eComms confirmation

The document:

181211 10 HR Orgs v the UK - GC referral.pdf

Was sent on:

11/12/2018 12:08 (Strasbourg local time)

by: megang@libertyhumanrights.org.uk

IN THE EUROPEAN COURT OF HUMAN RIGHTS **Application No. 24960/15**

B E T W E E N:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-

THE UNITED KINGDOM

Respondent

REQUEST FOR REFERRAL TO THE GRAND CHAMBER

Summary

1. In accordance with Article 43 of the Convention and Rule 73(1), the Applicants[1] request that the judgment of the First Section in *Big Brother Watch and others v the United Kingdom*[2] be referred to the Grand Chamber. This request is drafted in accordance with the Court's *General Practice Followed by the Panel of the Grand Chamber When Deciding on Requests for Referral* of October 2011.

2. The case is appropriate for referral to the Grand Chamber, to enable the Court to authoritatively state the law governing mass surveillance in light of modern technological developments:

    a) Modern mass surveillance raises serious questions affecting the interpretation or application of the Convention and serious issues of general importance. This is an appropriate case for the Grand Chamber to consider authoritatively what, if any, development is required in the Convention jurisprudence. There are wide legal, social and political implications. Further, the UK has adopted a role as a pioneer of widespread mass surveillance, including the bulk interception of

[1] Amnesty International Limited, the National Council for Civil Liberties (Liberty), Privacy International, the American Civil Liberties Union, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties and the Legal Resources Centre.

[2] This is the joined case of this case (*10 Human Rights Organisations v the United Kingdom* (Application No. 24960/15)), *Big Brother Watch and others v the United Kingdom* (Application No. 58170/13), and *Bureau of*

internet communications. Through the "Five Eyes" group,[3] the UK has also played a role in pioneering the large-scale sharing of intelligence with foreign governments, including information gathered through mass surveillance. The scale of UK mass surveillance, through both bulk interception and intelligence sharing, means that this case is therefore an appropriate one in which to provide guidance.

b) The judgment of the First Section was deeply divided. Of the seven members of the Court, only three judges subscribed to the reasoning of the judgment in its entirety. Two members of the Court (Judge Koskelo and Judge Turković) considered that *ex ante* judicial control of mass surveillance was now required, and that the UK regime for the sharing of intelligence was also in breach of Article 8. Significantly, these two members called for the Grand Chamber to reconsider the Court's jurisprudence. In contrast, two other members of the Court (Judge Pardalos and Judge Eicke) dissented even on whether the breaches of Article 8 identified by the majority were established.

c) There is also a division between the views of the First, Third and Fourth Sections on whether the safeguards identified by the Court in *Weber & Saravia v Germany* (Application No. 54934/00) for mass surveillance operations remain appropriate in the modern world. In *Szabó & Vissy v Hungary* (Application No. 37138/14), the Fourth Section unanimously held:

> "70. The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile… of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. Reference is made in this context to the views expressed by the Court of Justice of the European Union and the European Parliament (see paragraphs 23 and 25 above). This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices. However, it is not warranted to embark on this

Investigative Journalism and Alice Ross v the United Kingdom (Application No. 62322/14).

[3] The "Five Eyes" comprise the signals intelligence agencies of the United States of America, Canada, the United Kingdom, Australia and New Zealand. They pool their intelligence and resources and therefore are able to conduct mass surveillance with an unparalleled global reach.

matter in the present case, since the Hungarian system of safeguards appears to fall short even of the previously existing principles."

