NEW SQUARE

LEGAL Update

NEWS AND VIEWS
FROM 4 NEW SQUARE CHAMBERS

OCTOBER 2018

Big Brother Watch and ors v. The United Kingdom

IAN MCDONALD

Ian McDonald joined 4 New Square in October 2018 following the successful completion of his pupillage, and is developing a broad practice across Chambers' core areas. He is a graduate of Birkbeck, University of London (LLB; First Class Honours), and Balliol College, Oxford (Bachelor of Civil Law; Distinction). Prior to coming to the Bar, Ian originally trained and worked as a journalist before spending five years at Liberty, the human rights organisation, in various media and campaigns roles.

JOHN WILLIAMS

John Williams is a barrister at 4 New Square. He was called to the bar in 2017, and is developing a broad practice across chambers' core areas of work. Prior to joining chambers, John worked at the Law Commission, after graduating with a first class degree in Law from UCL, and a distinction in the Bachelor of Civil Law at Oxford University, where he specialised in private law theory, and legal and political philosophy.

In *Big Brother Watch and Others v the UK*, **Can Yeğinsu** and **Anthony Jones** of 4 New Square acted for the Center for Democracy & Technology and PEN American Center. Led by Hugh Southey QC, they argued that deficiencies in US interception programmes tainted the UK's own regime, given intelligence sharing between the two states. 4 New Square enjoys a leading reputation at the public law and human rights Bar and has a fast growing presence in the public International law field, with members regularly instructed by governments, corporate bodies, NGOs and individuals in the UK and across the world.

Introduction

The European Court of Human Rights' recent decision in *Big Brother Watch and Others v the UK* ("***Big Brother Watch***") – in which it was held that certain aspects of the UK's mass surveillance programmes, as unearthed by Edward Snowden, are a violation of various Articles of the European Convention on Human Rights – has unsurprisingly been lauded by campaigners as a clear statement that the UK Government is continuing to breach privacy rights (Open Rights Group) and "a significant and important enhancement of privacy protections" (Privacy International).

However, this landmark judgment is another signal, also, of the seriousness with which the Strasbourg Court in particular regards the impact of surveillance not only on the right to privacy, as protected by Article 8 of the Convention, but on the right to freedom of expression, as safeguarded by Article 10; and, more specifically, the chilling effect that such practices can have on investigative journalism and whistle-blowing.

Indeed, given the categorical nature of the findings on Article 10, compared with the arguably more nuanced determinations in respect of Article 8, *Big Brother Watch* can be seen as the latest instalment in a series of rulings from the European Court of Human Rights suggesting that it is freedom of expression – as much as, or perhaps even more so than, personal privacy – which is a benchmark, so far as the Convention is concerned, of a healthy and vibrant civil society.

Facts and procedural history

In *Big Brother Watch*, the First Section of the European Court of Human Rights considered three joined cases, brought by 16 applicants. It also considered written submissions from a number of third party interveners, ranging from the Center for Democracy & Technology and PEN America – who submitted that deficiencies in interception programmes in the United States tainted the lawfulness of the UK's regime, given the sharing of intelligence between the two nations – to the National Union of Journalists and the Media Lawyers' Association ("**the MLA**").

The applications arose out the disclosures of classified information made by Edward Snowden in 2013. These documents detailed a bulk communications interception programme run by GCHQ – codenamed "TEMPORA" – and two NSA surveillance programmes – "PRISM" and "Upstream".

The TEMPORA programme involved the bulk interception of communications (including both content and "metadata"), which was acquired by tapping into sub-sea fibre optic cables carrying internet traffic (known as "bearers"). GCHQ collected the data passing through targeted bearers, and sifted it using prescribed selection methods to obtain data of interest.

GCHQ acquired further communications collected by the NSA from its PRISM and Upstream programmes. In the case of PRISM, this data was sourced from Internet Service Providers (ISPs), following prior judicial authorisation. From Upstream, the NSA collected content and communications data directly from cables and infrastructure owned by communications service providers (CSPs) operating within the US.

The applicants alleged that the UK's legal framework regulating the acquisition, use, sharing and destruction of intercepted communications violated a number of Convention rights. These complaints focussed primarily on three parts of the domestic legal regime, governing the acquisition of intercepted communications:

- Sections of the Regulation of Investigatory Powers Act 2000 ("**RIPA**") and related Codes of Practice, controlling the granting of warrants for the interception of communications, and the terms on which acquired data was retained and used;
- The statutory framework governing intelligence sharing between the US and UK governments; and,
- Chapter II of RIPA, which regulated the acquisition of "communications data" (rather than the "content" of communications) from CSPs.

