Automated Number Plate Recognition: Data Retention and the Protection of Privacy in Public Places

Lorna Woods
University of Essex

Introduction

The Investigatory Powers Act (IPA) was a response to concerns about surveillance in the light of a series of cases from both European courts[1] which found the challenged regimes to be inadequately specified in law and disproportionate. The IPA is not, however, a complete regime for all types of surveillance and intelligence gathering. This article considers another such area, the use of Automated Number Plate Recognition (ANPR), which raises the difficult issue of privacy in public places and which in the main lies outside the IPA. Relying on jurisprudence on the right to a private life from the European courts, this article puts forward the argument that ANPR and the retention of ANPR data constitutes an interference with an individual's right to privacy. As well as the concerns arising from systemic retention of data and inadequate handling arrangements, this article addresses the question of whether ANPR constitutes an intrusion into locational privacy, a subset of privacy that has not been directly discussed yet in domestic legal literature. Any intrusion into privacy must be justified: that is, it must be for a legitimate purpose, in accordance with the law, and proportionate. It is argued that the current regime regarding ANPR is deficient in a number of respects when measured against these requirements, and that the domestic courts' approach to privacy is likewise insufficient. The ANPR regime also illustrates the problematic, minimalist response of the UK to European rulings on privacy generally and state surveillance specifically.[2] In failing to respect the underlying principles, any regime runs the risk of being challenged and the article concludes by recognising that risk in this context. With increased deployment of ANPR, this issue is one of significance for road users and law enforcement alike. As other surveillance technologies which contribute to the erosion of privacy in public spaces, notably drones (UAV) and body worn video (BWV), become increasingly used, the questions raised here have more general significance.

Automated Number Plate Recognition and the Current Domestic Regulatory Framework

ANPR, whether mounted in cars or in fixed locations, is a form of CCTV used to read and store vehicle number plates. The police ANPR system in England stores two images in respect of each 'read': one is of the number plate; the second, an image of the whole vehicle. The time and location of the read is also recorded. The data are processed locally by police forces before being transferred to the National ANPR Data Centre (NADC). The data is then available to the police for searching nationally. The Metropolitan Police (the Met) has a separate system, which was introduced to tackle terrorist threats connected to the London Olympics. Data in

[1] See e.g. Case C-362/14 *Schrems* v *Data Protection Commissioner*, judgment 6 October 2015 (Grand Chamber) ECLI:EU:C:2015:627 and 650; Joined Cases C-203/15 and C-698/15 *Tele2/Watson*, judgment 21 December 2016 (Grand Chamber) ECLI:EU:C:2016:572 and 970; *Roman Zakharov* v. *Russia* (App. no 47143/06), judgment 4 December 2015 (Grand Chamber); *Szabó and Vissy* v. *Hungary* (App. nos 11327/14 and 11613/14), judgment 12 January 2016.

[2] See e.g Emmerson et al *Human Rights and Criminal Justice* (2nd ed) (London: Sweet and Maxwell, 2007), para 7.13-14; S., McKay, *Covert Policing: Law and Practice* (2nd ed) (Oxford: OUP, 2015) para 1.16.

NADC is stored for all vehicles, including data for vehicles that are not known to be of interest at the time of the read, if ever. The amount of data stored is vast: the NPCC ANPR Strategy suggests a figure of 40 million reads daily. While the ANPR web-page states that ANPR data is held for two years,[3] The Commissioner for Surveillance Cameras (CSC) noted that there were plans to extend the period of data retention from two years to a maximum of seven. Further, according to ANPR User Group minutes, the Met has retained data for longer than two years.[4]

The ANPR system can cross check ANPR data with lists of driver information. These lists include, for example, details of those without valid insurance or of suspects in ongoing investigations. In addition to immediate cross-checking for problem cases, the data may be retained for future use in criminal investigations generally. The CSC's Report for 2014/15 noted that the NADC data can be used for data mining in a number of ways: real time and retrospective vehicle tracking; identifying all vehicles that have taken a particular route during a particular time frame (vehicle matching); identifying all vehicles present in a particular place at a particular time (geographical matching); verifying alibis, locating offenders or identifying potential witnesses; linking individuals to identify vehicles travelling in convoy (network analysis); and subject analysis when ANPR data is integrated with other sources of data (CCTV, communications analysis, financial analysis) to create an in-depth profile of an individual. These different types of analysis mean that the data generated by ANPR may be used predictively and generally. In this, we see a shift from specific and suspicion-based collection and use of data to a less discriminate system which poses greater risks for individual privacy.[5]

While there is no specific statutory mention of ANPR, certain legislation is relevant to its operation: the Data Protection Act 1998 (DPA), the Protection of Freedoms Act 2012 (PoFA) and possibly the Regulation of Investigatory Powers Act 2000 (RIPA) and IPA. The use of ANPR falls within the DPA as the registration number and the wider vehicle image could constitute 'personal data'.[6] Data protection principles therefore apply. The Information Commissioner issued a Code of Practice[7] with regard to CCTV, including ANPR cameras, elaborating the data protection rules in this context. It does not, however, provide a legal basis for the collection of data. PoFA (which applies only to England and Wales) established the CSC, who likewise developed a code[8] on the appropriate use of surveillance cameras by relevant authorities, including the police.[9] The obligation on relevant authorities is to have regard to the code; non-compliance is not in itself a civil wrong or criminal offence.[10] The

---

[3] See also ACPO, *The Police use of Automatic Number Plate Recognition: A review by a working group of interested parties aimed at addressing concerns and providing understanding of the workings and regulation of the system*, January 2013, available at: http://www.npcc.police.uk/Publication/ANPR/The%20police%20use%20of%20ANPR%20FinalJan2013.pdf, accessed 24th January 2017

[4] ANPR National User Group, Minutes, 3rd June 2015, available at: https://www.whatdotheyknow.com/request/289438/response/730763/attach/html/6/03%20ANPR%20NUG%20Minutes%2003062015.pdf.html, accessed 24th January 2017

[5] See e.g. European Data Protection Supervisor, *Towards a New Digital Ethics: Data, dignity and technology,* Opinion 4/2015, 11 September 2015, p 6, pp. 12-13

[6] S. 1 DPA

[7] ICO, *In the picture: A data protection code of practice for surveillance cameras and personal information*, 21 May 2015, available at: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf, accessed 24th January 2017

[8] Home Office, *Surveillance Camera Code of Practice*, June 2013.