In contrast, in *Centrum för rättvisa v Sweden* (Application No. 35252/08) the Third Section simply applied *Weber & Saravia* without considering whether any updated safeguards were required. It is noted that the Grand Chamber Panel has adjourned its consideration of a request for referral in *Centrum för rättvisa*. In the present case, the First Section was divided as to whether additional safeguards were needed. This case is an appropriate one for the Grand Chamber to address the compatibility of novel mass surveillance practices with the Convention.

d) Whether (and if so, how) to develop the case law of the Court on mass surveillance, including in light of a range of differing views expressed in recent Chamber judgments, is a proper matter for the Grand Chamber. Many Contracting States are operating or developing mass surveillance operations. There is great public interest and concern in those schemes. The authoritative analysis of the Grand Chamber is required to develop its case law appropriately, as well as to resolve the differences in approach between different Chambers to ensure consistency in the Court's case law and the proper protection of privacy and freedom of expression across the Contracting States. It is in the interests of all people and Contracting States that the Grand Chamber authoritatively address the compatibility of mass surveillance with the Convention and, if applicable, what minimum safeguards would be required.

The developing case law of the Court

3. The Court has long recognised the intrusiveness inherent in government interception of communications. It has repeatedly developed its jurisprudence to reflect technological change. In *Klass v Germany* (1979-1980) 2 EHRR 214 (decided in September 1978, over 40 years ago at a time when mobile telephones did not exist), the Court held that "*telephone conversations*" are "*covered by the notions of 'private life' and 'correspondence'*" (§41).

4. Since *Klass*, the advent of the internet and advancements in modern technologies have revolutionised the way we communicate. The Court has acknowledged these developments, expanding the scope of Article 8 protection to include "*e-mail*

communications" in *Weber & Saravia* (§77) and proposing a series of minimum safeguards that were designed to address a scheme of interception of a small proportion of international telephone calls in and out of Germany carried by satellite transmission.

5. The safeguards in *Weber & Saravia* reflect interception practices of a different technological age. The world has moved on. When the Court decided *Weber & Saravia* in 2006, smartphones were brand new (the iPhone was launched in 2007); Facebook was a website used mainly by university students; and Twitter had just been invented. The understanding of the intrusive power of the mass storage and analysis of large quantities of private data was in its infancy. Technological developments since then mean that governments can now create detailed and intrusive profiles of intimate aspects of private lives by analysing patterns of communications on a bulk basis.

6. Modern technology raises important questions of principle, suitable for consideration by the Grand Chamber. Contracting States face serious risks from organised criminality, including terrorism. It is important that the competent authorities have the right tools to be able to address those risks to democracy and freedom. Combatting these threats requires concerted police and intelligence activity, including the use of covert surveillance and interception of communications. However, these operations must be conducted within the framework of the Convention. Excessive or unaccountable state surveillance puts at risk the very core values protected by the Convention that terrorism seeks to undermine. The Court has therefore sought to develop principled safeguards designed to ensure an effective protection of Convention rights. However, significant changes in society and technology mean that those safeguards now require reconsideration and updating.

7. People living in Council of Europe States and beyond now live major parts of their lives online. Our use of communications technology has developed greatly in the last decade. We now use the internet to impart ideas, conduct research, expose human rights abuses, explore our sexuality, seek medical advice and treatment, correspond with lawyers, communicate with friends, colleagues and loved ones and express our political and personal views. We conduct many of our daily activities, such as keeping records, arranging travel and conducting financial transactions online. Much of this activity is

conducted on mobile digital devices, which are seamlessly integrated into our personal and professional lives. They have replaced and consolidated our fixed-line telephones, filing cabinets, wallets, private diaries, photo albums and address books.

8. The internet and modern communication devices have also enabled the creation of far greater quantities of personal data about our communications, known as communications data. Communications data is information about communications and patterns of communication, which may include the sender and recipient, the date and location from where a communication was sent and at which it was received, the duration and frequency of communication, patterns of communication between associates and the type of device used to send or receive the information and devices linked to it. Communications data reveals enormous amounts of often sensitive information about the life of individuals.

9. As modern communications have evolved, governments have developed more advanced ways to access, acquire, store and analyse this information. They have adopted methods for acquiring communications and data transiting the internet. The costs of storing this information have decreased drastically and continue to do so. At the same time, technology now permits revelatory analyses of types and amounts of data that were previously considered meaningless or incoherent. Communications data, in particular, is structured in such a way that computers can search through it for patterns faster and more effectively than similar searches through the content of communications.

