Consultation response: Open Rights Group

1 Compliance with the EU judgment

We are pleased that the Government is introducing a new independent authority to process requests for communications data. We have argued for independent authorisation consistently, on the basis that it reduces the risk for abuse. Cases of abuse have since come to light, even after the range of self-authorising agencies was reduced, including requests for journalists' information.

Independent authorisation is a key safeguard against corruption and abuse, thus should have the effect of improving police performance and trust in policing. There is everything to be gained from it, so it is perplexing that independent authorisation should have been resisted for nearly two decades until a court has made it plain that it must be implemented.

We are disappointed that the Government has decided to ignore several requirements of the judgment This can have no legal basis.

For avoidance of doubt, the requirements laid down in DRI[1] are to be found in paragraphs 59-68:

1. Retention cannot be general and indiscriminate, but must be focused on a particular need, such as a group, location and / or time period (para. 59);
2. Use of retained data must be limited to serious crime (paras. 60-61);
3. Retention periods need to be limited to what is strictly necessary (paras. 63-65);
4. Data needs to be held securely, destroyed when no longer retained, and that needs to be explained in law (paras. 66-67); and
5. Data must be retained within the EU (para. 68).

The Watson judgment added two further criteria:

1. Persons whose data is accessed must be notified, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities (para. 121);[2] and

[1] ECLI:EU:C:2014:238 (para. 59-68)

[2] "Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities.

2. Persons whose data is held must continue to have rights over their data (para. 123).[3]

The same judgment reiterates that the DRI criteria apply to member states and discusses at some length how retention cannot be generalised. We are disappointed that the Government does not concede this and instead has decided to exacerbate the problems, firstly by extending what is to be retained, and secondly by introducing new analytics capabilities called the "Request Filter" without understanding the limits these judgments place on them, and without introducing clear restraints.

To be clear, the court made it clear that all of the requirements outlined in the *Digital Rights Ireland* judgment ("DRI") applied equally to all member states.[4] Even if the Government argues that certain requirements were discussed in detail only in relation to the Swedish reference, that makes no difference to the fact that ***all requirements apply to all member states***.

That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy" (para. 121).

[3] "Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data" (para. 123).

[4] ECLI:EU:C:2016:970 (para. 125)

The mission of the Home Office is to provide for the enforcement of the law. Its work should provide the most basic support for the rule of law, without which society cannot properly function. For the Home Office to disregard key requirements of court judgments at its whim is therefore an extremely dangerous step. After all, if the Home Office ignores the courts and evades their will, why should anyone else pay attention to them?

2 Dismissal of notification rights

Despite the CJEU's insistence that notification is "necessary to enable the persons affected … right[s] to a remedy" the consultation dismisses the need for any change, in effect, continuing to deny people adversely affected the right to a remedy. Instead, only problems judged to be serious errors by oversight bodies will be notified. The document dismisses the CJEU's demand, stating:

> The Government's position is that a general requirement to notify an individual that their data has been accessed would unnecessarily inform criminals, suspected criminals and others of the investigative techniques that public authorities use.[5]

That is simply an admission that the Government disagrees with the Court, so has decided to ignore it. Further, the judgement provides for restriction of notification "for as long as it is liable to jeopardise the investigations being undertaken" which is not a "general requirement to notify" as the Government presents it. The Government appears to have deliberately misinterpreted the conditioned notification requirement from the judgement as a general requirement to notify. This should be rectified immediately.

Notification is a vital safeguard against abuse. General statements of concern about investigative techniques cannot be applied here: data is available; it is known that data is retained, thus methods of investigation are fairly obvious. Data evidence is used in court. The use of data analytics is also well known. These are not secrets.

Safeguards can be placed in specific circumstances so that notification does not always take place.

3 Extension of data retention

The Code introduces new kinds of data to be collected and retained, without explaining how this fits in with the judgments demand to limit retention. The DRI judgment stated that

[5] IPA Consultation document (pg. 20)

> … whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[6]

These criteria should be applied to the current regime before attempting to extend it.

4 Six-month threshold for "serious crime"

The Government cite some specific cases of six month sentencing for grooming in order to justify a general six month threshold.[7] This seems unnecessary. If the Government wants specific crimes such as grooming counted within a list of serious crimes, it could apply a general threshold of three years, with specific offences included in addition. There is no need to create an especially low bar for use of collected data when the CJEU have been entirely clear that such data must be used only for serious crimes.

5 The Request Filter

We welcome the fact that some attempt to describe the operation of the "filter" has made it into the draft Code of Practice. Nevertheless, the code of practice is a general description and does not appear to impose the constraints that we would expect from primary legislation. Constraints should be placed into the IP Act to ensure that any Request Filter is a tool designed for the narrow purpose of specific data analytics, and that data analytics are themselves not conducted in a broad and generalised manner.