[9] Section 29 POFA; Home Office, *Circular 011/2013: surveillance camera code of practice*, 12 August 2013

[10] Section 33 PoFA

code reflects at a very general level some of the concerns protected by Article 8 ECHR/ Article 7 EUCFR. The two codes have principles in common, as the Information Comissioner's code makes clear, though each has separate 'enforcement' processes. In particular, the role of the CSC is not enforcement of the code but rather to encourage compliance.[11]

Covert surveillance falls outside DPA and PoFA, being dealt with by RIPA. Part II of RIPA, which provides some basis for investigatory techniques which previously had none, applies to the use of covert directed or intrusive surveillance by designated public authorities[12] (as well as to covert human intelligence sources (CHIS)[13]). Authorization for directed surveillance and CHIS is given by a police superintendent[14] and for intrusive surveillance the approval of a senior authorising officer is required. A failure to obtain authorization seems, however, to have no legal consequences.[15] Note that electronic tracking devices are expressly excluded from the intrusive surveillance regime and other forms of surveillance – such as CCTV – do not fit easily in the framework.[16]

The IPA does not regulate the creation of ANPR datasets or their analysis by the police. Part VII IPA provides some control over the use by intelligence agencies of "bulk personal datasets". "Bulk personal datasets" are defined in s. 199 IPA as a set of information that includes personal data relating to a number of individuals where the majority of those individuals are not and are not likely to be of interest to the intelligence services and where an intelligence service retains the set, which is held electronically for analysis. ANPR data could fall within this definition. Therefore, an intelligence agency seeking to analyse ANPR data would require a warrant so to do. Whether the provisions themselves are acceptable from a privacy perspective is one question,[17] and one which falls outside the scope of this article. What is clear is that the IPA does not regulate the police use of ANPR.

Finally, it should be noted that some police powers to investigate are based in the common law.[18] In the case of *Wood*, [19] which involved the photography by the police of Wood, the Court approved older jurisprudence[20] which described police powers broadly as all steps necessary for preventing crime. Insofar as this is accepted, the common law basis, which is open-ended, could be used also in relation to ANPR.

Human Rights Standards

Answering the question of whether the ANPR regime is open to challenge requires the identification of standards against which that regime should be measured. In this context, the two European systems, the Council of Europe and the European Union, and their respective

[11] Section 34 PoFA

[12] Emmerson n. 2, para 7-47.

[13] S. 26(7) RIPA.

[14] S. 28 RIPA; see Emmerson, n. 2, paras 7-49- 7-53.

[15] *C* v. *Police and Secretary of State* IPT/03/32/H, para 42; C.f. Tugendhat J. in *AJK* v *Commr of Police of the Metropolis* [2013] 1 WLR 2734 .

[16] C Walker *Terrorism and the Law* (Oxford: OUP, 2011), para 2.70.

[17] See *Privacy International* v. *Secretary of State for Foreign and Commonwealth Affairs and Ors* [2016] UKIPTrib 15_110_CH. Bulk personal datasets are among the provisions being challenged by Liberty in a judicial review action launched 28 February 2017.

[18] O'Floinn and Omerod suggest that the common law could be used in respect of police activity which does not clearly fit into the existing statutory framework in the context of social media surveillance: 'Social Networking Sites, RIPA and Criminal Investigations' (2011) 10 *Crim LR* 766, p. 775.

[19] *Wood* [2008] EWHC 1105 (Admin).

[20] *Rice* v *Connolly* [1966] 2 QB 414.

human rights documents – the European Convention on Human Rights (ECHR) and the European Charter of Fundamental Rights (the Charter) – appear relevant, but are both applicable to the situation at hand?

The Human Rights Act (HRA) implements the ECHR. It requires public authorities, for example the police, to act compatibly with a number of rights in the ECHR, including Article 8. When considering a question concerning the ECHR, national courts must have regard to the case law of the European Court of Human Rights (ECtHR). While the ECtHR's jurisprudence is not binding on the English courts,[21] it will normally be followed[22] and, where a discrepancy in approach arises, an individual may still bring a claim before the ECtHR.

The Charter applies only within the scope of EU law[23] but the boundaries of EU law are not precisely delineated. While the protection of rights forms part of the basis of the EU, it cannot create the grounds for its own application.[24] Article 16 TFEU (and Article 39 TEU as regards common foreign and security policies) gives the EU power to take action in respect to the right to data protection (but not the right to private life). Are these provisions sufficient to bring all data protection activities within the scope of EU law? Notably, the UK takes the position that, in relation to shared competence, if the Union has not acted then the specific issue does not fall within the scope of EU law.[25] The position on this point is not yet clear,[26] though the Court of Justice is unlikely to view the matter so narrowly.[27] Furthermore, there are a number of EU instruments which particularise the right: the Data Protection Directive,[28] shortly to be replaced by the General Data Protection Regulation (GDPR);[29] and Law Enforcement Data Protection Directive,[30] replacing Framework Decision 2008/977/JHA.

