BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Big Brother Watch's response to the Government's consultation on the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention and acquisition of communications data

January 2018

CONTENTS

INTRODUCTION

Big Brother Watch welcomes the opportunity to provide a submission on this important topic. However, the Government is long overdue in amending the communications data regime following the CJEU's clear finding.

The Court of Justice of the European Union (CJEU) gave its judgment on 21 December 2016 on the joined cases *Tele2 Sverige AB v Post- och telestyrelsen* (Case C-203/15) and *R (Watson) v Secretary of State for the Home Department* (Case C-698/15) ("*Watson*"), specifying a number of requirements that need to be in place for a Member State's data retention regime to be compliant with EU law.

The Government has launched a public consultation on its proposed response to the CJEU's ruling one year later, on 30th November 2017.

The Court was clear in *Watson* that the UK's current communications data surveillance regime is unlawful in view of EU data protection laws and the European Charter of Fundamental Rights. The Court ruled on two issues in relation to communications data. The first element precludes the general and indiscriminate retention of communications data. The second clarifies that communications data may only be retained and accessed in relation to fighting serious crime, after independent authorisation has been granted, in addition to other safeguards. In light of the CJEU's judgment, the UK's regime urgently requires a serious overhaul.

We are perplexed by the Government's strategy to consult the public on the effect of the CJEU's judgment. Compliance with the law is not a matter for public deliberation. It is additionally concerning that the Government is consulting the public on proposed amendments that clearly seek to reject or evade significant requirements of the CJEU's judgment. Any amendments that fail to meet the standards required by law will be illegitimate, regardless of whether they follow a public engagement exercise.

In our response we cite the CJEU's judgment, which makes clear the express mandatory standards for the communications data regime. Government must respect these standards to uphold fundamental rights and liberties in the UK, as well as to ensure the UK's adequacy with EU law.

Summary and scope of the judgement

1. Application of the judgement to entity data

The Investigatory Powers Act 2016 ('IPA') contains an impractical number of data definitions, including:

- '(relevant) communications data' which may include
    - 'entity data'
    - 'events data',
    - 'internet connection records'
- 'secondary data' or 'equipment data' which may include
    - 'identifying data'
    - '(related) systems data'.

In its response to the CJEU's judgement, the Government argues that "*the CJEU's judgement should be read as applying to "events data" but does not apply to the retention or acquisition of "entity data",*[1] as defined in the IPA. This position arises from the Government's interpretation that "*The CJEU judgment refers to only certain types of communications data – traffic data and location data, as defined in Directive 2002/58/EC ("the ePrivacy Directive").*"[2] However, this interpretation is wrong. The CJEU's judgment did not distinguish different standards for traffic and location data to those for other communications data, but rather considered the national communications data regime as a whole. Furthermore, no such distinction was made in the Order for Reference from the Court of Appeal, or indeed by the Government following that Order. In fact, the Court of Appeal referred expressly to the communications data regime in the whole, identifying all of the categories of communications data contained.[3] The assertion that the judgment should apply only to 'events data' in the IPA is evidently wrong.

The CJEU's judgment recites Directive 2006/24/EC, which applies "*to traffic and location data on both legal entities and natural persons* ***and to the related data necessary to identify the subscriber or registered user.***"[4] The Court considers communications data to include data

---

[1] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.11

[2] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.10

[3] The judgment of the Court of Appeal, which made the reference to the CJEU, explained that communications data "*fall into three broad categories*" *including "(1) subscriber data: information held or obtained by a communications service provider… in relation to a customer, for example their name, address and telephone number*" [2016] 1 CMLR 47 at [5].

[4] European Union Directive 2006/24/EC, (Data Retention Directive), 15 March 2006 (emphasis added).

"…relating to subscriptions and all electronic communications ***necessary to trace and identify the source and destination of a communication****"*,[5] and also notes that *"(t)he data which providers of electronic communications services must therefore retain makes it possible to trace and* ***identify the source of a communication****"*.[6] The Court goes on to state unequivocally that "*that data includes, inter alia,* ***the name and address of the subscriber or registered user, the telephone number of the caller, the number called and an IP address for internet services."***[7] *Watson* clearly applies to communications data the Government has defined as 'entity data'.

