-held, important

[20] *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).

[21] Ibid.

[22] *Written evidence on Investigatory Powers Bill: Technology Issues* - IT-Political Association of Denmark, 2 Dec 2015, p.2

[23] *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

relationship between suspicion and surveillance, bulk surveillance produces data at a population level that can be sifted to uncover those deemed to display 'suspicious' behaviour. Speculative and suspicionless, the new Prime Minister, Theresa May, has even suggested that such surveillance should override legal professional privilege, telling the Joint Committee that "*it may be necessary to use some of these powers to identify that you are a naughty lawyer in the first place*."[24]

41. The Home Office has relied heavily on supposed examples of target discovery to demonstrate the value of bulk interception. 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, qualifies this by adding that the discovered target was in contact with "*a Daesh-affiliated extremist in Syria"*.[25] This plainly does not justify the broad bulk interception power currently exercised and provided for in the IP Bill. 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, to promote further target discovery. 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.

However, more speculative approaches – for example, discriminators that select dictionary terms for filtering (e.g. all forums containing the word 'jihad'), would clearly lead to storage of content disproportionately relating to people of no legitimate intelligence interest. It is difficult to envisage a scenario in which dictionary tasked terms could be deemed 'necessary' discriminators, as this leads to speculative, suspicionless, bulk surveillance.

It has been argued that such suspicionless surveillance may help to uncover would-be 'lone wolf' attackers – attackers who act independently of any network. To constitute any serious, preventable threat, an attacker must still undergo a process of radicalisation; be resourced with knowledge and weaponry with which to carry out an attack; and access extremist, suspect or illegal materials in the process.

Store

42. Depending on the filtering processes used, the store is a database of either targeted or bulk intercepted material. As explored above, a store of bulk data is unnecessary and has inherent risks both to privacy and triage of intelligence. Conversely, a comprehensive store of rich targeted data allows analysts to meet the same legitimate intelligence requirements as an indiscriminate bulk store, but arguably more efficiently and without such inherent risks.

43. A variety of protections can be added to the store – for example, isolating the store, encrypting the data, and limiting the period of time for which data are accessible. Such recommendations are outside the scope of this report, although the data retention period should be set according to necessity. The current evaluation sets bulk communications data retention at 12

[24] Theresa May in oral evidence to the Joint Committee on the Draft Investigatory Powers Bill, 13 January 2016
[25] Supplementary written evidence to the Joint Committee on the draft Investigatory Powers Bill (IPB0165) – Theresa May, December 2015, p.8

months. This period should be re-evaluated for a targeted communications data store – longer retention may be appropriate, as the data collected will be of intelligence value.

44. This store of targeted intercepted material helps to form one part of an overall intelligence picture – other targeted methods, some of which are discussed above, are also essential in intelligence gathering.

Query

45. Stored data is queried by analysts to produce relevant data, intelligence leads, and answers to complex questions. Queries should be focused, according to operational purposes. To ensure appropriate use of the stored data, isolation of stored data, protected by an automatic policy guard, can help to permit and restrict searches to what is necessary, and to produce an audit trail of all queries. This may help prevent discriminatory or otherwise inappropriate use of stored data. In the same way that a police search of a property must be linked to the cause for suspicion, it will only be necessary to use an individual's data in relation to the cause for suspicion.

Bulk acquisition of communications data

46. By contrast with bulk interception, where a half-hearted attempt is made to tie surveillance to "overseas" communications, bulk communications data acquisition has as its main purpose the acquisition of data held by UK based companies on the UK population.

47. In contrast to the situation with overseas targets, Government has readily available and enforceable access to the communications data of people in the UK via provisions contained in DRIPA and RIPA (due to be replaced by Parts 3 and 4 of the IP Bill). Government cannot therefore rely on the argument that some form of bulk access power is required in order to obtain data about the communications of targets. Instead, in this case, Government argues that this power is needed for speculative pattern analysis and fishing expeditions. However, strikingly, none of the bulk communications data case studies provided by Government in its 'Operational Case' document shows a causal link between bulk data acquisition and the factual outcome which could not have been achieved via targeted access to communications data under DRIPA and the use of investigative methods such as contact chaining. We examine and analyse each of these case studies further in the document annexed to this report.

Bulk Equipment Interference

48. Bulk EI is a foreign focussed power. It is by its nature indiscriminate, as acknowledged by the Draft Bill's Explanatory Notes: "*bulk equipment interference is not targeted against particular person(s), organisation(s) or location(s) or against equipment that is being used for particular activities".*[26] Instead, systems, services and software that have been carefully constructed to provide security are intentionally corrupted.

49. Astonishingly, all of the case examples provided in the 'Operational Case' document are hypothetical. A hypothetical case is not an operational case. It is even less an example of powers that have been shown to be "strictly necessary for the obtaining of vital intelligence in an individual operation".

Bulk Personal Datasets

50. The acquisition of bulk private and sensitive data on the UK population by the intelligence agencies is a new and radical development.

[26] *Draft Investigatory Powers Bill 2015: Explanatory Notes*, p. 83

51. They urgently require comprehensive review but it is difficult to see how this can be contemplated, yet alone delivered by the current Review team given that the Agencies themselves are apparently unable to provide basic information about their content and scope. The ISC reported in 2015 that "*None of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets*".[27]

52. There is no compelling operational case for the Agencies to collect, process and link personal data on the entire UK population. The ISC reported that the Agencies told them that BPDs are an "*increasingly important investigative tool*" to "*enrich*" information obtained through other techniques. "Enriching" and "relevant" does not meet the legal threshold for lawfulness. Current law allows data to be transferred across the private and public sector to further national security and the prevention and detection of crime. The Agencies therefore already have gateway powers to obtain information on those it identifies as being subjects of interest.