The position remains more complex than suggesting that this legislative activity results in all data processing activity falling within the scope of EU law.[31] It could be argued that, because the Framework Decision is in place,[32] the question of whether police activities fall within EU

---

[21] E.g. *R (Ullah)* v *Special Adjudicator* [2004] UKHL 26, para 20

[22] *R*. v *Horncastle* [2009] UKSC 14

[23] The Charter specifies refers to implementing EU law but the Court in Case C-617/10 *Åkerberg Fransson*, ECLI:EU:C:2013:105, returned to the phraseology adopted in pre-Lisbon case law.

[24] Article 6 TEU; Article 51(2) Charter

[25] Supported by Protocol 25 on the Exercise of Shared Competence

[26] The Court of Justice seems to have taken a very broad approach in *Fransson,* n. 23, but a much narrower one in Case C-446-9/12 *Willems* ECLI:EU:C:2015:238. *Willems* has been criticised: S Peers, 'Biometric Data and Data Protection Law: the CJEU Loses the Plot' (2015) August/September *Computers and Law*

[27] Safjan, M., 'Fields of application of the Charter of Fundamental Rights and constitutional dialogues in the European Union' EUI Distinguished Lectures 2014/02 (CJC DL 2014/02), 9 May 2014, available: http://cadmus.eui.eu/bitstream/handle/1814/32372/CJC_DL_2014_02.pdf?sequence=3, accessed 2 February 2017, p. 5.

[28] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

[29] Regulation (EU) 2016/679 General Data Protection Regulation [2016] OJ L119/1

[30] Directive (EU) 2016/680 on the protection of natural persons with regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data [2016] OJ L 119/89.

[31] Case C-442/00 *Caballero* v *Fondo de Garantia Salarial* (Fogasa) [2002] ECR I-11915, paras 29 – 30

[32] Implemented in the UK: Ministry of Justice, Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008/799/JHA, Circular 2011/01, 25th January 2011

law depend on that instrument's scope. The Framework Decision relates only to cross border data flows, however. The new Law Enforcement Directive covers police processing generally but will come into force in 2018.[33] This current gap may be more apparent than real because of the existence of the general data protection regime. Although there are exceptions for law enforcement in the Data Protection Directive,[34] a Member State's act of derogation still falls within the scope of EU law.[35] On that basis, while there may be scope for derogating from the substantive processing rules, relevant authorities would still have to comply with the Charter in so doing. As regards the new Law Enforcement Directive, the position is complicated by the UK's position under Title V of the TFEU: the UK is not bound by measures under Title V of TFEU unless it opts into them.[36] As a result, public authorities 'are not bound by the rules laid down' in the Law Enforcement Directive in respect of measures into which the UK has not opted.[37] The UK government argued that the Law Enforcement Directive will not apply to internal situations in the UK.[38]

It is far from clear that the Government's position is correct. First, the UK has opted in to some actions, for example those relating to terrorism, child pornography and people trafficking.[39] Insofar as data acquisition, retention and examination could be used in relation to those actions, the processes would have to comply with the Law Enforcement Directive and thus be within the scope of EU law. Attempting to separate data collected and retained on a bulk scale according to its use would be practically impossible. Secondly, the possibility to opt-in is provided by EU law and therefore, following *NS*, should fall within EU law.[40] In *NS*,[41] the exercise of a discretionary power by the Secretary of State in the context of the Dublin Regulation on asylum seekers was held to form part of the EU system of law. The commonality between discretion and derogation is that in both instances EU law provides the framework within which Member States' choices are exercised.[42] Finally, it makes little sense to suggest that an area that currently falls within the scope of EU law as derogation from the Data Protection Directive would subsequently fall outside EU law after the enactment of a directive

[33] Article 3(7) Law Enforcement Directive, n. 30

[34] Article 13 Data Protection Directive, n. 28

[35] Case C-260/89 *ERT* v *DEB* [1991] ECR I-2925, which is mentioned explicitly in the Explanations regarding Article 51 Charter; K Lenaerts and JA Gutiérrez-Fons, 'The Constitutional Allocation of Powers and General Principles of EU Law' (2010) 47 *Common Market Law Review* 1629

[36] Article 6a of Protocol 21 to the EU Treaties on the position of the UK and Ireland in respect of the area of freedom, security, and justice annexed to the TFEU.

[37] Recital 99 Law Enforcement Directive, n. 29. The UK chose to be bound by the Law Enforcement Directive: Kenneth Clarke, MP Personal Data Directive, Hansard, 19 June 2012, Column 57WS-58WS.

[38] Ministry of Justice, Call for Evidence on the Review of the Balance of Competences between the United Kingdom and the European Union: Information Rights (2014), available at: https://consult.justice.gov.uk/digital-communications/balance-of-competency-review-information-rights/user_uploads/boc-information-rights-call-for-evidence.pdf-2, (accessed 2nd February 2017), para 45

[39] See list of measures here: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/405887/Opt-in_webpage_update_-_data_-_Feb_2015.pdf, accessed 3 February 2017

[40] Accepted in e.g. *R (on the application of Zagorski and Base)* v *Secretary of State for Business, Innovation and Skills* [2010] EWHC 3110 (Admin), paras 69–70.

[41] Joined Cases C‑411/10 and C‑493/10 *NS* v. *Secretary of State for the Home Department* (C-411/10) and *M. E. and Ors* v. *Refugee Applications Commissioner* (C-493/10) (Grand Chamber), judgment 21 December 2011, ECLI:EU:C:2011:865.

