IN THE EUROPEAN COURT OF HUMAN RIGHTS **Application No. 43514/15**

BETWEEN:

JOHN OLDROYD CATT

Applicant

and

THE UNITED KINGDOM

Respondent

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL

---

1 Introduction and Summary

1.1 These written observations are served on behalf of the intervener, Privacy International, pursuant to leave granted by the President on 1st September 2016.

1.2 Privacy International was founded in 1990. It is a UK charity working on the right to privacy at an international level. It focuses, in particular, on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development, and the United Nations.

1.3 Privacy International's primary aims are to raise awareness about threats to privacy, to monitor and report on surveillance methods and tactics, to work at national and international levels to ensure strong privacy protection, and to seek ways to protect privacy through the use of technology. In accordance with those aims, Privacy International has intervened in this Court in cases such as *S and Marper v UK* (App. Nos 30562/04 and 30566/04), *Tretter and others v Austria* (App. no. 3599/10), and *Breyer v Germany* (App. no. 500001/12). It seeks in this intervention to assist the Court by explaining the wider context of this application and by emphasising the seriousness of the privacy interference that arises as a result.

2. The Context

2.1 The starting point in any analysis of whether the retention of the applicant's personal data in the "*Extremism Database*" is "*in accordance with the law*" and "*necessary in a democratic society*" (Article 8(2) of the Convention) is a consideration of the significance of the intrusion into the Article 8(1) rights of the applicant (and those of other so-called "*domestic extremists*").

2.2 The Supreme Court's analysis of this issue was coloured by a serious misstatement. In his majority judgment, Lord Sumption described the interference with the applicant's private life as "*minor*" (§26) because the information retained was:

> "*… in no sense intimate or sensitive information like, for example, DNA material or fingerprints. It is information about the overt activities in public places of individuals whose main object in attending the events in question was to draw public attention to their support for a cause. Although the collation of the information in the form in which it appears in police records is not publicly available, the primary facts recorded are and always have been in the public domain. No intrusive procedures have been used to discover and record them, another marked contrast with DNA material. The material records what was observed by uniformed police officers in public places.*"

2.3 This analysis is fundamentally flawed. The mere fact that information is obtained through so-called "*overt*" methods of intelligence-gathering does not mean that the resulting interference with an individual's private life is "*minor*". The "*Extremism Database*" at issue in this application is known to contain a wealth of highly personal information about individuals, including descriptions of their physical appearance, their date of birth, their political opinions, and their professional occupation. However, in order to fully understand the significance of the privacy infringement in this case, it is necessary to set the "*Extremism Database*" in the context of other known "*overt*" forms of intelligence-gathering that are used by public authorities in the UK.

3. Developing Technology

3.1 If Lord Sumption's analysis were left undisturbed by this Court, it would set a dangerous precedent to Council of Europe states, particularly as new forms of technology permit law enforcement agencies to record and monitor large amounts of increasingly intimate information about those involved in public protest. The following "*overt*" methods of intelligence-gathering exemplify this concern:

3.1.1 **Social media intelligence**[1] and **open source intelligence** refer to the collective tools and solutions that allow organisations to monitor social channels, conversations and internet use, respond to social signals and synthesise social data points into meaningful trends and analysis. Police forces make use of these forms of intelligence to gather and analyse social media and internet postings from so-called "*domestic extremists*". Entries on the "*Extremism Database*" included information obtained from social media postings, such as posts on *Twitter* by the Green Party peer, Baroness Jenny Jones.[2] Guidance produced by the Association of Chief Police Officers of England, Wales, and Northern Ireland on the policing of anti-fracking protest in 2011 suggests that, "*Social media is a vital part of any … intelligence picture.*"[3] A 2013 report suggested that a staff of 17 officers in the National Domestic Extremism Unit was scanning the public's tweets, YouTube videos, Facebook profiles, and other public online postings.[4] The UK independent reviewer of terrorism legislation has commented that, "*UK law enforcement and security and intelligence agencies of course use [open source intelligence], though the extent of that use is not publicly known. By way of example, following a review by the Her Majesty's Inspectorate of Constabulary of the August 2011 disorders in English cities, an 'all-sources hub' was created to help police to tackle disorder, which includes social media monitoring*".[5] The UK Chief Surveillance Commissioner added, "*Perhaps more than ever, public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices. I repeat my view that just because this material is out in the open, does not render it fair game*";[6]

[1] David Omand; Jamie Bartlett; and Carl Miller "*#Intelligence*" (Demos, 2012).
[2] Applicant's bundle, Tab G, pp.553 and 589.
[3] Association of Chief Police Officers, "*Policing Linked to Onshore Oil and Gas Operations"*, at §4.7.3; available at: https://netpol.org/wp-content/uploads/2015/08/Onshore-Oil-and-Gas-Operations-2015.pdf
[4] *Wired,* 26th June 2013: http://www.wired.co.uk/article/socmint
[5] David Anderson QC, *"A Question of Trust: Report of the Investigatory Powers Review"*, June 2015, at §4.29.
[6] Office of Surveillance Commissioners Annual Report for 2014-15, at §5.72.

