Submission by Open Rights Group to the IPCO request for comments on bulk warrants

For comments and further information please contact Javier Ruiz <javier@openrightsgroup.org>

Disclaimer: the arguments presented here are based to an extent on partial, leaked and incomplete information. It is likely that there are factual mistakes. We will welcome corrections and hope that more transparency will improve the quality of public debate on surveillance.

We welcome the opportunity to contribute and support the efforts of IPCO to engage civil society and the flexibility demonstrated.

These notes do not form a comprehensive approach to proportionality and bulk warrants, but raise a series of issues that we believe would be useful to consider. We do not wish to lecture or preach to the commissioners and staff, but hope to bring a critical perspective.

It would be important to state from the onset that we do not support bulk powers and do not want to see this intervention perceived as an endorsement for powers we have campaigned against in the past and will continue to oppose.

Providing some constructive engagement while remaining critical is a difficult line to tread as we are concerned about contributing to the "surveillance realism" described by academics such as Lina Dencik.[1] Surveillance realism refers to the increasing normalisation of surveillance and its deleterious effects on society, as evidenced in the Cambridge Analytica scandal, which is only the tip of the iceberg. The surveillance activities of the state that IPCO tries to regulate need to be seen in this context.

Below we cover a variety of issues but a key aspect is a critical discussion on the nature of bulk powers, which has shifted from being explained as taking a picture of a crowd where a suspect is located in order to find her – the proverbial needle in the haystack. After Cambridge Analytica we understand much better how the crowd can be broken into its individual components, analysed and even manipulated in minute detail.

Another important "meta-issue" is the relationship between technology, society and the legal system. David Anderson has made the argument that it would almost be a dereliction of duty on the part of the State not to use any available surveillance technologies, provided that the UK as an advanced democracy can provide safeguards. This simple view of technology as a

[1] Dencik, L. (2018). Surveillance realism and the politics of imagination: is there no alternative? Krisis Journal for Contemporary Philosophy

given that simply happens to be there for the taking masks very complex processes where regulation and also state action shape the nature of what is available. These arguments also demonstrate that the regulation of surveillance should not be left just to lawyers and possibly computer scientists, and needs broader perspectives, including from the social sciences, and of course from ordinary citizens.

We also have to add a caveat that the oft-heard arguments about the benign nature of targeted surveillance versus the intrusion of bulk powers are being criticised by many rights campaigners. Groups working with minorities complain that this distinction masks the targeting of whole communities, and we stand in solidarity with them. Cases such as the Spycops scandal demonstrate that the problems with state surveillance go much further than bulk powers.

The purpose and scope of bulk

The security agencies have argued that they need to tap whole data cables in order to sieve through the data stream because they cannot selectively look at individual pieces of information. After Snowden they rebranded this process as “bulk collection” or “bulk interception”, which in their view does not constitute mass surveillance because the collected data will be processed and analysed by computers meaning only a small amount relating to suspects will be seen by human operatives.

The Royal United Services Institute (RUSI) report on Internet surveillance claims that even “bulk data is a misleading term as it most frequently refers to the interception of data in bulk rather than to the data itself (hence use of the term bulk interception)”.[2]

The claim that GCHQ must intercept the Internet communications of a wider pool than their targets may be technically true because of certain aspects of how the Internet works. Internet communications are based on what is called packet switching networking.[3] This means that each message is broken into many smaller pieces called “packets”, all containing the sender and destination. Packets are then left to find their own way through the most optimal route to the recipient – with the help of Internet infrastructure such as the aptly-named routers – where they are put back together. Internet surveillance requires the ability to look into all individual packets in this raw flow, in order to classify them and reassemble the actual contents of messages.

However, the essence of Internet surveillance is not simply reconstructing the content of targeted communications, but analysing the flow of the general Internet traffic, metadata, looking at all packets regardless of any previous suspicion. All the various reports commissioned after the Snowden leaks – from the ISC, the Independent Reviewer of Terrorism and RUSI – acknowledge the increasing role of non-targeted surveillance for so-called ‘target discovery’ of unknown threats.

[2] https://www.rusi.org/downloads/assets/ISR-Report-press.pdf (p.18)
[3] See a very accessible introduction here http://labs.rs/en/packets

If the argument is that tapping backbone Internet cables is necessary as a precursor to targeted surveillance under certain circumstances – and we must therefore accept certain levels of intrusion and that the agencies will need to look into traffic and “see” at the very least individual packets – this intrusion should be minimised by reducing the degree to which traffic is captured, reconstructed and processed.