'Entity data' under the IPA includes location data

The Government suggests that the CJEU's judgment applies only to 'events data', which concerns traffic and location data, but does not apply to 'entity data' because – the Government argues – it does not include traffic or location data. 'Entity data' is defined in Part 9, Chapter 2 (Interpretation) of the IPA as:

> *(3) "Entity data" means any data which –*
>
> *(a) is about –*
>
> *(i) an entity,*
>
> *(ii) an association between a telecommunications service and an entity, or*
>
> *(iii) an association between any part of a telecommunication system and an entity,*
>
> *(b) consists of, or includes, data which* ***identifies or describes*** *the entity* ***(whether or not by reference to the entity's location)****, and*
>
> *(c) is not events data.*

In fact, 'entity data' as defined in the IPA explicitly includes location data. Even on the basis of the Government's restrictive and incorrect interpretation of the CJEU's judgment, the judgment still applies to both 'events' and 'entity' data. As such, 'entity data' that identifies a subscriber of a home phone and broadband service includes the individual's address.

Policy recommendation

- ***Watson*** **applies to the communications data retention and acquisition regime as a whole. Amendments must apply to the communications data regime as a whole, including both 'entity' and 'events' data in the IPA.**

[5] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para 17
[6] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para 98
[7] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para 98

2. Application of the judgment to national security

In its response to the CJEU's judgment, the Government has stated, "*the Government's position is that the judgment does not apply to the retention or acquisition of data for national security purposes".*[8]

Furthermore, Government considers that the three UK intelligence agencies, which bear great responsibility for investigating serious crime, are exempt from the CJEU's judgment: "*the Government considers that* [MI5, MI6 and GCHQ's] *activities, **including requests for communications data for the statutory purpose of crime**, fall outside the scope of EU law and the CJEU's judgment".*[9]

Despite stating this illogical position, the Government is not consulting on this issue.

However, Big Brother Watch finds the Government's position unacceptable and urges reconsideration.

The CJEU's judgment applies to the communications data regime and the activities of telecommunications operators who retain their customers' data – to which EU law clearly applies.

The CJEU explicitly addressed the fact that some data retained by companies is subsequently used in the national security context, and made clear the restrictions that the European Charter of Fundamental Rights applies to data collection for a general purpose:

> *"Further, while the effectiveness of the fight against serious crime, **in particular organised crime and terrorism**, may depend to a great extent on the use of modern investigation techniques, **such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention** of all traffic and location data should be considered to be necessary for the purposes of that fight".*[10]

[8] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.11

[9] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.11 (emphasis added)

[10] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 103 (emphasis added).

The CJEU's judgment is clear that communications data may not be retained for a *general* national security purpose, but data may be retained if it relates to a specific threat to public security or a serious criminal offence.[11]

The Government's position that the Agencies should not be subject to the CJEU's ruling, even where data is sought in relation to crime, is particularly objectionable and demonstrates an open disregard for the CJEU's judgment. The adoption of this proposal would mean that a significant amount of communications data sought in the UK would be retained and accessed in absence of the mandatory safeguards required by law, and would remain accessible via self-authorisation within the Agencies. We urge Government to reconsider this plainly unacceptable position.

Policy recommendation

- ***Watson* applies to the communications data retention and acquisition regime as a whole. Furthermore, the judgment is clear that national security as an objective of general interest does not negate the necessity of mandatory safeguards. Amendments to the communications data regime must be applied to all competent public authorities, including the UK's three intelligence agencies.**

[11] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 106

Scope and permissibility of the regime

3. Permissibility of a retention regime

The CJEU's judgment was clear that the retention of mass communications data for a general purpose is incompatible with Charter rights. This important ruling necessitates vital change to the UK's communications data regime.

The Government acknowledges the principle of the CJEU's judgement, reciting the Court's first ruling:

> *"(EU law) must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication".*[12]

However, the Government appears to be seeking to evade the effect of the ruling by declaring in the consultation paper that, "*we do not consider that the existing data retention regime is 'general and indiscriminate'".*[13]

The UK's retention regime is plainly general and indiscriminate, as it captures the data of millions of people who are of no intelligence interest. In any event, the UK regime must be subject to the safeguards expressly required by the CJEU's judgment. Specifically, the regime must "*require there to be* [a] *relationship between the data which must be retained and the threat to public security*" – without such a targeted purpose, retention is incompatible with Articles 7, 8 and 11 of the Charter and *"cannot be considered to be justified, within a democratic society".*[14] The CJEU's judgment allows for a regime where data is retained on a targeted basis for the purpose of fighting serious crime where the persons concerned, categories of data retained, means of communication affected, and retention period are limited to what is strictly necessary.[15]

This is clearly not the case with the UK's current data retention regime, which permits the general retention of communications data relating to the majority of the population.