3.1.2 **Facial recognition technology** has been trialled by UK police forces. A trial was conducted by Leicestershire Police at a music festival in 2015.[7] In August 2016, the Metropolitan Police Service used automated facial recognition technology to monitor and identify people at the Notting Hill Carnival.[8] This technology, which is classed by police forces as "*overt surveillance*", works by scanning the faces of those passing by overt cameras and then comparing the images against a database of images populated by the police force in question. At the Notting Hill Carnival, the database was populated with images of individuals who were forbidden from attending Carnival, as well as individuals who the police believed may attend Carnival to commit offences. The combination of image databases and facial recognition technology could be used to track people's movements by combining widespread CCTV and access to a huge searchable database of facial images. Such technology has attracted concern from the UK Commissioner for the Retention and Use of Biometric Material, Alastair R MacGregor QC[9] and from the Science and Technology Committee of the UK Parliament;[10]

3.1.3 **Body worn cameras** are increasingly used both by police and prison officers in the UK. First trialed by a UK police force in 2006 and 2007, the technology is now "*a key focus for investment across many forces and its use is now widespread within policing*".[11] By the end of 2016, the majority of front-line police officers across the country will have access to body worn cameras.[12] The Association of Chief Police Officers guidance on the policing of anti-fracking protest makes it clear that police will use live video sources, including video cameras worn by individual officers, when policing such protests.[13] The use of body worn

[7] *Daily Telegraph,* 17th July 2014: http://www.telegraph.co.uk/technology/news/10973185/Police-trial-facial-recognition-software-that-can-ID-suspects-in-seconds.html
[8] *Police Oracle*, 27th August 2016: https://www.policeoracle.com/news/police_it_and_technology/2016/Aug/26/met-trialling-facial-recognition-technology-at-notting-hill-carnival_92773.html/specialist; Metropolitan Police Service, 30th August 2016: http://news.met.police.uk/news/statement-from-police-commander-for-notting-hill-carnival-2016-182480
[9] Commissioner for the Retention and Use of Biometric Material, "*Annual Report 2015*", at section 7.
[10] House of Commons Science and Technology Committee: "*Current and future uses of biometric data and technologies*", Sixth Report of Session 2014-15, at §§53-59 and §§94-100.
[11] Hampshire Police: http://www.hampshire.police.uk/internet/advice-and-information/general/body-worn-video
[12] *The Independent,* 1st March 2016: http://www.independent.co.uk/news/uk/crime/how-the-polices-body-worn-camera-technology-is-changing-the-justice-system-a6905691.html
[13] Association of Chief Police Officers, "*Policing Linked to Onshore Oil and Gas Operations*", at §4.7.7.

cameras in the gathering of information relating to protests by police forces has provoked privacy concerns from civil society organisations;[14]

3.1.4 **CCTV and automated number plate recognition technology** ("ANPR") are also used by public authorities to carry out "*overt*" monitoring. ANPR systems are designed capture an image of the vehicle's number plate as a vehicle passes an ANPR camera within the system and then to read that number using optical character recognition technology. When operated by law enforcement agencies, a record of that vehicle registration mark as identified by the system is then stored.[15] The use of CCTV and ANPR is regarded as "*surveillance by consent*" and the police consider that its use "*does not generally result in the obtaining of private information*."[16]

3.2 As they are classed as "*overt*" forms of intelligence-gathering, the recording of information from these forms of technology in large-scale databases is subject to broadly similar legal safeguards as those identified by the Supreme Court in the applicant's case, namely the Data Protection Act 1998, a generalised code of practice and Article 8. As in the applicant's case, safeguards designed specifically to govern the use of "*overtly*" collected intelligence are often lacking. By way of example:

3.2.1 As regards social media intelligence, the Association of Chief Police Officers 2013 guidance on "*Online Research and Investigation*" provided, at p.8: "*Recording, storing and using open source information in order to build up a profile of a person or a group of people must be both necessary and proportionate and to ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, it must be retained and processed in accordance with the principles of the Data Protection Act 1998.*" No more detailed guidance on its use is provided;

3.2.2 There is "*no specific legislation covering*" the use of facial recognition technology (with associated image databases) according to the Information

[14] Network for Police Monitoring, "*Police chiefs reject body-worn video camera privacy concerns*", 22nd August 2016: https://netpol.org/2016/08/22/privacy-body-worn-video/
[15] Home Office: "*The Use of ANPR by Law Enforcement Agencies*", at §1.1.
[16] [ibid], at §§2.1 and 2.5.

