1. Who we are

Open Rights Group is the UK's leading digital campaigning organisation, working to protect the rights to privacy and free speech online. With 3,200 members, we are a grassroots organisation with local groups across the UK. Our ethos is that we believe people have the right to control their technology, and oppose the use of technology to control people.

Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share and learn across the world. But for all the benefits, technological developments have created new threats to our human rights. We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions and technical projects.

We have engaged extensively in the pre-legislative process of the Bill and our Executive Director, Jim Killock, has given evidence to the Joint Committee.

2. Scope of the filter as a power

What is the Request Filter?

The Request Filter is described by the Home Office as a safeguard designed to reduce the collateral intrusion produced in searching for small, specific information in a large dataset[1].

However, because the Request Filter allows automated searches of very large datasets it can comprise a highly intrusive search facility that has the potential for population profiling, fishing trips and generation of new data.

In both evidence to the Joint Committee and in the code of practice, the Home Office describes the filter in terms that severely understate its impact and intrusiveness. The Bill itself offers no meaningful restraint to the operation of the Request Filter.

How is the Request Filter defined in the Bill and Code of Practice?

[1] See Filtering Arrangements Factsheet or Home Office evidence to Joint Committee http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26435.html

Clause 58 of the Bill describes in very general terms the “filtering arrangements for obtaining data”, giving power to the Secretary of State to make the necessary arrangements for obtaining, processing and disclosing data. There is no description of what “filtering” means and no stated purpose to reduce the amount of data to be disclosed.

On the face of the Bill the filter’s only function is simply to help a designated senior officer deal with data requests. Indeed, the choice of the term “filtering” appears to be completely arbitrary, and “data access and processing arrangements” would appear a more accurate description. It is impossible to understand what the “filter’ is meant to be just from reading the Bill.

Clause 59 simply sets out that the filter has to be used under specific authorisations and that the designated senior officer must consider that it is proportionate. The BIll does not provide any specific criteria to establish proportionality.

Clause 60 sets the procedures for the handling of the data - access, disclosure, security, destruction, etc. - which are mainly straightforward but not detailed and include arrangements for oversight by the Investigatory Powers Commissioner.

Section 9 of the DRAFT Code of Practice on Communications Data provides more information, explaining that the Filter is designed to speed up complex queries and “reduce the analytic burden on public authorities” (9.3).

The Code makes the argument that the Filter is a privacy “safeguard” because it will “limit the volume of communications data being provided to a public authority”. However, this seems to be based on unwarranted expectations. The Code sets the possibility that the Filter *may* be used to minimise collateral intrusion (9.7), but there is no obligation in the Code for the tool to be used in this way.

The Code includes some guidance on proportionality (9.9-10) and more details on data management, oversight and reporting.

What sources of data can be interrogated by the Request Filter?

The Filter appears in the Part of the Bill that deals with authorisations for Communications Data. This means that any data retained under Part 4 of the BIll could be accessed and processed.

Who has access to the Request Filter?

The Code specifies that the Filter can be used as part of a “targeted communications data authorisation”, available to all relevant public authorities to assist in obtaining the

communications data that they are permitted to use. Schedule 4 of the Bill contains a list which includes the Food Standards Agency and NHS trusts.

Security and Intelligence Agencies can acquire communications data in bulk under the provisions in part 6 of the Act, but the Code explains that they must consider a "less intrusive power" such as the Filter as an alternative (9.4).

Method of authorisation

The Filter is integrated in the authorisations for "targeted communications data", which is described in detail in the Code. The Single Point of Contact (SPoC) will advise the investigator (applicant) on the suitability of using the Filter, and a Designated Senior Officer may impose restrictions during the authorisation.

The SPoc will receive the results and will be responsible for managing compliance. The Code sets out that proportionality must consider "future evidential requirements" through follow up requests, but does not spell this out in enough detail.

The only constraints in both the Bill and the Code of Practice are general requirements that the searches must be justified as necessary and proportionate during the application process.

How will the Request Filter operate?