---

[12] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970)
[13] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.14
[14] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): paras. 106-107
[15] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 108

Despite believing it does not need to reform, the Government has proposed an amendment that would merely to add to a list of factors that the Secretary of State should consider when issuing a data retention notice to a telecommunications operator. These factors include a consideration of the operator's services to which the notice should relate; *whether* it would be appropriate to restrict a notice by geography or to exclude groups of customers; and to "*take into account"* the statutory purpose for which a notice is being given (e.g. for the prevention and detection of crime).[16] The fact that the considerations include *whether* it would be appropriate to restrict a notice by geography or to exclude groups of customers demonstrates that the default position will be to issue mass data retention notices that are not restricted solely to specific suspects or investigations.

The CJEU's judgment explicitly stated that "*the system put in place by Directive 2002/58 requires the retention of data to be the exception"*[17] – however, the retention of millions of innocent people's data remains the rule in the UK. These proposed factors for consideration do nothing to ensure that there is a direct link between data retained and a specific security threat or serious crime, as required by law, resulting in the continuation of an unlawful communications data regime in the UK.

Policy recommendation

- **The UK's communications data regime must require there to be a relationship between the data ordered for retention and the specific threat to national security or serious crime investigation.**

[16] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.14

[17] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 104

4. Restriction to serious crime

The second ruling of the CJEU's judgment was clear that the ePrivacy Directive, read in light of the EU Charter of Fundamental Rights,

> "*(…) must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access,* ***in the context of fighting crime, is not restricted solely to fighting serious crime*** *(…)"* [18]

Furthermore, it made clear that "*prior review by a court or an independent administrative authority*", and retention of the data concerned "*within the European Union*", are necessary safeguards for the communications data regime to be lawful.[19]

There is an overarching definition of serious crime in the IPA, which, in light of the CJEU's judgment, should be incorporated into the communications data regime as a safeguard. However, Big Brother Watch is concerned that the Government proposes introducing a new watered-down definition of 'serious crime' that clearly does not qualify as 'serious crime'. Such an approach would fail to bring the UK's communications data regime into line with EU law, falling short of our obligations under the EU Charter of Fundamental Rights in particular.

The proposal to redefine serious crime

'Serious crime' is defined in s.263 of the IPA as:

- conduct involving the use of violence,
- conduct that results in substantial financial gain,
- conduct by a large number of persons in pursuit of a common purpose;
- an offence for which an adult **could reasonably be expected** to be sentenced to **three years or more in prison**.[20]

However, the Government proposes redefining 'serious crime' in the context of communications data by introducing a parallel, but extremely watered-down definition. Furthermore, it proposes that this emaciated safeguard apply only where 'events data' is sought[21] – not 'entity data' – on

---

[18] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970)
[19] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970)
[20] Investigatory Powers Act 2016, s.263
[21] The Data Retention and Acquisition Regulations 2018 (Draft Statutory Instruments), amendment of section 61, p.3: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/663677/November_2017_IPA_Consultation_-_Draft_regulations_amending_the_IP_Act.pdf

the basis of its incorrect, overly restrictive interpretation of the CJEU's judgment (see section 1 of our response, pp.4-5).

The new definition would drastically weaken the existing serious crime definition with the following additions:

- an offence for which an adult **should be capable of being** sentenced to **six months or more in prison,**
- **any offence "*by a person who is not an individual*",** and
- **any offence which involves "*the sending of a communication*".**[22]

This proposal represents an unacceptable evasion of the CJEU's judgment and the fundamental rights that protect UK citizens from undue interference.

This proposal would set a threshold so low as to be, in practice, almost meaningless. It would permit UK authorities to access 'entity data' on exactly the same basis as in the current, unlawful framework, whilst 'events data' could be accessed to investigate offences as minor as possession of diazepam for personal use, for example. In fact, in a meeting at the Home Office regarding this consultation, Big Brother Watch and others were told that the only offences not included in this definition of 'serious crime' would, in practice, be summary offences – e.g. motoring offences.