[42] P Eeckhout, 'The EU Charter of Fundamental Rights and the Federal Question (2002) 39 *Common Market Law Review* 975, p. 978.

specifically on point. It therefore seems likely that the activities of law enforcement do fall within the scope of EU law and must comply with the Charter (as well as the ECHR).[43]

Following Brexit, it is unclear how much will change. The UK, unless steps are taken to change the position here too, will still be part of the ECHR and will continue to have effect through the HRA. The Charter will not be directly relevant to the UK, but it may still have an indirect effect. If the UK wants to maintain data flows with the EU an adequacy decision under the GDPR will effectively be required. Achieving this has the effect of bringing the UK into a position where its laws may be assessed by reference to the Charter, as can be seen in *Schrems*.[44] *Schrems* concerned the challenge to the adequacy decision made in respect of the United States. In that case, the internal arrangements of the United States were assessed for their impact on privacy by reference to Articles 7 and 8 of the Charter and this included policy fields – such as national security – which normally fall outside the scope of EU competence. It may be that this indirect review of the UK is broader than that to which it is currently subject as a Member State.

Privacy in Public Spaces

The first consideration is whether privacy, and specifically Article 8 ECHR or Articles 7 and 8 of the Charter, apply. Article 8 ECHR is broad, comprising a number of elements: private life, family life; home; and correspondence. The Charter provides protection in similar terms in Article 7; Article 8 EUCFR provides a separate right to data protection. The ECtHR has interpreted 'private life' broadly.[45] In general terms, the Charter will be interpreted in line with the ECHR.[46] 'Private life' includes personal, social and economic relations; moral and physical integrity;[47] personal identity;[48] personal information;[49] reputation;[50] and personal or private space.[51] As the ECtHR noted in *Pretty*, the notion of personal autonomy is central to its understanding of Article 8 ECHR[52] and '[t]he very essence of the Convention is respect for human dignity and human freedom'.[53] It is certainly not limited to confidentiality, secrecy or aloneness. Nonetheless, Article 8 ECHR, and its Charter equivalents, cannot cover every aspect of our lives or every relationship that we might form.[54] In the context of a claim that a ban on hunting was an interference with Article 8 ECHR, Baroness Hale in the Supreme Court, stated that the protection of psychological and physical space protected by the right fell 'some way short of protecting everything they might want to do even in that private space; and it certainly does not protect things that they can only do by leaving it, and engaging in a very public gathering and activity'.[55] This raises the question as whether individuals can rely on Article 8 ECHR (or Articles 7 and 8 EUCFR) in relation to public activities, such as driving down a road and what sorts of State activity constitute interference. The position in this area

[43] D. Anderson *A Question of Trust* (2015) accepted this point but without distinguishing between different activities, para 5.2
[44] *Schrems*, n. 1
[45] *Pretty* v. *UK* (App no. 2346/02), judgment 29 April 2002.
[46] C-400/10 PPU, *J. McB.* v *L. E* [2010] ECR I-8965; Article 52(3) Charter
[47] E.g. *Bensaid* v. *UK* (App no. 44599/98) [2001] ECHR 82
[48] E.g. *Stübing* v. *Germany* (App no. 43547/08), judgment 12 April 2012
[49] E.g. *L.H*. v *Latvia* (App. no 52019/07), judgment 29 April 2014
[50] *Mikolajová* v. *Slovakia* (App. no 4479/03), judgment 18 January 2011
[51] *Peck* v *UK* (App no. 44647/98), judgment 28 January 2003, [2003] ECHR 44; *Wood* v. *Commissioner of Police for the Metropolis* [2009] EWCA Civ 414
[52] *Pretty*, n. 45, para 61
[53] *Pretty*, n. 45, para 65
[54] *Barbulescu* v *Romania* (App. no. 61496/08), judgment 12 January 2016
[55] *Countryside Alliance and others* v *Attorney General and another* [2007] UKHL 52, para 116

is not entirely clear, and it is arguable that there is some difference in approach especially as regards the domestic courts.

The starting point for the domestic courts and the ECtHR is similar[56]; that being observed in public does not trigger privacy.[57] Equating the taking of a photograph to the act of observing with the naked eye, photography (in a public place) on its own is not contrary to English law,[58] though its subsequent dissemination might constitute misuse of private information.[59] In *Peck*, the ECtHR distinguished between the monitoring of someone in a public place (via CCTV) and the recording of that image.[60] It found that the further dissemination of the CCTV images to the media constituted an infringement of Article 8, but did not consider the question of whether the process of creating the images also constituted an intrusion because Peck did not argue this point. While in practice there may be close connections between these stages, it is important to note that there are at least three of them: the viewing of an individual; the creation of a record (howsoever structured); and use of that information. Dissemination could be a fourth state. It is an open question whether the creation of a temporary record as part of the observation process fits in stage one or two. These different stages may affect privacy to different degrees. The ECtHR has also recognised the interests affected by unwanted photography. In *Reklos*,[61] *r*easoning from the fact that Article 8 protects an individual's identity, it held that a person's image revealed his or her unique characteristics and constituted one of the chief attributes of his or her personality. Effective protection of the right to control one's image required the consent of the person concerned when the picture was being taken and not just in relation to publication of that image. The image in this case was taken in the hospital. It may not therefore translate exactly to photography/recording in public places. Although the ECtHR recognised this point about location, it is significant that the judgment was not based on spatial considerations, but on concerns for personality.