Commissioner's Office. The Biometrics Commissioner has questioned how "*appropriate*" it was for the police to put *"a searchable database of custody photographs*" into "*operational use*" in the absence of any "*proper and effective regulatory regime […] beyond that provided for in the Data Protection Act 1998*";[17]

3.2.3 Draft national guidance suggests that, "*The use of overt CCTV cameras by public authorities does not normally require an authorisation under the [Regulation of Investigatory Powers Act 2000]. Members of the public will be aware that such systems are in use, and their operation is covered by the Data Protection Act 1998 and the CCTV Code of Practice 2008, issued by the Information Commissioner's Office. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under the 2000 Act.*"[18]

3.3 It follows that the Court's decision in the applicant's case is also likely to be of assistance in providing guidance in the use by law enforcement agencies of other large-scale databases of "*overtly*" collected information. Those responsible for the "*Extremism Database"* are also likely to have access to the above forms of intelligence-gathering, and seem to be making use of it.[19]

4. A "minor" infringement?

4.1 Each of the above forms of technology can be used to monitor and record individuals' activity in public. Although ostensibly "*overt"*, they represent a significant intrusion into individual privacy. By way of example, "*tweets"* posted from mobile phones can reveal location data,[20] and their content can also reveal individual opinions (including political opinions) as well as information about a person's preferences, sexuality, and health status. Images recorded on body-worn cameras at protest encampments can reveal not only, "*any interactions with individual officers, but potentially images of protesters cooking meals, talking to each other, and other activities that are a routine part of daily life. This allows police to establish family relationships, friendship groups and identify different*

[17] House of Commons Science and Technology Committee: "*Current and future uses of biometric data and technologies"*, Sixth Report of Session 2014-15, at §97.
[18] Home Office: "*Covert Surveillance and Property Interference: Revised Code of Practice"*, at §2.27.
[19] As the references to "tweets" sent by Baroness Jenny Jones in the applicant's evidence suggest.
[20] "*A Question of Trust"*, at §4.30.

people's roles at or visiting a camp. It also enables the police to monitor movements to and from a camp or protest site and their vehicle details."[21] The use of CCTV and ANPR can then monitor and record individual movements (including vehicle movements) around the country.

4.2 Accordingly, the combination and cross-reference of this publicly accessible data allows a substantial picture to be built of a person's habits, interests, connections, opinions, and location. For example, the systematic recording of individual movement in a searchable database, even if the movement is in the "*public domain*", is highly intrusive. As the Venice Commission of the Council of Europe commented,

> "*… the physical location of a person at a given moment of time may sometimes be established by merely observing that person in a public place, which arguably reduces the "privacy expectation" attached to this information. At the same time systematic tracking of all movements of a particular person during a certain period of time, or even real-time, constitutes a much deeper penetration into his or her private life.*"[22]

4.3 This Council of Europe finding reflects the recent judgment of the United States Supreme Court in *United States v Jones*, 132 S Ct 945 (2012), a case considering monitoring of largely public movements by GPS technology. As Justice Sotomayor explained in her concurring opinion, at 956:

> "*Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'*"

4.4 When attending public demonstrations, members of the public may expect to be seen by members of law enforcement agencies. But they are also entitled to expect that they would not, simply as a result of peaceful attendance, be identified and recorded on a searchable database relating to "*domestic extremists*". The retention of their data on a database of "*domestic extremists*" removes their autonomy over their personal data. It can give an overview of their behaviour, their social relationships, their private

[21] Network for Police Monitoring,, 22nd August 2016: https://netpol.org/2016/08/22/privacy-body-worn-video/
[22] Venice Commission: "*Poland - Opinion on the Act of 15 January 2016 amending the Police Act and certain other Acts, adopted by the Venice Commission at its 107th Plenary Session*" (Venice, 10-11 June 2016), at §26.

preferences and their political identity. It has the potential to impact seriously on their personal reputations and employment prospects, if wrongly or accidentally disclosed.

4.5 Accordingly, Privacy International respectfully disagrees with the suggestion that this is a case about a "*minor*" interference with individual privacy. The rapidly developing dimensions of data created by new technology permits the large-scale recording of "*overt*" activity in a way that represents a highly intrusive infringement with personal privacy. The issue in this case was therefore better encapsulated by Lord Toulson, in his dissenting judgment in the Supreme Court, at §69:

> "*One might question why it really matters, if there is no risk of the police making inappropriate disclosure of the information to others. It matters because in modern society the state has very extensive powers of keeping records on its citizens. If a citizen's activities are lawful, they should be free from the state keeping a record of them unless, and then only for as long as, such a record really needs to be kept in the public interest*."