The leaked Snowden documents showed that instead the guiding principle appears to be maximising every aspect of surveillance. Limited resources seem to be the main obstacle to the capturing and automated processing of everything the agencies can get hold of; not considerations of privacy, which mainly come into play once analysts start interacting with the databases.

We remain convinced that the term “mass surveillance” reflects the whole process of wholesale interception of data and population level analytics, while “bulk collection” does not adequately reflect what is actually taking place and is too narrow. But ultimately the focus should be reducing the level of intrusiveness of Internet surveillance. This will involve technical decisions at every stage as agencies work from pure electronic signals to individual packets, fragments of traffic and full messages, all the way up to rebuilding complete Internet histories and social maps. It is unclear how bulk warrants could be so restricted and we would welcome more information from IPCO on these matters.

Bulk and targeted surveillance

The law makes a very clear distinction between bulk and targeted surveillance, but we are not completely sure that these lines are that clear. In March 2015, the Intelligence and Security Committee (ISC) of the UK Parliament published Privacy and Security: A modern and transparent legal framework. This report claimed that the bulk interception of Internet data by GCHQ is not mass surveillance because only a proportion of data is collected, thanks to a combination of policy, operational and technical limitations.

It describes two completely separate physical systems of surveillance operated by GCHQ.

One is an “investigative tool”, targeted at “specific identifiers relating to a known suspect” to be analysed by intelligence operatives. This system collects data from an unspecified number of cable points they call 'bearers' (we discuss how these work below). According to the ISC, these comprise “a very small percentage of the ‘bearers’ that make up the Internet”. Only a small proportion of the collected information – deemed of high intelligence value – is ever seen by analysts, who have to prioritise their limited resources.

A completely different and smaller “discovery, or intelligence gathering tool” would truly provide the “‘bulk interception’ capability that has led to allegations that GCHQ are monitoring the communications of everyone in the UK”. Selected categories of data likely to be of interest are collected and then computers run “complex searches” to reduce the “odds of false positives”. The resulting list of communications is presented to analysts. This system would operate on an even smaller set of Internet bearers than the targeted tool above.

However, we are not sure if the ISC's clear cut depiction of a main system of targeted interception and a smaller more limited, non-targeted system fully matches the actual operations. The documents leaked by Snowden show a much more dynamic picture of constant experimentation and opportunistic growth, where the lines between targeted surveillance and “discovery” are constantly redrawn, with new potential target identifiers being created all the time.

We would welcome more clarification on how these supposedly separate systems operate and how the discovery or strategic monitoring tools feed into targeted surveillance of relevant individuals instead of creating a permanent cloud around myriad potential suspects. The proportionality assessment of bulk warrants would relate to how much of a “funnel” they provide, rather than simply becoming floating dragnets.

The necessity fallacy

The Anderson review did not properly examine the proportionality of the measures involved, only whether there was evidence that bulk data collection had served a purpose. The cases used were to the best of our knowledge self-selected by the security and intelligence agencies, clearly to showcase the need for the powers they had been strongly lobbying for. This limits the utility of basing the analysis of proportionality on this body of evidence. In addition, Anderson ignored dissonant evidence, such as the report from the Intelligence and Security Committee that criticised bulk hacking, or the US Privacy and Civil Liberties Board report that found there was no value in giving all phone records to the US Government for analysis.

We think that this utilitarian “necessity” approach based on presenting selected cases where bulk has served a purpose is fundamentally flawed and could ultimately be used to justify any abuse of human rights. We have seen it, for example, in the “ticking bomb” justifications of torture – and proposals for its proper regulation – by US scholars such as Alan Dershowitz,[4] which have been severely criticised.[5]

It is worth pointing out that Dershowitz only advocates torture as an exceptional last resort, while bulk data collection has become the default modus operandi of modern Internet surveillance, routinising widespread human rights intrusions on the basis of some exceptional necessity.