Conclusion

53. Bulk collection and storage of millions of pieces of personal data and communications of people of no interest to the intelligence agencies has not been shown to be "*strictly necessary for the obtaining of vital intelligence in individual operations*". In the case of interception, targeted filtering based on reasonable suspicion *before* storage provides rich, insightful intelligence that permits successful contact chaining, target discovery, and the discovery of alternate identifiers. Rapid target discovery using policy-oriented algorithms in targeted filtering results in almost immediate onset of collection upon identifying a target, and minimises the need for bulk retrospective records. This, combined with other targeted surveillance methods, means there can be no case for the strict necessity of bulk retrospective records. We urge the Review to put the intelligence agencies to strict proof of their claims across all bulk powers in the IP Bill and to provide detailed evidence and methodology to support its conclusions.

[27] Ibid, footnote 142.

ANNEX A

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

The Home Office published a 47 page 'Operational Case for Bulk Powers' on 1st March 2016 as an accompanying document to the Investigatory Powers Bill. The document presents 'a series of examples and case studies to illustrate the value of (bulk) powers' to the security and intelligence agencies. In the following analysis, we reproduce and scrutinise each case study with particular focus on whether any provide evidence of the *strict necessity* of bulk powers. We conclude that none of the case studies or examples provided has yet provided evidence to meet this threshold.

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.

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

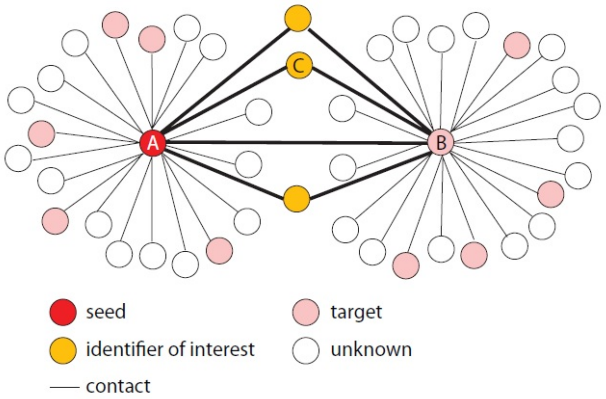


FIGURE 1: Contact chaining [28]

[28] *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.43

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'.[29] These methods do not involve bulk equipment interference.

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.

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

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".*[30] 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.

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

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.

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 questionableflawed, 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.[31] 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.

[31] *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

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'.

Policing the 'dark web'

The 'dark web' is an online space in which users, and some websites, can be anonymised. By the Home Office's own admission, there are 'many valid uses for these internet tools and sites, including by citizens campaigning for civil rights under authoritarian regimes'.[32] Indeed, the possibility of anonymity is essential in a democracy and is important for free speech, empowering minorities and protecting those who may be vulnerable to persecution.

David Kaye, the United Nations Special Rapporteur on Freedom of Expression, described anonymity tools as a leading vehicle for online security and freedom:

> *Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.*[33]

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'.[34] The Home Office claims that data 'obtained through bulk interception' is used to identify anonymous users of the dark web. Whilst the data was 'obtained' through bulk interception,– desired data on uniquely identified internet users could be obtained through the targeted model of signals intelligence we have described.

However, the claim that bulk data is used to uncover the identities of anonymous internet users is an unusual and challenging one. 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

[32] Paragraph 3.12
[33] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* – UN Human Rights Council, 22 May 2015, paragraph 1
[34] Paragraph 3.13

the identification of users, whose traffic is distributed through Tor relays around the world. Tor is designed specifically to protect users from such dragnet, authoritarian surveillance. The only foreseeable application of bulk powers to law enforcement on the dark web would be an indiscriminate surveillance exercise such as identifying all users of Tor – an illegitimate, unnecessary and undemocratic task. There is some controversial evidence in the Snowden documents of broad attacks against the Tor network, combining bulk powers and computer network exploitation.[35]

More recent coverage of 'dark web' law enforcement efforts indicates the use of traditional and targeted investigative techniques, the exploitation of the anonymity network to impersonate key facilitators of criminal networks, and equipment interference (computer network exploitation) powers to identify suspects, leading to arrest. Notably, the FBI's takedown of the dark web marketplace Silk Road;[36] the FBI's prolific operation to takedown the 'Playpen' paedophilia site and identify over 1,000 of its anonymous visitors;[37] and the Australian Taskforce Argos' operation against the paedophile network 'The Love Zone', including the serial British sex offender Richard Huckle,[38] 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 and permit further arrests.

More evidence would be required to make the operational case for the necessity of bulk powers in order to police the dark web. The operational case has not been made, and from a technological point of view it is implausible. Identifying all users of anonymising technologies is absolutely not necessary to deal with criminals who operate online, and would certainly not be proportionate.

[35] *How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID* – Bruce Schneier, 7 Oct 2013, https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

[36] *The Dark Web Dilemma: Tor, Anonymity and Online Policing* – Eric Jardine, Sept 2015, Global Commission on Internet Governance, p.8

[37] *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

[38] *The takeover: how police ended up running a paedophile site* – Michael Safi, 13 July 2016, The Guardian, https://www.theguardian.com/society/2016/jul/13/shining-a-light-on-the-dark-web-how-the-police-ended-up-running-a-paedophile-site