The applicants argued that all three parts of the domestic regime breached Article 8 of the Convention, and that the terms of RIPA were in violation of Article 10. Further complaints were raised by some of the applicants in relation to alleged violations of Articles 6, 14, and 41 of the Convention.

Admissibility

The UK Government, as a preliminary matter, took issue with the applicants' rights to bring their complaints before the Court.

First, it was argued that in two of the three joined cases, because the applicants had not previously put their complaints before the Investigatory Powers Tribunal ("**the IPT**") – which was constituted specifically to hear complaints of unlawful conduct relating to the operation of RIPA – they had not "exhausted" domestic remedies, for the purposes of Article 35, and the Court should therefore decline to hear their cases.

The First Section accepted the UK Government's arguments that the IPT was "effective", in that it provided adequate redress to applicants. Although the IPT did not have the power to issue formal declarations of incompatibility under section 4 of the Human Rights Act 1998, its decisions had still provoked substantial changes in the RIPA framework.

However, the applicants were saved by their reliance on the Fourth Section's earlier decision in *Kennedy v the UK* (Application no. 26839/05), in which it was held that the IPT did not provide an effective remedy in relation to "general" complaints about the Convention compliance of interception regimes. Although that opinion had been given early in the life of the IPT, and was now unsound given the Court's view on the Tribunal's adequacy (above), it was legitimately used to justify the applicants' decision not to bring first instance proceedings in the IPT, and thus their complaints were admissible.

Further objections to admissibility related to the applicants' lack of "victim" status, as required by Article 34 of the Convention. In accordance with its prior jurisprudence relating to victimhood in the context of secret surveillance and interception, the Court adopted a broad and pragmatic approach, taking into account the nature of the applicants (human rights groups and individual journalists) and the wide scope of the interceptions programmes under RIPA. The Court held that the applicants were sufficiently likely to have been the targets of interception to count as "victims", and therefore had standing to bring their complaints.

The Court did, however, render inadmissible the complaints of applicants in the third case relating to alleged infringements of Article 10. Although those applicants had first brought proceedings before the IPT, they had failed to raise arguments under Article 10 at the hearing before the Tribunal and their complaint was therefore deemed inadmissible under Article 35. Further complaints under Articles 6 and 14 were also rendered inadmissible on the grounds that they were "manifestly ill-founded".

Complaints relating to Article 8

The applicants complained that three distinct surveillance regimes violated their Article 8 rights: (i) the regime under section 8(4) of RIPA for the bulk interception of communications, which was said *inter alia* to be so complex as to be inaccessible, and therefore lacking the requisite quality of law ("**the section 8(4) regime**"); (ii) the receipt of material from foreign intelligence services, particularly information intercepted by the NSA under PRISM and Upstream, for which it was said there was no basis in law (and certainly no regime satisfying the Court's "quality of law" requirements) ("**the intelligence sharing regime**"); and the regime for the acquisition of communications data under Chapter II of RIPA, which was said to permit the obtaining of such data in a wide range of ill-defined circumstances and without proper safeguards ("**the Chapter II Regime**").

The section 8(4) regime

Section 8 of RIPA (in tandem with other provisions) regulates the granting of warrants for the interception of communications and related data. Section 8(4) specifically provides for the "bulk" or "untargeted" interception of communications, subject to the terms of the Act.

RIPA contains a number of safeguards relating to how bulk interception is carried out: a certificate from the Secretary of State is required, only "external" communications can be targeted, the copying and disclosure of intercepted communications is limited to the minimum necessary for the purposes authorised, and the selection of data for review cannot depend on factors referable to individuals within the British Islands (for which a targeted warrant must be obtained).

Section 72(1) of the Act also requires any person exercising powers under the Act to have regard to relevant Codes of Practice, which aim to ensure Convention compliance.
The Court found that there was a clear interference with the applicants' Article 8 rights. It went on to consider whether this interference was justified, taking into account (i) whether it was in accordance with the law; (ii) whether it pursued one or more legitimate aims set out in Article 8; and, (iii) whether the interference was necessary to achieve that aim.