This proposed amendment is in direct conflict with the CJEU's clear judgement, that:

> "*Given the seriousness of the interference in the fundamental rights concerned (…)* ***only the objective of fighting serious crime is capable of justifying such a measure*** *(…)".*[23]

Protection from harassment

A reason often cited for rejecting or drastically reducing the serious crime threshold in the communications data context is that such data is valuable in investigating stalking and harassment cases, many of which (it has been suggested) do not qualify as 'serious crime' under the IPA definition. We recognise the value of communications data in such cases. However, we think the very separate issue of low sentencing for these crimes does not make it rational to disregard the legal requirement for a serious crime threshold in the communications data context.

[22] The Data Retention and Acquisition Regulations 2018 (Draft Statutory Instruments), amendment of section 87, pp.5-6

[23] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 102

A more sensible approach would be to insert the serious crime threshold (as defined in s.263 of the IPA) into the communications data regime, and to specifically include offences under the Protection from Harassment Act 1997 as those for which communications data can also be sought.

Often, stalking and harassment cases involve the 'use of violence' and thus qualify as serious offences under s.263 for which access to communications data would be permitted. In any event, the specific inclusion of the Protection from Harassment Act 1997 would acknowledge the seriousness of such offences and the fact that communication is often the primary tool of those offenders.

An invalid proposal

The Government's proposal to weaken the meaning of 'serious crime' in the communications data context would be not only an evasion of the CJEU's judgment, but would also be practically unworkable.

This is because Government has already sought to create watered-down thresholds in the IPA for access to a particular subtype of communications data – internet connection records (ICRs).

After the Shadow Home Secretary lobbied for the serious crime threshold to be applied as a safeguard for access to ICRs,[24] the Government inserted a threshold of 'serious crime or other relevant crime' as an apparent compromise. This 'safeguard' is only invoked where the identity of the individual concerned is already known, and defines 'other relevant crime' as:

- an offence for which an adult **should be capable of being** sentenced to **twelve months or more in prison,**
- **any offence *"by a person who is not an individual"*,** and
- **any offence which involves *"the sending of a communication".***[25]

The Government initially proposed that 'other relevant crime' include offences capable of incurring a *six* month sentence – exactly as per the new serious crime definition proposed in present consultation – but this was rejected.

As it stands, ICRs can be accessed under the IPA in relation to 'serious crime or other relevant crime'. However, if the Government's proposed legislative amendment to weaken the serious

---

[24] *Letter to the Home Secretary on the Investigatory Powers Bill* – Andy Burnham MP, 4th April 2016, http://andyburnhammp.blogspot.co.uk/2016/04/letter-to-home-secretary-on.html: "*I do not think it is necessary or proportionate for information held in ICRs to be accessed in connection with lower-level offences. Instead, I think* ***this threshold should be set at serious crime and that this should be defined in the Bill as an offence that attracts a maximum sentence of not less than three years in prison."***

[25] Investigatory Powers Act 2016, s62(5) and (6)

crime threshold were adopted, the meaning of this ICR 'safeguard' would be diluted further still. This is because the proposal would redefine the meaning of 'serious crime' for the purposes of Parts 3 and 4 of the IPA. Consequentially, 'serious crime or other relevant crime' would not correspond to offences that could reasonably be expected to incur a three year sentence, or other relevant crime, but rather offences that theoretically could incur a sentence of six months in prison, or other relevant crime.

The Government's proposal therefore lacks competence. More importantly, it would plainly fail to restrict the use of communications data to serious crime and thus would perpetuate a complex and unlawful communications data regime.

Suspicion of serious crime

The CJEU's judgment is clear that only the data of persons suspected of involvement in serious crime can be accessed:

> *"access can, as a general rule, be granted, in relation to the objective of fighting crime,* ***only to the data of individuals suspected of planning, committing or having committed a serious crime*** *or of being implicated in one way or another in such a crime."*[26]

Individualised suspicion where data is sought for the purpose of preventing or detecting crime is a clear requirement in law and is a general safeguard similarly required for the use of investigatory powers by *Zakharov v Russia*[27] and *Szabó and Vissy v Hungary.*[28]

Currently, there is no objective threshold of individualised suspicion in the IPA and data can be sought merely when it is deemed necessary and proportionate for the general purpose of preventing and detecting crime. This is at odds with the CJEU's judgment.