Disconnection between operations and warrants

The cases presented in the Anderson review describe the uses of data that were obtained under bulk certificated warrants under RIPA s 8(4). However, unless we are mistaken, the warrants themselves were unrelated to these operational cases. To the best of our knowledge there were a very limited number of bulk certificates under RIPA in operation,

[4] Dershowitz, A.M.. (2003). Why terrorism works: Understanding the threat, responding to the challenge.
[5] e.g. Kramer, M. H. (2015). Alan Dershowitz's Torture-Warrant Proposal: A Critique. http://doi.org/10.2139/ssrn.2559237

reissued every six months, covering a variety of telecommunications providers and infrastructure, including one that covers all of GCHQ's key bases in Bude, Menwith Hill and Cyprus.[6] These broad certificates enable a range of activities such as "political intentions of foreign powers", terrorism, proliferation, mercenaries and private military companies, and serious financial fraud."[7]

Under the old regime, GCHQ analysts would have been able to target individuals that they believed fell under these certificates. In principle this has changed now, but it remains unclear what level of sign off from IPCO each of the cases in the Anderson report would have involved. Our impression is that in most cases the processing of bulk data would be governed as internal operations by GCHQ, and only when a named target had been developed would a warrant for their targeted surveillance, or access to their already obtained communications content, be sought. IPCO would only have the opportunity to review these operations as part of their routine oversight.

Experimental and novel and controversial techniques

The same warrants could have been used to enable unjustifiable intrusions. Indeed these bulk warrants have probably enabled cases such as the mass capture of private Yahoo webcam video streams. There are leaked documents showing that GCHQ tapped into the private webcam communications of innocent Yahoo! subscribers without clear legal authorisation. The agency collected millions of pictures, including substantial amounts of explicitly sexual materials.[8] Apparently unknown to Yahoo!, the programme OPTIC NERVE affected 1.8 million unwitting users of the service in a six month period without any form of individual targeting. The images were apparently used to improve facial recognition software. According to The Guardian, metadata and images were also fed into the NSA database and search engine XKEYSCORE.[9]

US senators have launched an investigation[10] into these activities, accusing GCHQ of "breathtaking lack of respect for privacy and civil liberties". GCHQ has simply provided a boilerplate response about compliance with UK laws, but this programme seems very hard to justify under current legislation. We believe this particular incident deserves full investigation as one of the most egregious privacy intrusions documented.

IPCO's Advisory Notice on Judicial review[11] says that "there will be applications, such as those raising novel or controversial techniques, which will require a much greater level of scrutiny than others." This is a welcome position that we have advocated in our previous communications with the commissioners, however the question remains on the level of actual authorisation involved in innovative and experimental techniques such as those

[6] MacAskill, Borger, Hopkins, Davies and Ball, "The legal loopholes that allow GCHQ to spy on the world", The Guardian, (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world
[7] See Eric King's witness statement to Case No. IPT/13/92/CH
[8] http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-Internet-yahoo
[9] http://www.theguardian.com/world/2014/feb/28/nsa-gchq-webcam-spy-program-senate-investigation
[10] Ibid
[11] https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf

described above. For example, leaked GCHQ documents show that the agency shared large amounts of data with academics to develop novel surveillance methods. We would welcome clarification on whether any such activities would now be subjected to judicial review or even oversight. While it may be impossible to foresee all the potential pitfalls, there should be some due diligence along the line of privacy impact assessments.

Infrastructure, warrants and operations

The above raises a fundamental problem with the examination of the necessity and proportionality of mass surveillance.

The enabling of bulk data acquisition though such broad warrants has created very general capabilities around specific companies or infrastructures. It seems very hard to establish the proportionality of these warrants that collectively create a potential dragnet that affects the majority of the population. This approach to warrants does not allow for a proper assessment of proportionality. A system of nimbler warrants with a much narrower scope and with shorter time spans would be required. Routine extensions every six months are not acceptable.

Technical Capability Notices set out in more detail what companies have to do before they are able to comply with bulk warrants, e.g. what machinery and processes must be in place. However, it is not a prerequisite to have a surveillance warrant in place to impose a Technical Capability Notice.

These notices should allow for a better examination of the necessity of the measures involved, and it is a very positive step that, after extensive lobbying from civil rights groups, these will be under double-lock. However, we are still at the level of infrastructure, not operations. The Judicial Commissioners are required to assess whether “the notice is proportionate to what is sought to be achieved by that conduct.[12] But at this stage the aim could simply be to enable bulk powers, so it would be important to explain how this proportionality assessment will be carried out.

GCHQ and the NSA describe their surveillance activities in terms of programmes, not warrants or even specific operations. For example the INCENSER programme described as the “NSA's fourth-largest cable tapping program”[13], located at Skewjack Farm in Cornwall, has survived various changes of ownership in the cables affected. There is little discussion in any of the documents as to the proportionality of continuing this tapping operation, which seems to have become semi-permanent surveillance infrastructure.

The original company behind the program, Cable and Wireless, had been copying all international telegrams for the Government to read since World War I until the 1960s. In the leaked documents, whenever capability is lost, it is generally due to some technical problem or the loss of a relationship. We have not seen a single document where UK bulk surveillance infrastructure is willingly decommissioned to reduce human rights intrusions.