Key to the Court's assessment were the six criteria set out in *Weber and Saravia v Germany* (Application no. 54934/00) ("***Weber***"), which detailed a series of "minimum requirements" that should be met by the relevant law to guard against abuses of power. These factors were: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed.

The Court rejected an argument by the applicants that it should "update" those requirements by including further criteria of reasonable suspicion, prior independent judicial authorisation of interception warrants, and the subsequent notification of surveillance subjects.
By a majority, however, the First Section found that the section 8(4) regime was a violation of Article 8. It failed to meet the "quality of law" requirement, and was therefore "incapable of keeping the 'interference' to what is 'necessary in a democratic society'.

The Court reached this conclusion based on two areas of concern. First, it noted that the process by which bearers were selected for targeting, and intercepted communications were filtered and selected for examination by analysts, was insufficiently robust. Coupled with the fact that warrants were commonly phrased in open terms, and given the lack of "ex-ante" independent oversight, there was scope for abuse. Second, the section 8(4) regime maintained an unwarranted distinction between the "content" of communications, and "related communications data" ('where', 'when', 'how' etc). By exempting the latter type of data from the safeguards applicable to content, RIPA failed to strike a fair balance between the competing public and private interests at stake.

In reaching this view, the Court acknowledged that "the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security". Although features such as prior judicial authorisation may be "best practice", they were "neither necessary nor sufficient" to ensure Article 8 compliance. A pragmatic and contextual approach was more appropriate than a prescriptive one.

Applying this approach, the applicants' proposed additions to the *Weber* criteria were not accepted. Future applicants will, in all likelihood, face similar difficulties in convincing the Court to adopt more restrictive constraints. However, and as demonstrated by the majority's finding of breach, it should also not be assumed that the existing criteria lack teeth. If the battle-tested framework in RIPA is susceptible to challenge, it is likely that less refined surveillance programmes will also be vulnerable.

In addition, the Court took a firm stance on the distinction between content and metadata. Human rights groups and academics have long warned that the collection of metadata (or other "communications data") is as grave a threat to privacy as the collection of content. By contrast, the intuitive logic – reflected in the UK government's submissions to the court – has been that by its very nature, the collection of metadata is "less intrusive than the covert acquisition of content". The Court strongly rebutted this position – stating that when metadata is collected in bulk, the degree of intrusion into an individual's private life may even be magnified, and exceed that which results from the collection of content.

Following this analysis, the Court will likely view with suspicion any "two-tier" system, which differentiates between the safeguards applicable to the content of communications, and their associated metadata. Given the usefulness of metadata to the military and security services, either in addition to or as a proxy for "content", this aspect of the Court's judgment may be of particular significance and concern to Convention states.

The intelligence sharing regime

After noting that this was the first time that it had been asked to consider the Convention compliance of such a regime, the First Section found, by contrast, that the regime as used by the UK Government for sharing intelligence with foreign administrations did not violate Article 8.

In particular, the Court was persuaded that the procedure for requesting either the interception or conveyance of intercept material from overseas intelligence agencies was now set out with sufficient clarity (and accessibility) in domestic law, in light of clarifications brought about via the amendment of the relevant Code of Practice, the Interception of Communication Code of Practice ("**the IC Code**"), following recent disclosure of the internal arrangements referred to in the Security Services Act 1994 and the Intelligence Services Act 1994.

Further, the First Section observed that the high threshold recommended by the Venice Commission – namely, that material transferred from foreign authorities should be searched only if all the requirements for a national search of material obtained by the UK security services were fulfilled – was met by the intelligence sharing regime. And the Court was satisfied, too, that there was no evidence of any significant shortcomings in the regime's application and operation, or any evidence (according to an Intelligence and Security Committee of Parliament investigation) to suggest that the intelligence services were abusing their powers.

The Chapter II regime

The rules governing the selection of "related communications data", for the purposes of the Chapter II regime, were deemed to be inadequate, however.

The Court observed that the Chapter II regime does have a clear basis, in both section 22 of RIPA and the Amended Acquisition and Disclosure of Communications Data Code of Practice ("**the ACD Code**"). It also stressed, though, that as the UK is (for now, at least) a Member State of the European Union, where there is a conflict between domestic and EU law, the latter prevails.