Peck reminds us that Article 8 protections are not limited to private spaces. Numerous cases affirm that there is 'a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'[62]. While there is no automatic claim for privacy in a public space, especially for public persons,[63] such a claim cannot be totally excluded either. In *von Hannover* Article 8 was held to be applicable.[64] The case concerned the applicant, a public person, engaged in activities such as shopping, horse-riding or meeting her boyfriend, activities which the Court held fell within her private life. In finding that there had been an infringement, the ECtHR emphasised that the images of 'intimate "information"' were taken 'in a climate of continual harassment'.[65] Although *von Hannover* concerned less

[56] The Court of Justice has not ruled on this point. The case of *Ryneš v Úřad pro ochranu osobních údajů* (Case C-212/13), ECLI:EU:C:2014:2428, concerned CCTV overlooking a public space but focussed on the meaning of 'household exception' in Article 3(2) Data Protection Directive. Nonetheless, the Court of Justice emphasised the importance of privacy, albeit as an interpretive principle of the Directive generally.

[57] *Herbecq* v *Belgium* (App no 32200/96 and 32201/96) Dec 14 Jan 1998, Decisions and Reports (1999) 92-9.

[58] Clayton, R., and Tomlinson, H., *The Law of Human Rights* (2nd ed) (OUP) para 12.142, c.f. more recently *Weller* v *Associated Newspapers* [2015] EWCA Civ 1176 para 61, discussed *Clerk and Lindseel on Torts* (21st ed) Main Volume, 'Breach of Confidence and Privacy', para 27-42.

[59] *Campbell* v. *MGN* [2004] UKHL 22

[60] *Peck*, n. 51, para 59

[61] *Reklos* v *Greece* (App no 1234/05) judgment 15 January 2009, para 40

[62] *Von Hannover* v. *Germany* (App no. 59320/00), judgment 24 June 2004, [2004] ECHR 294, para 50; *Peck*, n. 51, para 57; *PG and JH* v. *UK* (App no. 44787/98), ECHR 2001 IX, para 56.

[63] *Von Hannover* (No 2) v *Germany* (2012) 55 EHRR 15, paras 109 to 113

[64] *Von Hannover*, n. 62, para 69

[65] *Von Hannover*, n. 62, paras 59 and 70.

clearly sensitive information than *Peck* and was more public than *Reklos*, it also involved an ongoing monitoring that of itself could be intrusive. In sum, in each of these cases, there was some exacerbating factor beyond the taking of the photograph, though the factor was not the same in each case.

Von Hannover also referred to the applicant's 'legitimate expectation of privacy'. This phrase, or its variant 'reasonable expectation of privacy', has become central to the jurisprudence on Article 8 ECHR and the English tort, misuse of private information, developed from *Campbell*.[66] Following *Campbell*, the taking of a photograph is viewed as a use of private information in a particularly sensitive format. Many of the cases have involved intrusion by the media, rather than the State. They therefore require the balancing of two rights: the right to private life and the right of the media to freedom of expression, but before this balancing takes place, the claimants must demonstrate that there is a 'reasonable expectation of privacy' in the information.[67] This is a fact sensitive analysis in which a range of factors are taken into account: the sensitivity of the information; the context in which the information was obtained; and whether the information was in the public domain.[68] Significantly, in these media cases, the English courts have recently accepted that even innocuous public activities could give rise to a reasonable expectation of privacy.[69] Note, however, that in these cases, photography of children who had not themselves courted publicity was involved. Without such exacerbating factors would the court have so found?[70]

We must also question whether the approach in *Von Hannover* and *Campbell*, which applies in the relationship between non-state actors, is - or should be applied - in exactly the same way when the intrusion is committed by the State. In *Kinloch*, which concerned police observation of a suspect, the Supreme Court held that a person cannot have a reasonable expectation of privacy in criminal acts, and such a person in public takes the risk that his actions will be noted.[71] In the subsequent *Re JR38*,[72] the Supreme Court was split as to whether Article 8 ECHR was engaged. The case concerned the publication of CCTV stills in the media to facilitate the identification of an individual who had been involved in rioting. While most of their Lordships felt that the test of a reasonable expectation of privacy was the key, and that the criminal nature of a person's activities was found to be relevant in limiting that expectation, Lord Kerr in the minority held that it was an important factor but not determinative.[73] Arguably, the majority over-emphasised a particular conception of 'reasonable expectation of privacy', a conception which blurs factors for the applicability of the right to private life with considerations taken into account when justifying any interference. Such an approach runs the risk of undermining the human rights protection of those suspected or convicted of an offence. Indeed, the ECtHR has ruled that the publication of images of those involved in criminal cases have violated Article 8.[74] Moreover, the question of whether an assessment of the privacy right's engagement should not be solely about whether there is a reasonable expectation of privacy. Rather, as suggested by Lord Kerr in *JR38*, this test although important factor is not

[66] *Campbell*, n. 59, Lord Nicholls, paras 11-22
[67] *McKennit* v *Ash* [2008] QB 73
[68] Clayton and Tomlinson, n. 58, paras 12.27-12.40; for the position at the ECtHR see *von Hannover* (No 2), n. 63.
[69] *Murray* v *Big Pictures (UK) Ltd* [2008] EWCA Civ 446; *Weller* n. 58
[70] *Campbell* n. 59; *Wood*, n. 51, paras 32-36.
[71] *Kinloch* v *HM Advocate* [2013] 2 AC 93.
[72] *In re JR38* [2015] UKSC 42.
[73] *Re JR 38* n. 72, para 56.
[74] E.g. *Sciacca* v *Italy* (App no. 50774/99) ECHR 2005-I, paras 28-29

the only factor. It is submitted that Lord Kerr's approach reflects the recent trend in Strasbourg jurisprudence.