[12] IPA 2016, s. 254(2)b
[13] http://electrospaces.blogspot.co.uk/2014/11/incenser-or-how-nsa-and-gchq-are.html

It feels misleading to describe this kind of infrastructural development in terms of warrantry, as if it was in any way comparable to targeted surveillance operations. In addition, it is well documented that the same deep processing of Internet traffic is used to enable hacking operations so in practice it is difficult to see how these types of bulk processes -interception and interference - can be separated other than through some level of artifice.

International collaboration and data transfers

The INCENSER example also highlights another challenge to the proportionality assessments. The traffic collected is sent to the US and other close allies, and there are few restrictions on what they can do with that data, including on drone assassinations, as far as we understand. We believe these aspects should be incorporated in any assessment but there seems to be limited grounds.

Governance and accountability of bulk surveillance

The reviews of surveillance by the ISC and Anderson explained that data is collected from fibre optic cables at the level of discrete frequency channels, called “bearers”, and that the switching on and off of “probes” that will copy all the traffic through such bearers is a dynamic process, driven by operational priorities. Given that there is not enough information processing capability to handle the data if all probes were turned on simultaneously, this technical limitation creates a practical safeguard against complete surveillance. What is less clear is the process by which these probes are turned on or off.

We understand that the agencies are constrained at a very broad level to only generate intelligence for the purposes determined in the Intelligence Services Act: national security, the economic well-being of the UK, and serious crime. The National Security Strategy, produced every five years, sets out further directions. Every surveillance operation must relate to some priorities and objectives, as we can see in some leaked GCHQ policy documents.[14]

When it comes to directing surveillance for intelligence purposes, our understanding is that although the Home and Foreign Secretaries are directly responsible for the Intelligence and Security Agencies, the agencies' priorities are established by the National Security Council (NSC) and the Joint Intelligence Committee (JIC). The JIC can be asked by departments to produce intelligence, but it is mainly directed by the NSC, which sets priorities according to current policy issues. The RUSI report explained this process:

> *“The NSC process for Priorities for Intelligence Collection (PICs) sets out the priorities of SIS and GCHQ. The PICs are divided geographically and thematically and are set with a three-year outlook. They are reviewed annually. The intelligence agencies can also be set mid-year requirements in the form of a Temporary Intelligence Watch, ordered by the chairman of the JIC, in response to events unforeseen by existing PICs (such as the Ukraine crisis, Arab Spring, or the*

[14] http://theintercept.com/document/2015/09/25/hra-auditing/

emergence of ISIL). This ensures the process can be flexible when necessary. The PICs are informed by statements of demand from government departments, and take the form of detailed questions that align with specific policy objectives. They do not dictate what specific resources should be allocated; however, the intelligence agencies use the PICs to prioritise and guide their own resourcing decisions." [15]

It appears that the high level priorities for which cables are to be monitored will come from the National Security Council and the specific decisions from operations managers at GCHQ. Strategic decisions on which new cables to tap and where to expand existing capabilities will be taken by the leaders of the organisation. The exact role of IPCO in this system is unclear and ideally should be explained.

We understand from the published Advisory Notice on Judicial Review that the commissioners will not be second guessing national security decisions, but there must be some limits. Simon McKay has criticised the Advisory Notice for failing to emphasise "the importance of a current and relevant intelligence case justifying the decision to issue warrants",[16] particularly in national security cases, where the advisory leans towards a wider margin of judgment. We fully support this view. This is the more relevant because while in the past national security would mainly involve state to state relationships and spies, with some innocent foreigners also affected, modern surveillance affects whole populations.

Five years after the Snowden revelations, it is still unclear who, in any of the branches of Government, knew about the existence of mass surveillance programmes. In October 2013, ex-cabinet minister Chris Huhne stated that neither the Cabinet nor the National Security Council had been told about the TEMPORA programme. It also appears that the oversight bodies themselves did not know about the programmes, although that has been difficult to ascertain.

We agree that IPCO should not be, but at the same time the development and governance of mass surveillance infrastructure is a critical aspect that will determine the proportionality of the conduct of the state as a whole. At the very least, the commissioners signing off bulk warrants should understand the wider systemic implications of the surveillance infrastructure they are enabling and be able to question the proportionality of certain operations that interfere with the communications of potentially millions of people.