10. The expanded scope and scale of intelligence gathering has led to a concomitant expansion in the scope and scale of sharing of intelligence between governments. The internet has also transformed the nature of intelligence sharing by facilitating remote access to information. Communications and data no longer need to be physically transferred from sender to recipient but can be directly accessed by foreign partners.

The present claim

11. The issues in this case first came to light as a result of the disclosures of classified information made in 2013 by Edward Snowden, who formerly worked for the CIA and

as a contractor for the United States National Security Agency. Mr Snowden revealed for the first time:

a) the enormous scale of modern mass collection of communications, and the fact that GCHQ do not simply collect the communications in bulk, scan them, and keep the data of the persons in whom they have an interest. GCHQ retain and store very large volumes of data, relating to hundreds of millions of people, even where the individuals are of no intelligence interest;

b) that GCHQ keep *all* the communications data: in other words, the data associated with a communication which reveals a person's location, the identity of the persons or websites they have contacted, and the occasions when contact has been made. Such data enables intrusion into the most intimate aspects of a person's private life; and

c) that GCHQ, in partnership with the signals intelligence agencies of the other Five Eyes governments, benefits from large-scale sharing of the information collected through mass surveillance.

12. The majority of the First Section in *Big Brother Watch and others v the United Kingdom* identified breaches of Articles 8 and 10, as a result of the inadequate safeguards applied to mass interceptions of data. However, the judgment of the Court was divided on crucial issues, including whether the minimum safeguards identified in *Weber & Saravia* require updating.

13. The Court also ruled for the first time on the "*Convention compliance of an intelligence sharing regime*" (§416). However, the judgment was also divided on whether the UK regime for the receipt of shared intelligence was also in breach of the Convention.

Proposed issues for consideration by the Grand Chamber

14. In *Weber & Saravia* the Court considered the lawfulness of general surveillance of a proportion of international satellite communications (which were around 10% of the total volume of communications) (§30). Communications by fixed telephone lines were not included. The purposes of surveillance were strictly limited.

15. In *Liberty v United Kingdom* (Application No. 58243/00) the Court considered a system of interception of a single microwave telecommunications link carrying Irish telecommunications traffic, solely for the purposes of preventing or detecting acts of terrorism (§5 and §24).

16. The present case concerns far wider surveillance. The scheme considered in the Application may cover large numbers of high capacity fibre-optic links, with interception occurring for broad purposes, including the general protection of national security, serious crime or the economic well-being of the United Kingdom. The Application further considered the large-scale sharing of intelligence between the United States and the United Kingdom.

Is mass surveillance compatible with the Convention?

17. The first issue suitable for the Grand Chamber is whether such blanket surveillance is in principle acceptable under the Convention. The First Section held that mass surveillance was acceptable in principle, given the margin of appreciation. However, such a blanket approach falls foul of principles established by the Grand Chamber in *S and Marper v UK* (Application Nos. 30562/04 & 30566/04) and by the First Section in *MK v France* (Application No. 19522/09), in relation to the mass retention of DNA or fingerprints, even from those not charged, or who had been acquitted. The fact that it is now *possible* for the state to retain private information about the population of a whole nation (or even many nations), which it was not in the past, and that retaining such information may be operationally useful, does not justify the intrusion of doing so. Just because the state *can* do something, doesn't mean that it *should*.

18. For example, no doubt it would be possible to take DNA from every person in the UK and store it. It could then be searched to identify the perpetrators of crimes where DNA evidence had been found. And no doubt this would assist the police in identifying hitherto unsuspected criminals. But that is not a good enough reason to justify so wide an intrusion into everyone's Article 8 rights.

19. In *S & Marper* the United Kingdom submitted that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "*inestimable*

value" and produced "*enormous*" benefits in the fight against crime and terrorism (§92). The Grand Chamber nonetheless held that the retention was a "*disproportionate interference*" with those individuals' private lives (§135). Similarly, in *MK,* the Court rejected the justification given for the French national fingerprint database by the first instance court, that "*retaining the fingerprints was in the interests of the investigating authorities, as it provided them with a database comprising as full a set of references as possible*." (§13) Rather, it warned that the logic of the French government's arguments "*would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*" (§37).