There is another line of jurisprudence which partially overlaps with that on photography; it concerns the distinctive position of the State as regards the records it holds on citizens. Consistent case law suggests that the storing of information relating to an individual's private life triggers Article 8.[75] In *PG and JH*, the ECtHR held that private life considerations may arise once a systemic or permanent record comes into existence; that person's expectation as to privacy may be relevant but not conclusive.[76] In *Rotaru*, the information concerned the applicant's public protest and political affiliations – activities that are not particularly private. In finding an intrusion, the nature of the information so recorded and the question of whether the information has been accessed are irrelevant.[77] In focussing on the creation of files, the ECtHR reflects the concerns that underpinned the development of data protection rules.[78] While the Court of Justice has had little opportunity to rule on media intrusion, it has emphasised the importance of data protection, both in its own right and in connection with the right to privacy. Significantly, focusing on data storage and the State use of databases as a specific intrusion takes the courts away from considering only the 'reasonable expectation of privacy', a problematic - if not circular – and potentially subjective test.[79]

Although the vast majority of the cases concerning State storage of data have taken the view that storage of data is sufficient no matter the nature of the data, an outlier case should be noted: *S and Marper*.[80] While it re-affirmed the previous jurisprudence, the ECtHR also seemed to limit the concern about storage to 'data relating to the private life of an individual'. In so doing, it suggested that relevant factors would not be limited to the content of the data, but – referring to the cases broadly about photography in public by authorities- also the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.[81]

The approach of the Supreme Court to this issue is uneven. In *Catt*,[82] the police took photographs of Mr Catt at demonstrations. Although he was not convicted of any public order offences, the police kept the photographs, along with further information on Mr Catt and his relationships with other protestors. His challenge to the legality of this went through the domestic court system to the Supreme Court, and is now pending at Strasbourg.[83] In *Catt*, one point on which their Lordships were unanimous was that Article 8 applied. Lord Sumpton

---

[75] *Rotaru* v. *Romania* (App. no. 28341/95), judgment 4 May 2000 (Grand Chamber), [2000] ECHR 192, paras 43 and 48; *Leander* v. *Sweden* (Series A/116), judgment of 26 March 1987, para 48; contrast Joint Select Committee on Human Rights, *Legislative Scrutiny: the Investigatory Powers Bill*, 1 June 2016, para 2.3.

[76] *PG and JH*, n. 62, para 57

[77] *Kopp* v. *Switzerland* (App. no. 23224/94), judgment 25 March 1998, (1999) 27 EHRR 91, para 93; *Rotaru*, n. 75, para 46; to similar effect in the EU, see Joined Cases C‑465/00, C‑138/01 and C‑139/01 *Österreichischer Rundfunk and Others*, [2003] ECR I-4989, para 75; Joined Cases C‑293/12 and C‑594/12 *Digital Rights Ireland and Others* v. *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform*, judgment 8 April 2014 (Grand Chamber), EU:C:2014:238, para 33; and *Schrems* n. 1 para 87

[78] *Amann* v. Switzerland (App no. 27798/95) (Grand Chamber), judgment 16 February 2000, para 65

[79] C.f. *Weller* n. 58; Lord Kerr's remarks in *JR38*, n. 72; N A Moreham 'Privacy in the common law: a doctrinal and theoretical analysis' (2005) 121 LQR 628, pp. 647-8; E Barendt, 'Problems with the "reasonable expectation of privacy" test' (2016) 8 JML 129

[80] *S and Marper* (App no 30562/04), judgment 4 December 2008 (Grand Chamber) [2008] ECHR 1581

[81] *S and Marper*, n. 80, para 67

[82] *R (on the application of Catt)* v. *Commissioner of Police of the Metropolis* and *R (on the application of T)* v *Commissioner of Police of the Metropolis* [2015] UKSC 9.

[83] *Catt* v. *UK* (App. no. 43514/15), communicated 19 May 2016.

stated, 'there may be some matters about which there is a reasonable expectation of privacy notwithstanding that they occur in public and are patent to all the world. In this context mere observation cannot, save perhaps in extreme circumstances, engage Article 8, but the systemic retention of information may do'.[84] The question of whether the information obtained would be stored or form part of a record was not discussed in *Kinloch* or in *JR38*, suggesting that the Courts there may have thought that storage or further dissemination were also conditional on a reasonable expectation of privacy rather than separate routes to trigger privacy.

It is submitted that the systematic storage of ANPR reads, as well as their subsequent analysis in a variety of ways, constitute intrusions into privacy which must be justified. Insofar as *S and Marper* can be seen as imposing further requirements, either the photographing of the car and its occupants or the impact on 'locational privacy' (discussed below) satisfies any such sensitivity threshold. The argument based on photography is, however, comparatively weak. The main focus is the number plate. The photographing of the driving of a car – without more -is unlikely to be an intimate action, even given the sensitivity of a person's image and the ECtHR's views in *Reklos*, unless the inside of a car is seen as private space. The argument on locational privacy is not only stronger, it raises wider questions about the impact of other interconnected surveillance and tracking devices in public spaces.

Locational privacy refers to the ability of individuals to move in public spaces in normal circumstances without their locations being systematically monitored and/or recorded. Surveillance based on location data can occur in a number of ways. It starts with capture of an individual's location at a particular point in time but can include real time monitoring of a succession of locations providing direction of movement; predictive tracking, which infers a person's near future behaviour by extrapolating from a person's direction of travel; and retrospective tracking, which uses the individual's data trail to reconstruct that person's movements, behaviour and associates, but can be used to suggest purposes and intention.[85] Even without any particularly embarrassing or sensitive incident taking place, the accumulation of many points of incidental information can be intrusive affecting our 'zone of interaction'.[86] So, 'privacy results not from locked door and closed curtains, but also from the way our publicly observable activities are dispersed over space and time'.[87] Location data is seen as sensitive in data protection terms, particularly in the context of smart phones,[88] although other devices –e.g. bank cards and registered Oyster cards - could produce location data having a comparable impact. Locational privacy issues may arise in contexts beyond data storage and analytics; monitoring location data is akin to virtual tracking or directed surveillance of an individual.[89] Recognising this category of privacy is important in understanding the extent of the intrusion into privacy created by the use of technologies including but not limited to ANPR.