Specificity and national security

Where data is sought for national security purposes, *Watson* does not require an objective threshold of suspicion of planning, committing or implication to be met. However, it is clear that objective evidence is required to demonstrate that the data sought is necessary to combat a specific threat, rather than merely sought for a general purpose. The judgment reads:

> "*However, in particular situations, where for example* ***vital national security****, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is* ***objective evidence*** *from which it can be*

[26] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 119 (emphasis added)
[27] Zakharov v Russia (App No 47143/06, 4 December 2015, Grand Chamber) [260]
[28] Szabó and Vissy v Hungary (App No 37138/14, 12 January 2016, Fourth Section) [71]

*deduced that that data might, **in a specific case**, make an effective contribution to combating such activities".*[29]

Big Brother Watch is concerned that the Government has not acknowledged the requirement of individualised suspicion of serious crime, or specificity in relation to national security, in its proposed amendments. These vital safeguards are required in the IPA if the UK's framework is to comply with the law.

Policy recommendations

- **Where communications data, either 'entity' or 'events' data, is retained or accessed for the prevention and detection of crime, it must only be sought in relation to serious crime as defined in s.263 of the IPA, or in relation to offences under the Protection from Harassment Act 1997.**
- **In relation to serious crime, only the communications data of individuals suspected of involvement in a serious crime may be sought.**
- **In relation to national security, data may only be sought where there is objective evidence that it will make an effective contribution to a specific threat.**

[29] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 119 (emphasis added)

Access safeguards

5. Independent authorisation for access to communications data

The Government accepts that *Watson* requires independent authorisation of requests to access communications data:

> "*The CJEU's judgment is clear that requests to acquire retained communications data must be approved by a court or independent administrative body".*[30]

The Government proposes establishing a new, non-judicial, administrative body to authorise requests on behalf of the Investigatory Powers Commissioner, to be named the Office for Communications Data Authorisations ('OCDA').

The case for judicial authorisation

Big Brother Watch believes that independent authorisation for access to communications data should be judicial. Judges are best placed to evaluate the important legal tests of necessity and proportionality, which safeguard individuals' rights from unlawful interference. It is the constitutional function of our independent judiciary to oversee application of the law to individuals and to act as a check on the State's use of intrusive powers on its own citizens.

A weakened safeguard for urgent requests

Under the Government's proposals, independent authorisation by OCDA would not need to be sought in urgent cases. Urgent requests for access to individuals' data would be authorised internally within a public authority by a designated senior officer. It is quite unlike the other urgent authorisation procedures in the IPA that the proposed amendments would not provide for the authorising body (in this case the OCDA) to be notified of urgent requests and consider them retrospectively. This is clearly an oversight by Government and a missed opportunity to ensure consistent procedural accountability.

A weakened safeguard for local authorities

Big Brother Watch has long campaigned against the disproportionate use of surveillance powers by local authorities. Following the amendment of RIPA by the Protection of Freedoms Act 2012, which required a magistrate's authorisation for local authorities' use of investigatory powers, the IPA requires a magistrate's approval for local authorities' use of IPA powers. Much was made of this reform, including by the then Home Secretary, now Prime Minister, Theresa

[30] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.18

May, although for many of those on the Government's back benches, this safeguard was still seen as inadequate.[31]

However, the Government's new proposals would remove this important safeguard in favour of administrative approval from the OCDA and in fact make it easier for local councils to use intrusive investigatory powers. We are concerned that this marks a return to a purely administrative request and authorisation procedure by which local authorities can be empowered with intrusive investigatory powers. This proposal represents a particularly unwelcome rollback on existing safeguards.

Policy recommendations

- **Judicial authorisation should be sought by all public authorities for access to communications data. Access safeguards for local authorities must not be weakened.**
- **The independent authorising body should be notified of any urgent requests granting access to communications data to enable post-facto review.**

[31] For example, see Second Reading of the Investigatory Powers Bill in the House of Commons, 15 March 2016 – Hansard, vol. 607: https://goo.gl/HoO19W

6. Notification

The CJEU's judgment expressly requires authorities who access communications data to notify the persons affected.

The Court is clear that this is required for two reasons: firstly, to ensure that the range of mandatory safeguards are upheld; secondly, to enable persons affected to access legal remedy.