5. The impact on freedom of expression and assembly

5.1 The use of such large-scale databases as the "*Extremism Database*" is not only a very serious infringement with personal privacy, but also a serious interference with freedom of expression rights. Privacy International notes with concern the evidence summarised at paragraph 13(b) of the applicant's "*Supplementary Information on the Facts and Complaints*". The inclusion of dismissive comments about independent journalists, among others, in the "*Extremism Database*" graphically underlines the seriousness of the Article 8(1) infringement in this case and the absence of adequate safeguards under Article 8(2). The more serious the interference with freedom of expression and assembly, the more clear the need for strict legal safeguards:

5.2.1 In *McCartan Turkington Breen v Times Newspapers Ltd* [2001] 2 AC 277, at 297, and *R v Shayler* [2003] 1 AC 247, at §21, Lord Steyn and Lord Bingham respectively described freedom of expression as having "*the status of a constitutional right with attendant high normative force*", and "*a fundamental right*" which "*has been recognised at common law for very many years*". One of the consequences of giving constitutional status to freedom of expression is that clear words are required to restrict it and there is a narrower approach to the interpretation of legislative provision that restricts it;

5.2.2 This *dicta* reflects a wider common law position, as memorably set out by Holmes J in *Abrams v United States* 250 US 616, Holmes J, at 630:

> *"… the best test of truth is the power of the thought to get itself accepted in the competition of the market …. That, at any rate, is the theory of our Constitution … I think that we should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death, unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country."*

5.2.3 This Court's jurisprudence has repeatedly stressed the need to narrowly interpret any provision which infringes an individual's freedom of expression. In *Sunday Times v United Kingdom (No 2)* [1992] 14 EHRR 123, the Court held, at §50(a), that "*Freedom of expression constitutes one of the essential foundations of a democratic society*" and that any exception to freedom of expression "*must be narrowly interpreted*" and "*convincingly established*". In *Goodwin v United Kingdom* (1966) 22 EHRR 123, at §39, the Court stressed the importance of safeguards for the press, particularly as regards the protection of journalistic sources, which "*is one of the basic conditions for press freedom*".

5.3 This clear line of authority demonstrates that any interference with political expression is inherently serious and not merely "*minor*". It also suggests that particularly strict safeguards are required to regulate any interference with freedom of expression and assembly.

5.4 Given that this application arises in the context of the collection and retention of information relating to political expression, this authority is clearly of assistance. The act of recording participants at an assembly may have a chilling effect on the exercise of freedom of assembly and expression rights.[23] Databases that record who members of the press speak to and when could be seen to interfere with the protection of journalistic sources, an aspect of freedom of expression rights that usually requires

[23] Joint report of the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, 4th February 2016 (AHRC/31/66), at §76.

judicial oversight.[24] The overt surveillance capabilities produced by such databases also permit the police to identify protestors and then to take practical steps in preventing them from attending demonstrations even before they have arrived at a protest site. Where a person is prevented from attending a peaceful assembly, the oversight measures must be foreseeable and formulated with sufficient precision to enable the citizen to regulate his conduct.[25] The measures in place in this case do not meet these standards.

6. Conclusion

6.1 When the context of this application is fully understood, the interference with the applicant's Article 8(1) rights is significant. This renders it difficult to justify the lengthy retention of his personal data and strengthens the need for strict safeguards. Privacy International therefore encourages the Court to consider how its judgment in this case may impact the legal safeguards applicable to all forms of "*overt*" intelligence-gathering. In doing so, the Court may wish to look to well-established minimum safeguards in the Court's case law on state databases, which establish the need for clear time limits for retention, independent review of the retention, guidance as regards the risk of stigmatisation of those entitled to the presumption of innocence, and clear, strict rules regarding the creation, nature, scope and duration of use of the database.[26] These safeguards are mandatory and reflect wider international law principles.[27]

JUDE BUNTING
Doughty Street Chambers

CAMILLA GRAHAM WOOD
Privacy International
23rd September 2016

[24] *Sanoma Uitgevers BV v Netherlands* [2011] EMLR 4, at §§88-92, *Telegraaf Media Nederland Landelijke Media BV v Netherlands* (2012) 34 BHRC 193, at §§101-102, *Nagla v Latvia* (App. No. 73469/10), at §§89-90
[25] See, for example, *Djavit An v Turkey* (2005) 40 EHRR 45, at §§65-68.
[26] *S and Marper v UK* (2009) 48 EHRR 50, at §119; *MM v UK* (App. no. 24029/07), at §§202 and 206; *Shimovolos v Russia* (2014) 58 EHRR 26, at §§68-70. These standards are similar to those that apply in respect of "*covert*" surveillance; see, most recently, *Szabo v Hungary* (2016) 63 EHRR 3, at §§61-89 and *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources* (C-293/12) [2015] QB 127, at §§60-68.
[27] Many of these minimum safeguards are reflected in the recommendations in the joint report of the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, at §78.