---

[84] *Catt* n. 82, para 4; see Bullen Leake and Jacob's *Precedents of Pleadings from Sweet and Maxwell*, Part V-Invasion of Privacy, Section 79 Invasion of Privacy, para 79-07.

[85] K. Michael and R. Clarke, 'Location Tracking of Mobile Devices: Uberveillance Stalks the Streets' (2013) *Computer Law and Security Review*, 209, p. 219.

[86] Clayton and Tomlinson, n. 58, paras 12.31-13.33, noting changing emphasis; *Weller*, n. 58; N A Moreham 'Beyond Information: physical privacy in English law' (2014) *Cambridge Law Journal* 350, p. 355

[87] Uteck, Anne 'Ubiquitous Computing and Spatial Privacy' in Ian Kerr, Valerie Steeves and Carole Lucock (eds) *Lessons from the Identity Trail* (OUP, 2009) citing Reiman, Jeffrey, 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future' (1995) 11 *Santa Clara Computer and High Technology Law Journal* 27

[88] Article 29 Working Party Opinion; *Ittihadieh* v *5-11 Cheyne Gardens RTM Company Ltd & Ors* [2017] EWCA Civ 121

[89] See e.g. Monmonier, M., 'The Internet, Cartographic Surveillance and Locational Privacy in *Maps and the Internet* (Elsevier, 2003); Michael and Clarke, n. 85, p. 220

While locational privacy was never perfectly guaranteed, the development of some technologies (for example BWV, UAV, devices with GPS embedded in them, as well as CCTV and ANPR) pose a greater threat to locational privacy, especially given the greater computing capacity available to store and to analyse any resulting data and the greater ubiquity of such devices. Monitoring of location has similarities to monitoring of social media activity (SOCMINT) in that both may be seen as relating to public, but nonetheless potentially sensitive, activities and the monitoring is consequently intrusive. Omand *et al* suggest that the use of SOCMINT needs careful control for this reason, and suggests that it is similar in impact to directed surveillance.[90]

The ECtHR considered some aspects of locational privacy in *Uzun*.[91] Uzun was suspected of committing terrorist offences so he was tracked via GPS. Uzun argued that the GPS had enabled the authorities to draw up a comprehensive picture of his movements in public for months by means of a measure which was both precise and difficult to detect. The ECtHR accepted that tracking constituted an intrusion with an Article 8 right, even though the car in which the tracker was installed did not belong to Uzun, but a friend of Uzun's, S. It argued that:

> by the surveillance of the applicant via GPS, the investigation authorities, for some three months, systematically collected and stored data determining, in the circumstances, the applicant's whereabouts and movements in the public sphere. They further recorded the personal data and used it in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to, which was later used at the criminal trial against the applicant.[92]

In its analysis, the ECtHR downplayed the impact of such surveillance. It distinguished surveillance by GPS from other methods of visual or acoustical surveillance which, according to the Court, 'are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings'.[93] Even so, Article 8 was clearly engaged though on the facts the interference was justified.

Given that the ECtHR accepted that the determining of the whereabouts in public falls within Article 8, the same argument could be made with regard to ANPR; given the approach to 'passenger name record data' (PNR), which includes travel habits, a similar approach is likely to be taken by the Court of Justice.[94] Of course, ANPR is designed to record cars not people, so not all movements might be recorded – not even all car movements may be recorded. Nonetheless, *Uzun* accepted the link between person and car and implicitly that a perfect record of personal movements would not be required to trigger Article 8. It also seemed to accept that the fact that a car may not have the same occupants in each instance would not undermine this link between car and person. Of course, one might argue that surveillance by ANPR is less intrusive than GPS because of these factors[95] and – by contrast to, for example, UAV and

[90] Omand, Bartlett and Miller 'Introducing Social Media Intelligence' (2012) 27 *Intelligence and National Security* 801, p. 822; see also O'Floinn and Omerod n. 18 on the transformative nature of systemic surveillance in social media, p 777.

[91] *Uzun* v. *Germany* (App no. 35623/05) Reports of Judgments and Decisions 2010-VI 31 December 2010

[92] *Uzun*, n. 91, para 51

[93] *Uzun*, n. 91, para 52

[94] A-1/15 *Canada PNR Opinion,* Opinion 8 September 2016, ECLI:EU:C:2016:656

[95] See Joined Cases C-317 and 318/04 *European Parliament* v *Council and Commission* [2005] ECR I-2467, Opinion of the Advocate General; view of Advocate General in Opinion A-1/15 n. 94.

BWV, limited to public spaces. This argument goes to the intensity of the intrusion, not whether Article 8 is engaged in the first place.

Insofar as it is arguable that ANPR gives only a partial picture, the argument becomes less convincing as increasing numbers of ANPR cameras are installed, making it hard to avoid being recorded and also facilitating a more detailed picture of individuals' movements. While the car does not equate to a person, through DVLA and insurance records likely drivers can be identified; the faces of those in the front seats may also be visible, perhaps bringing in some of the concerns about photography generally. Potentially, this increase in cameras affects our autonomy, as we lose the ability to be free from surveillance, and our choices are limited by the invisible choices of the state. Furthermore, ANPR can be used not just to help identify who drove down a particular road, but also for vehicular matching, network analysis and (possibly in conjunction with other data) in-depth individual profiling, which are more intrusive forms of location surveillance. As with other bulk collection of data, the innocent are 'transformed into potential suspects'[96]. Further, depending on the location of ANPR, some places or areas[97] could be under effectively constant surveillance: a place of worship; a sports stadium. Tracing the vehicles then gives you a means to identify individuals and their connections. This is particularly problematic, however, when specific groups are singled out, raising the risk of discrimination in terms of groups consequently the subject of surveillance.