The CJEU ruled that:

> *" (…) 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.* ***That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy*** *(…)"*[32]

Big Brother Watch is incredibly disappointed that the Government has not proposed amendments to respect this important element of the CJEU's judgment. The Government has denied adding provisions for notification on two, somewhat conflicting, bases: the first is that it does not need to make any changes as the current framework is adequate; the second is that it practically cannot meet this requirement.

The necessity of post-notification

EU law is clear that notification is necessary both to enable individuals to access their right to a legal remedy, and as a general safeguard.

Watson clarifies that notification is a vital general safeguard *"to ensure, in practice, that those conditions* [other safeguards] *are fully respected".*[33] Notification provides an important measure of accountability, which is vital in the context of the *"very far-reaching"* and *"particularly serious"* interferences with Articles 7 and 8 of the Charter as described by the Court:

> "*The fact that the data is retained* ***without the subscriber or registered user being informed*** *is likely to* ***cause the persons concerned to feel that their private lives are the subject of constant surveillance****".*[34]

[32] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 121 (emphasis added)
[33] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 121
[34] Court of Justice of the European Union, Judgement of 21.12.2016 -Joined Cases C-203/15 *Tele 2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970): para. 100

The CJEU's judgment referred to *Digital Rights Ireland,* which was unequivocal on the necessity of notification as a safeguard for citizens' rights:

> *"It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, (…),* ***wide-ranging****, and it must be considered to be* ***particularly serious****. Furthermore, (…), the* ***fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance****."*[35]

Despite the clear legal requirement, the Government contends that it does not need to provide for a notification procedure for two reasons: first, that a "*person who believes that investigatory powers have been unlawfully used against them can make a complaint to* [the Investigatory Powers] *Tribunal";*[36] and second, that *"the Investigatory Powers Commissioner can notify a person if a serious error occurs".*[37]

Both of these positions rely on a clearly incorrect interpretation of *Watson*, which in fact requires notification of the use of investigatory powers irrespective of whether access to the data was unlawful or involved a serious error.

The Investigatory Powers Tribunal

The Investigatory Powers Tribunal (IPT) may only confirm a person has been subjected to investigatory powers if it deems the exercise of such powers was unlawful. However, the ability of the IPT to provide effective remedy is more limited still. In the frankly Kafkaesque system, individuals must first apply to the IPT to seek remedy – despite the fact that they will have absolutely no idea that they have been subjected to intrusive investigatory powers that are designed and used with the express purpose of being undetectable. In addition, the IPT recently added a further obstacle for applicants – individuals must now demonstrate that, "*due to their personal situation*", they risk having been subjected to investigatory powers. In *Human Rights Watch & Others*, the IPT found that only six claimants out of over 600 applicants could adequately demonstrate that they were at risk of being subjected to investigatory powers.[38]

---

[35] Court of Justice of the European Union, Judgement of 8.4.2014 – Joined Cases C-293/12 *Digital Rights Ireland Ltd.* and C-594/12 *Kärntner Landesregierung and Others* (ECLI:EU:C:2014:238): para. 37

[36] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.20

[37] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.21

[38] [2016] UKIPTrib 15_165-CH available at - http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

This condition of application is plainly obstructive and wrong. It is an absolute obstruction to justice for those subjected to investigatory powers for unforeseeable reasons - for example, those whose data is sought purely due to their location at a particular time, or as a result of mistaken identity. In any event, it is unfathomable that any individual should be expected to guess that they have been subjected to entirely undetectable powers in order to seek legal remedy.

Error Reporting

The provision in the IPA enabling the Investigatory Powers Commissioner (IPC) to inform victims of a 'serious error' as defined under the Act does not in any way mitigate the clear requirement in *Watson* for all those affected by investigatory powers, regardless of the lawfulness or erroneousness of their use, to be notified after the fact when it is safe to do so.