The Filter will be operated on behalf of the Secretary of State by one or more unspecified third parties[2], which will sit between public authorities and CSPs.

Adrian Gorham from Telefónica described the filter to the Joint Committee in simple and clear terms: "a third party will take bulk data from us and analyse it for the police"[3].

The filter will introduce a two step process that in some cases may reduce the data that is disclosed to the investigators originating the request, but not the amount disclosed by CSPs to the organisation operating the filter. However, by centralising and facilitating the processing of data, the filter will likely increase the overall flow of communications data from CSPs. European courts have repeatedly clarified that intrusion starts the moment data is retained, not at the end point of disclosure[4], and introducing a two step funnelling of requests does not necessarily minimise the overall intrusion.

---

[2] DRAFT CoP Communications Data 9.16

[3] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/26271.html

[4] See for example CJEU C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others

3. What are the capabilities of the filter?

(a) The Home Office View

The Home Office stresses that the request filter is not a data mining tool or a search engine and simply provides efficiencies over the same capabilities in place today.

(b) Federated searches

The filter will have the ability to search all records across many datasets, including location data, web data and phone records. The new retention requirements and introduction of ICRs provide a much richer source of information than it is available today. Location data will become much more detailed once mobile internet usage is routinely recorded. The Internet of Things will also increase the data available to the Home Office, as personal devices, cars, thermostats and lighting get commented to the internet. The filter will glue those disparate data sources into a "federated database", as acknowledged by Parliament when these proposals were rejected in 2013 as part of the Communications Data Bill.[5]

(c) Complex queries

The filter will be able to perform complex queries over such database. The Home Office has presented the example of matching location data to identify who was present at various places linked to a murder investigation, but location matches could be equally used to identify flying trade union pickets. By combining location and internet data the Home Office could identify not just participants at protests, but the organisers. Queries could be constructed along known modus operandi or patterns of life of target groups without the need to expressly profile individuals.

(d) Generation of new information

The filter may not simply match records and provide these to investigators. The system is described as being able to *generate* new information, which is a major step. Clause 58.2.b mentions "obtaining the target data or data from which the target data may be derived."

A particular concern is the lack of explicit controls over multiple queries, a well known information security problem. This issue was raised by Mark Hughes from Vodafone during evidence to the Joint Committee: *"more work needs to be done through consultation to ensure that we—again, going back to my previous point about intrusiveness—level up if*

---

5 http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/news/full-publication-of-report/

multiple questions lead to a point where it is becoming overintrusive (sic).”[6] In some cases, even a negative reply that did not generate any data can be an insight to investigators, and combining various negative replies can help identify a target. As we mention above, the Code sets out some general concerns but no detailed guidance.

3. Retention of information from the filter

According to the Home Office, the request filter will not retain any communications data acquired for an authorisation once the processing for that authorisation is complete or it is no longer necessary to retain the data for the purpose of the authorisation.

It is welcome that that bill sets out an obligation to delete data when no longer needed, but this should be made more prescriptive.

The CoP for Communications Data states that communications data associated with an authorisation will be temporarily retained in the request filter until either the authorised processing is complete, and those operating the request filter may periodically check with the relevant SPoC whether an authorisation remains valid if it has not been able to complete the processing (p. 64).

It is unclear how long the authorisations will be in place for, and it is possible that data could be kept in the filter for longer that its 12 month retention period. The CoP also states that deletion is independent of CSP retention systems which will continue to hold the data for their normal retention period, but once that data is deleted by CSPs it should also be deleted by the filter.

4. How to restrain the Request Filter

ORG’s view is that the Request Filter should be deleted from the Bill. While data correlation and minimisation techniques can be legitimately used, we believe that provision of a common front end search to highly intrusive datasets is simply too open to abuse and mission creep.

The filter is not a safeguard but, as the Code makes clear, functionally equivalent to a bulk access and processing system; and elsewhere in the bill those are subjected to judicial authorisation and restricted to the more serious cases that may require surveillance.

---

6 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25977.html