Accordingly, the UK Government has previously conceded, in proceedings brought by Liberty, the human rights group, that Part 4 of RIPA was incompatible with fundamental rights in the EU, because access to retained data was not limited to the purpose of combating "serious crime" and was not subject, either, to prior review by the courts or an independent administrative body.

It was therefore clear, the Court concluded, that any domestic law regime permitting the authorities to access data retained by CSPs must include these two safeguards. As the Chapter II regime permits access for the purpose of combating "crime" (rather than "serious crime") and is not, save for in certain specific circumstances, subject to such prior review, the Court found that it was not in accordance with domestic law within the meaning of Article 8.

Complaints relating to Article 10

The applicants in the second of the joined cases – the Bureau of Investigative Journalism ("**the BIJ**") and Alice Ross, a reporter with the BIJ – complained under Article 10 of the Convention about both the section 8(4) regime and the Chapter II regime, arguing that their right to freedom of expression – which is of vital importance to them, as a newsgathering organisation and journalist respectively – had been violated, thus undermining their roles as "public watchdogs".

In particular, the BIJ and Ms Ross contended that, as a free press is one of the cornerstones of any democratic society, and the protection of journalistic sources is indispensable for such press freedom, Article 10 should impose additional and more burdensome requirements where state surveillance measures run the risk of revealing those sources, or exposing confidential journalistic material more generally. Such a risk, they submitted, had to be justified by an "overriding public interest" (as per *Goodwin v the UK* (Application No. 28957/95) ("***Goodwin***")), and be subject to authorisation by the Courts or another independent adjudicative entity.

In relation to the section 8(4) regime, the applicants argued that the interception of material via bulk surveillance was not protected by sufficient safeguards. As to the Chapter II regime, they complained that the ACD Code failed to acknowledge (i) that communications data could be privileged; and (ii) that the acquiring of even a single piece of such data – given that it alone could reveal the identity of a journalist's source, or other journalistically sensitive material – was as intrusive as obtaining actual content.

The First Section found that the applicants' rights under Article 10 had indeed been violated by the bulk surveillance regimes under RIPA.

Setting the tone, the Court began this section of its judgment by stressing the paramount importance, from a democratic perspective, of freedom of expression, and the concomitant significance of the safeguards that are afforded to journalists in a surveillance context. Without proper protection, the Court warned, sources may be dissuaded from helping the press to inform the public about fundamental matters, thereby undermining the "vital public-watchdog role" that journalists occupy.

Reflecting upon its own jurisprudence, the Court noted that, resultantly, it has routinely subjected safeguards for freedom of expression to unique scrutiny, and accepted that, as per *Goodwin* (above), any interference cannot be compatible with Article 10 unless it is warranted by an "overriding requirement in the public interest". The Court further held that, where a journalist's communications are selected for examination, such interference could be justified only if accompanied by adequate safeguards – relating both to the circumstances in which those communications are selected and to the protection of confidentiality once they are so selected.

As to the section 8(4) regime, the Court observed that paragraphs 4.1 to 4.8 of the IC Code do state that special consideration should be given to the interception of communications involving confidential journalistic information. However, these provisions apply only to the decision to issue an interception warrant, and are therefore of little value in the context of such a bulk interception regime.

Further, the Court was especially troubled that there were no requirements, under the regime, either curtailing the intelligence agencies' ability to search for confidential journalistic material or requiring analysts to have any particular regard as to whether such material is (or may be) implicated.

Therefore – and notwithstanding the fact that protections are in place in respect of storing such confidential data, once identified – the Court concluded that – in light of the potential chilling effect that apparent interference with journalistic communications and sources might have on press freedom, and in the absence of satisfactory arrangements to circumscribe the intelligence services' powers to delve into such information – the section 8(4) regime was a violation of Article 10.

Turning to the Chapter II regime, the Court recognised, first, that said regime does afford heightened protection where data is sought in order to identify a journalist's source (see, for instance, paragraph 3.77 of the ACD Code, which provides that, where an application is intended to determine a source in this way, there must be an overriding requirement in the public interest, and such applications must be brought pursuant to the Police and Criminal Evidence Act 1984).

However, the Court reasoned that these safeguards apply only where the specified purpose of the application is to uncover the identity of a journalist's source. They are not engaged, therefore, in every case where a request is made for the communications data of a journalist, or where such collateral intrusion is likely. Nor, the Court remarked, are there any provisions to restrict this kind of access to the purpose of combating "serious crime". Consequently, the regime simply could not be "in accordance with law" for Article 10 purposes.