In fact, 'serious error' reporting under the IPA is an overly-restricted function of the IPC and, in our view, obstructs rather than enables individuals' right to redress. The Act defines a 'serious error' as one that causes *"significant prejudice or harm to the person concerned"*[39]. It is only where significant harm is deemed to have been demonstrated that the IPC is permitted to inform a person of the serious error by which they have been affected.[40] Astoundingly, the Act specifically exempts a breach of a person's rights under the Human Rights Act 1998 as qualifying in and of itself a 'serious error'. [41] The threshold for what legally constitutes "*significant prejudice or harm"* in this context therefore appears to be impossibly high – in fact, the terms are left undefined in the Act – but in any event, it is not an appropriate condition to have in order for individuals to access their legal rights.[42]

Far from promoting individuals' right to redress, the restrictive error reporting function in the IPA actually forces the IPC to be complicit in obstructing that right as they cannot inform an individual that their rights have been breached except in tightly delineated circumstances. This arguably compromises the constitutional function of the IPC and is in itself a significant issue that only increases the imperative on Government to provide for post-notification in the manner required by the CJEU's judgment.

It must also be considered that the CJEU was aware of both the function of the IPT and the IPA (passed in November 2016) when it made clear the requirement of notification to all persons affected by investigatory powers in its December 2016 judgment.

[39] Investigatory Powers Act 2016, s.231(2)
[40] Investigatory Powers Act 2016, s.231(7)
[41] Investigatory Powers Act 2016, s.231(3)
[42] S.7(1) of the Human Rights Act 1998 makes no such condition on the ability of individuals to exercise their right to remedy.

Would it be practical to provide for post-notification?

In its consultation paper, the Government sets out its position 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".*[43] The Government further argues that notification would be "*practically impossible"* where one person is of interest to different public authorities.

However, the CJEU's judgment states clearly that notification should be given when it is "*no longer liable to jeopardise the investigations being undertaken"* – therefore, operational concerns should be fully taken into account before each disclosure is made. We believe that compliance with the legal requirement for notification should not be "*impossible*" and more work should be done to find practical solutions. In any event, the presumption should be in favour of notifying affected individuals where possible rather than the current blanket rejection of the notification procedure required by law.

We would draw the Government's attention to relevant case law from the European Court of Human Rights on the necessity of notification for a rights-compliant communications data framework – in particular, *Klass v Germany* in 1978, *Weber and Saravia v Germany*[44] in 2006, *Zakharov v Russia* in 2015, and *Szabo and Vissy v Hungary*[45] in 2016. The requirement for notification could not be clearer – it is vital that the Government observes this important element of the CJEU's judgment.

Policy recommendation

- **Public authorities that access retained data must notify the persons affected as soon as notification is no longer liable to jeopardise the investigations being undertaken by those authorities.**

[43] Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.20

[44] *Weber and Saravia v Germany*, 2006, application 54934/2000, para. 135: *"**The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards** against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned **unless the latter is advised of the measures taken without his or her knowledge** and thus able to challenge their legality retrospectively"*

[45] *Szabo and Vissy v Hungary, para. 86: "As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, **information should be provided to the persons concerned**…In Hungarian law, however, no notification, of any kind, of the measures is foreseen. This fact, coupled with the absence of any formal remedies in case of abuse, indicates **the legislation falls short of securing adequate safeguards**."*

POLICY RECOMMENDATIONS

1. *Watson* applies to the communications data retention and acquisition regime as a whole. Amendments must apply to the communications data regime as a whole, including both 'entity' and 'events' data in the IPA.

2. *Watson* applies to the communications data retention and acquisition regime as a whole. Furthermore, the judgment is clear that national security as an objective of general interest does not negate the necessity of mandatory safeguards. Amendments to the communications data regime must be applied to all competent public authorities, including the UK's three intelligence agencies.

3. The UK's communications data regime must require there to be a relationship between the data ordered for retention and the specific threat to national security or serious crime investigation.

4. Where communications data, either 'entity' or 'events' data, is retained or accessed for the prevention and detection of crime, it must only be sought in relation to serious crime as defined in s.263 of the IPA, or in relation to offences under the Protection from Harassment Act 1997.

5. In relation to serious crime, only the data of individuals suspected of involvement in a serious crime may be sought.

6. In relation to national security, data may only be sought where there is objective evidence that it will make an effective contribution to a specific threat.

7. Judicial authorisation should be sought by all public authorities for access to communications data. Access safeguards for local authorities must not be weakened.

8. The independent authorising body should be notified of any urgent requests granting access to communications data to enable post-facto review.

9. Public authorities that access retained data must notify the persons affected as soon as notification is no longer liable to jeopardise the investigations being undertaken by those authorities.

Silkie Carlo