20. The UK seeks to argue that mass intercept is a practical necessity. That is incorrect. Even if it were technically unavoidable to intercept a whole cable in order to obtain the data of a particular target, the excess data should then be immediately and automatically discarded. Vast amounts of data belonging to individuals of no intelligence interest are not only being collected: such data is being kept automatically for substantial periods of time, and subsequently analysed and examined. The authoritative judgment of the Grand Chamber is sought as to whether bulk interception is compatible with the Convention.

Should the Weber safeguards be updated?

21. The second issue suitable for the Grand Chamber is what safeguards are required if mass surveillance is in principle permissible. The minimum requirements in *Weber & Saravia* as applied in *Liberty v UK* now require updating in light of developments in communications technology.

22. The UK legislation attempted to provide a safeguard by its requirement that a bulk interception warrant be primarily targeted at "*external*" not "*internal*" communications. However, as a result of technological changes in the way data is transmitted, the distinction drawn in national law between the legal regimes governing "*external*" and "*internal*" communications has become meaningless in practice. This is for two reasons. First, where a person in the UK communicates with a webpage, or email portal, which is hosted abroad, this will be classified as an "*external*" communication. Second, it is now routine for "*internal*" communications, such as an email between persons in the UK who

might be in the same office building, to be routed through servers on the other side of the world in the course of delivery. It is not possible to distinguish between "*internal*" and "*external*" communications at the point of interception. So the former has effectively become subject to the bulk interception powers as an *"incidental"* product of mass interception of *"external"* communications.

23. This means that the world has also changed dramatically from the position considered by this Court in *Weber & Saravia* and *Liberty*. For example, *Liberty* primarily concerned the bulk surveillance of communications between the UK and the Republic of Ireland, and solely for counter-terrorism purposes. It was unlikely that many "*internal*" communications would be collected. Telephone calls between two Londoners would be unlikely to be routed via Dublin. But Facebook messages between two Londoners will be routed via California and are likely to be caught by mass interception and subjected to automated profiling and analysis. The notional legal safeguards for "*internal*" communications have failed to keep up with the development of technology. This is incompatible with the quality of law requirement inherent in Article 8.

24. The combination of changes to the technological means of transmission of data, the vastly expanded capacities to intercept data and to draw up a picture of a person's private life and the exponential growth in use of electronic media to conduct private life mean that State intrusion into private life and correspondence has greatly increased. The limited safeguards in *Weber & Saravia* have not proven effective to prevent or control this development. Additional safeguards are required, including:

    a) A requirement for objective evidence of reasonable suspicion of a serious crime or conduct amounting to a specific threat to national security in relation to the persons for whom the data is being sought.

    b) *Ex ante* independent judicial authorisation for the issue of any warrant permitting interception and collection of the content of communications and associated communications data, since nothing could replace the critical role of the judge in deciding on the legality, strict necessity and proportionality of warrant requests.

c) Judicial approval to prevent the misuse of collected data. Approval should be required of searches and analysis, to ensure that the use of data is justified by objective evidence.

d) Wherever possible, a requirement for the notification of affected persons, so that they have a meaningful opportunity to challenge the lawfulness of the action taken against them. In the absence of such notification, any right of access to the courts is meaningless. Other jurisdictions have been able to make provision for notification after the event, apparently without jeopardising their intelligence operations: they include Germany, Austria, the Czech Republic, Denmark, Belgium and Switzerland. This Court was right in its judgment in the case of *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* (Application No. 62540/00) to note that the lack of provision for such notification under Bulgarian law was a missing "*important safeguard*" against improper use (§91).

What safeguards should apply to intelligence sharing arrangements?