Some of the examples in the Code of Practice do not give us comfort. For instance,

> *… the authorisation should consider the likely effectiveness of the specified criteria in achieving the expected reduction in records. For example a large number of people are likely to be in both Brighton Station at 07.30 on a Monday and London Victoria at 09.00 the following Thursday.*[8]

---

[6] ECLI:EU:C:2014:238 (para. 59)
[7] IPA Consultation document (pg. 14-16)
[8] Draft communications data code of practice (para. 11.7)

Such an approach risks exacerbating the problems outlined in the DRI judgment, which stated that retained communications data:

> … make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.
>
> Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[9]

The Request Filter aims to take advantage of these data to make "precise conclusions" by drawing on large volumes of initial data. It is presented as a privacy safeguard but it is in essence a highly intrusive tool that will examine many people's data in order to produce very specific results.

These results may be relatively simple (a person at two locations) or very detailed and complicated to deduce (a person in a certain social sphere with a particular regular habit that knows a particular person). They turn retained data into a very powerful tool; the existence of the Request Filter is itself an argument for the reduction of the retained data available to it, in the terms set out by the DRI judgment, because it makes the retention considerably more intrusive.

Aside from security arrangements, the only reference in the code to privacy safeguards for people whose data is queried is that:

> The authorisation should also consider the proportionality of the data to be disclosed to the request filter by the telecommunications operators or postal operators, even if the majority is not expected to be released to the public authority.

This appears to be optional, as it employs the language "*should"* rather than "*must"*, and no guidance is given as to how that proportionality might be calculated. In practice, how this undefined balance is applied lies at the heart of whether this tool is either a useful and

[9] ECLI:EU:C:2014:238 (para. 26-27)

necessary addition to the police toolkit, or an intrusive and unwarranted extension of surveillance capabilities designed to turn retained data into a readily searchable database of the activities of the population as potential suspects.

It is unclear how data requests to ISPs will take place, but they may over time become automated. They should not be, in our view, but should take place on a case by case basis, and this should be clear in the code.

There are also evidential questions that will require transparency over the nature of queries made, if the results are to be trusted by the courts, especially as defence lawyers will not have same opportunities to design queries that could demonstrate the innocence of their clients.

Analysis of data could contain algorithmic processes, and machine learning which could create errors or biases, and could lead to profiling. This would be dangerous without considerable consultation and should be clearly ruled out in this Code of Practice. At this point, the Code does not make it clear what kinds of data searching and matching techniques will be used.

Safeguards must be spelled out and include:

1. A reduction in retained data, along the lines demanded by the CJEU judgment, to limit the potential intrusion from the filter;
2. Objective, defined limits to explain what size and kinds of dataset may proportionate to be brought into a search;
3. Individuals should be able to discover if their data has been accessed, whether or not they are the focus of a query;
4. Limitations to the use of the Request Filter to serious crimes as defined in section 263 of the Investigatory Powers Act 2017;
5. A prohibition on automated requests to data holders and a requirement for requests to be reviewed by a senior person at an organisation receiving a request;
6. The ability for an ISP or data holder to refuse a particularly broad data request, and ask for an appeal;
7. Regular reviews of data requests by the Commissioners;
8. Public information about the scale of data accesses made, including numbers of records, numbers of persons and size of files per search;
9. Rules to control machine learning and preclude the use of profiling techniques;

10. Rules to ensure the full transparency of algorithms used to produce evidential conclusions;
11. Transparency to the courts of the specific nature of queries and searches when relied on for evidence;
12. The nature of the search and data queried should be clear in any notifications made to persons who have been investigated.

6 Transfer of data outside the EU

The Government rejects the requirement to keep retained data within the EU, on the basis that companies may be retaining it outside of the EU for business reasons. However, rejecting this requirement enables easy transfer to intelligence agencies outside of the EU, particularly the USA. This would not be acceptable. If it is not the Government's purpose to pass data in bulk to overseas' agencies, then the law should clearly rule it out.

The requirement imposed by the court makes sense because of the lack of protection for privacy rights in countries such as the USA, which do not give regard to the privacy of non-citizens. It is a rich data source and would be valuable for many countries' surveillance purposes. Companies handling the data would find it hard to resist governmental claims over it if it is stored in the USA and some other jurisdictions, so it should remain within the EU.

7 Conclusion

It is not for the Government to reinterpret the judgment of court, but to apply it.

The approach in the current draft Code of Practice will be open to further legal challenges, at cost to the taxpayer and to the government's claim to respect the law.