Intrusiveness and metadata

The Report of the Office of the United Nations High Commissioner for Human Rights in 2014, *The right to privacy in the digital age* (A/HRC/27/37), explains how the Human Rights Committee of the UN analyses proportionality as "the least intrusive instrument amongst

[15] https://www.rusi.org/downloads/assets/ISR-Report-press.pdf p51

[16] https://simonmckay.co.uk/covert-policing/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/

those which might achieve the desired result",[17] in relation to the specific risk being addressed. It is difficult to see how this can be ascertained when the same bulk certificates can cover such a variety of risks from terrorism to economic espionage. The Anderson report discussed in passing alternatives to bulk, but any such options were quickly dismissed. It would be important to have clear criteria on what constitutes the least intrusive method, but these analyses also need to be grounded on concrete operations.

One issue here is that there seems to be an accepted hierarchy or intrusion where interception of content is worse than capturing metadata. But in light of modern techniques and given the vast troves of metadata available we now have to accepts that both forms of surveillance can be highly intrusive, albeit in different ways.

The proportionality assessment of bulk metadata suffers from similar problems to those experienced elsewhere in trying to deal with big data. The privacy impacts may not be immediately obvious, they may only come after the data is mixed with other sources, or the processing may give new insights into a category of people not initially perceived as the target of the surveillance.

Purpose limitation and the Counter-Terrorism Act 2008

The report cites "use limitations" as a key element in assessing proportionality, with concerns about regimes that allow the "collection of data for one legitimate aim, but subsequent use for others". The UK Government has insisted that the safeguards around access to data present in RIPA and carried in stronger form into the IPA provide for limitations. However, at a more fundamental level, the Counter-Terrorism Act 2008 sets out that "Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions." (s. 19.2).

This loophole could make any proportionality assessment impossible in practice. It would be good for IPCO to seek assurances on the reuse of data and explain how the public can be certain that information collected under a specific bulk warrant is not used for completely different purposes.

Data minimisation

According to leaked documents, GCHQ appears to rely heavily on the Human Rights Act (HRA) for internal compliance and proportionality. Many leaked NSA and GCHQ documents make reference to the United States Signals Intelligence Directive 18 (USSID 18) and the HRA (Human Rights Act) in almost equivalent terms, and GCHQ repeatedly alludes to HRA compliance throughout its operations, from tasking to searches of collected materials.

---

[17] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

The partially declassified USSID 18 *Legal Compliance and U.S. Persons Minimization Procedures* was put in place in 1980 as part of the tightening of the US surveillance regime following the Watergate scandal. USSID 18 sets fairly detailed criteria for how information can be collected, processed, retained and disseminated. For example, it sets out that communications between persons in the US accidentally collected in foreign surveillance must be promptly destroyed.

Describing the UK HRA as equivalent may be useful for analysts to understand that they must act within limits, but they are not the same. The HRA only provides general principles for proportionality, in contrast to the detailed minimisation guidance in USSID 18. Without more specificity, reliance only on these general principles can result in lower standards of protection in the UK. Going back to the example above, as far as it is known, GCHQ analysts do not have an obligation to destroy UK communications that are accidentally captured.

Data minimisation should be mandatory, more detailed and built into the IPCO proportionality assessment and authorisation system, not left to general HRA compliance under internal GCHQ processes.

Access to other types of data

Bulk collection capabilities allow for the development of many projects not directly related to communications. German news organisation Der Spiegel revealed that the NSA, with the help of GCHQ, tracked financial transactions, including bank transfers and credit card transactions, and had collected some 180 million datasets by 2011.

This programme, referred to as “Follow the Money”, apparently led GCHQ’s lawyers to raise concerns about the collection, storage and sharing of such “politically sensitive" and "bulk data – rich personal information. A lot of it is not about our targets".[18]

While the data already obtained may be governed under the BDS provisions in the IPA, the obtention of such data using bulk surveillance warrants would require special scrutiny.

The CJEU Data Retention Ruling

In April 2014, the Court of Justice of the European Union ruled that the Data Retention Directive, which obliged ISPs to collect and keep personal communications data, interfered with privacy rights. The Court declared the Directive invalid because it failed to limit surveillance “to what is strictly necessary” and did, “not require any relationship between the data whose retention is provided for and a threat to public security”.[19]

[18] http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html

[19] https://wiki.openrightsgroup.org/wiki/Data_Retention_Directive#ECJ_incompatibility_ruling

We believe that these principles apply more generally to bulk and that the criteria of the court to make retention more proportionate would also mean that bulk warrants should be made more proportionate. We will not elaborate here on those proportionality criteria as they have been extensively discussed elsewhere.