25. The same safeguards applying to direct surveillance must also apply to a decision to receive data a foreign intelligence agency has intercepted or collected, no matter whether the sharing of such data is solicited or unsolicited. There is no difference in terms of intrusion into privacy if data is intercepted by GCHQ in the UK, or if the same data is intercepted in the USA (often at the other end of the same cable) and then passed to GCHQ. As previously mentioned, the safeguards applicable to such intelligence sharing arrangements were addressed by the Court for the first time in the present case, albeit to a limited extent since the First Section wrongly decided not to discuss the issue of *unsolicited* information sharing. The solicited and unsolicited sharing of intercepted communications is a novel issue of interpretation of the Convention rights and of such fundamental importance, including in light of the extent of information thus being shared, that it requires a comprehensive assessment by the Grand Chamber.

26. While the judgment of the First Section determined that the safeguards applying to "*the acquisition of surveillance material*" must apply equally to "*the regime for the obtaining of such material from foreign Governments*", its application of this principle was internally

inconsistent (§422). The Court determined that the UK regime for the sharing of intelligence was lawful. However, the finding that aspects of the UK's bulk interception regime breach Article 8 of the Convention must logically extend to the intelligence sharing regime. For example, the Court determined that "*those requirements which relate to… storage, examination, use, onward dissemination, erasure and destruction*" in the direct surveillance context must also "*be present*" in the intelligence sharing regime (§423). But it did not extend its finding that the way the UK filters and searches bulk intercept material breaches the Convention to intelligence sharing, despite the fact that the UK may similarly filter and search bulk intercept material shared by a foreign government. Two members of the Court (Judge Koskelo and Judge Turković) did consider that the UK regime for the sharing of intelligence was also in breach of Article 8.

Conclusion

27. Worldwide, the most senior Courts are in the process of applying fundamental rights principles to new surveillance technologies. In *Riley v California* 134 S.Ct. 2473 (2014); 573 US (2014), Chief Justice Roberts of the United States Supreme Court noted that "[t]*he term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers*." The consequence is that there is a "*digital record of nearly every aspect of their lives*". This is "*qualitatively different*" from the recent past. Modern communications reveal:

> "an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building ... a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." (pp.19-20)

28. In a series of cases heard by the Grand Chamber of the Court of Justice of the European Union, that Court has identified and applied necessary safeguards for the use of bulk data, including prior judicial or independent authorisation and notice to persons whose

data has been collected. See Case C-292/12 *Digital Rights Ireland v Minister for Communications* [2015] QB 127 and Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* and *Watson* [2017] QB 771.

29. In the UK Supreme Court, Lord Sumption identified the same technological developments and emphasised the importance of the role of the Court in the proper protection of privacy. See *R. (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] A.C. 1065, p.1077F-G at [2]:

> "Historically, one of the main limitations on the power of the state was its lack of information and its difficulty in accessing efficiently even the information it had. The rapid expansion over the past century of man's technical capacity for recording, preserving and collating information has transformed many aspects of our lives. One of its more significant consequences has been to shift the balance between individual autonomy and public power decisively in favour of the latter."

30. Nevertheless, the legal response in the UK (and many other Contracting States) has been limited and hesitant. As Lord Sumption put it "*the concept of a legal right of privacy whether broadly or narrowly defined fell on stony ground in England. Its reception here has been relatively recent and almost entirely due to the incorporation into domestic law of the European Convention on Human Rights*" (p.1077H, ibid). The proper protection of privacy in the UK has been almost entirely due to the role of this Court.

31. While a reference to the Grand Chamber is exceptional, for all the reasons summarised above, the present case raises issues of general importance and serious questions affecting the interpretation or application of the Convention. The development of technology and the inadequacy of existing privacy safeguards mean that this case is an appropriate one for the Grand Chamber to authoritatively address a range of fundamental questions on mass surveillance, intelligence sharing, and minimum safeguards required. Whether (and if so, how) to develop the case law of the Court on mass surveillance, including in light of a range of differing views expressed in recent Chamber judgments, is a proper matter for the Grand Chamber.

BEN JAFFEY QC
BLACKSTONE CHAMBERS

11 December 2018