One of the third party interveners in the Article 10 application – the MLA – had expressed deep concern, in its submissions, that domestic law was departing from the previously strong presumption that journalistic sources are sacrosanct, and should be afforded special legal protection.

Whether that fear is well-founded, at a domestic level, is another question for another day. However, the MLA and others like it can take real heart from the Court's decision in *Big Brother Watch*, and rest easy in the knowledge that – at this supranational level, at least – the freedom of the press and the safeguarding of journalist's sources are treated with the utmost seriousness, and appear to be in safe judicial hands.

Indeed, the categorical and immediate nature of the Court's findings in respect of Article 10 – particularly when considered against the arguably more nuanced and protracted determinations in relation to Article 8, are striking. The Court's invocation of the potential chilling effect on press freedom, for example, is notable; as is the fact that the Court was unpersuaded, in its consideration of the Chapter II regime, by what some would regard as relatively robust safeguards (such as the requirement for judicial authorisation where identification of a journalist's source is intended).

On the other hand, though, perhaps the Court's conclusions on Article 10 are not altogether surprising. After all, the European Court of Human Rights – particularly in recent years – has held time and again that journalists, as well as whistle-blowers and human rights campaigners, are the guardians of any rights-protecting democracy, and that restrictions upon their freedom of expression will only dilute the very values that the Convention seeks to uphold.

This trend towards the viewing of Article 10, in particular, as a beacon of democracy is particularly evident in the Strasbourg Court's modern approach to so-called right of access to information cases.

There was a time – see, for example, *Gaskin v the UK* (Application no. 10454/83) and *Guerra v Italy* (Application no. 14967/89) – where the Court denied that such a right fell within Article 10 at all. In more recent authorities, however, the Court has stated that Article 10 can in fact confer such a right – particularly on those, like the press, who exercise the functions of a "public watchdog". In *Magyar Helsinki Bizottság v Hungary* (Application no. 18030/11), for example, the applicant NGO complained that the refusal of police to disclose information on how (and how often) public defenders were appointed was a breach of Article 10. The Strasbourg Court, by 15 votes to two, agreed. As the majority put it:

> *The manner in which public watchdogs carry out their activities may have a significant impact on the proper functioning of a democratic society. It is in the interest of a democratic society to enable the press to exercise its vital role of "public watchdog" in imparting information on matters of public concern… just as it is to enable NGOs scrutinising the State to do the same thing. Given that accurate information is a tool of their trade, it will often be necessary for persons and organisations exercising watchdog functions to gain access to information in order to perform their role of reporting on matters of public interest.*

It is submitted that, despite its broader scope, *Big Brother Watch* can therefore be seen as the latest episode in this emerging series of cases which suggests that it is freedom of expression – as much as, or perhaps even more so than, personal privacy – which is a benchmark, so far as the Convention is concerned, of a healthy and vibrant civil society.

Conclusion

None of which is to say, of course, that personal privacy has been relegated to the cheap seats. The most instant impact of Edward Snowden's revelations was to focus minds on the importance of maintaining a private space, free from government interference; and in *Big Brother Watch*, even in the face of strong national security considerations, the Court nonetheless adopted a robust and detailed approach to its Article 8 deliberations.

However, the case highlights a crucial synergy which exists between the rights and interests protected under Articles 8 and 10. As the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression has recognised, "privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other". The facts underlying *Big Brother Watch* are a striking example of this: but for the work of reporters at *The Guardian* and *The Washington Post*, Snowden's documents may never have seen the light of day.

In the years since those revelations, across Europe and around the world, a resurgence of authoritarian nationalism has focused its attention primarily on the free press – and its core ideals of truthfulness, transparency and open discourse. Article 10 is the battleground of the moment, and blows struck for freedom of speech are also struck for Article 8, and for all of those rights which sustain liberal and democratic political orders.
In an increasingly unstable yet technologically advanced world, it will be fascinating to see where the Courts, whether supranational or domestic, go next, and how they continue to deal with the urgent threats to the rights protected by both Articles 8 and 10 of the Convention.

Enquiries should be directed to:

Ian McDonald: i.mcdonald@4newsquare.com
John Williams: j.williams@4newsquare.com

CLERK:

Alex Dolby: a.dolby@4newsquare.com
DDI: + 44 207 822 2036