The ECtHR has recognised that the accumulation of data and its analysis, even where the data points in isolation seem quite harmless, can be revealing. In *Zakharov* and in the EU communications data retention cases both European courts highlighted the impact of communications data, rather than content, being retained and analysed.[98] The Court of Justice noted that such data allows the profiling of the individuals and so is no less sensitive than the actual content of communications.[99] It concluded that the interference, which led to an individual feeling under constant surveillance, was 'very far-reaching and must be considered to be particularly serious'.[100] A similar argument could be made in the context of ANPR, especially where there is an increased density of cameras, the fact that searches may take place across a national dataset and consequently wide geographic scope, and given the potentially broad range of analytic techniques that may be used across NADC. In sum, the courts have recognised that a high degree of monitoring, even in public of insignificant actions can cumulatively be problematic,[101] even a harassment.[102] It may be that in future such

[96] Case A-1/15 *Canada PNR Agreement*, n. 94, Opinion, para 176

[97] Under Project Champion two suburbs in Birmingham were to be monitored by a network of 169 ANPR, including covert cameras, were to form "rings of steel", so that residents could not drive into or out of the areas without being tracked. Project Champion was funded from the police Terrorism and Allied Matters Fund. After this was revealed, the project was abandoned. See Surveillance Camera Commissioner, Speech to the automatic number plate recognition (ANPR) national user group, in York, 26 November 2015, available: https://www.gov.uk/government/speeches/surveillance-camera-commissioners-speech-to-the-anpr-national-user-group-2015, accessed 17 February 2017. A further ring of steel around Royston was subject of a complaint to the ICO, resulting in an enforcement notice

[98] Joined Cases C‑293/12 and C‑594/12 *Digital Rights Ireland*, n. 77, para 27

[99] *Tele2/Watson*, n. 1, para 99

[100] *Tele2/Watson*, n. 1, para 100

[101] R. M. Pomerance, 'Shedding Light on the Nature of Heat: Defining Privacy in the Wake of R v. Tessling (2005) 23 CR (6th) 229, p.234-5 made this point in the Canadian context

[102] *Von Hannover* n. 62; The English courts have also recognised the impact of ongoing surveillance, admittedly obiter and not in this context: *Bernstein* v. *Skyways* [1978] 1 QB 479; contrast a one –off instance where the photography by the police and its context was clear: *Catt* n. 82, para 34 but note comments of Lord Collins of Mapesbury as to the potentially chilling effect of such police behaviour, para 97.

monitoring[103] - because of this particular pervasive and on-going characteristic - itself engages Article 8 ECHR and Article 7 of the Charter.

Justification

Both the Charter and the ECHR permit the justification of an intrusion into privacy/data protection rights provided certain requirements are met. As far as the ECHR is concerned, Article 8(2) specifies three stages. The interference must be based in law, for a legitimate aim and 'necessary in a democratic society'. For the Charter, Article 52(1) constitutes an analogous provision. While its requirements may be similar, its terminology is different.[104] Any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and must respect the essence of those rights and freedoms. Further, limitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.[105] Finally, any restriction should apply only insofar as is strictly necessary.[106] The exception should not turn into the rule. While these tests are well-established in the courts' respective jurisprudence, the framework is not always clearly applied in a structured manner. Nonetheless, the cases to date are sufficiently clear to raise questions about the acceptability about the current ANPR framework as regards acquisition of data (the categories of person whose data is acquired), access to the data and data retention.

'based in law'

Article 8(2) ECHR requires that an interference be 'in accordance with the law', which is different from the text used in relation to other Convention rights where an interference must be 'prescribed by law'. While this difference could suggest that mere compliance with general norms (such as DPA, PoFA) might suffice, in practice the difference in wording between Article 8(2) and Article 10(2) has been described as 'irrelevant'.[107] Even if the ECtHR is flexible as to the form the law must take,[108] the qualitative requirements (discussed below) mean that the requirement here is more than 'not illegal'. Furthermore, this textual difference is not found in the text of Articles 7 and 8 of the Charter. Article 52(1) of the Charter specifies that exceptions 'must be provided for by law …'. It is an open question whether the form of

[103] In *Vukota-Bojic* v. *Switzerland* (App no. 61838/10), judgment 18 October 2016, which concerned the monitoring of the individual's activities in public, as well as the taking of photographs of those activities, the Court stated 'the applicant was systematically and intentionally watched and filmed by professionals' para 58 which indicates that there were two aspects in issue: the watching (no record) and the filming (record) – but both in a systematic context. Again, a 'reasonable expectation of privacy' was not the sole criterion.

[104] It is sometimes suggested that there are four elements: legitimacy; suitability; necessity; proportionality *strictu sensu*. See e,g L. Feiler, 'The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection' (2010) 1(3) *European Journal of Law and Technology* [Internet Publication] section 7.3

[105] *Tele 2/Watson*, n.1, para 94; *Digital Rights Ireland* n. 77, paras 46-7; more generally see e.g. Feiler, n. 104

[106] *Tele 2/Watson* n. 1, para 96 and cases cited

[107] S. Sottiaux *Terrorism and the Limitation of Rights* (Oxford: Hart Publishing, 2008) p. 298

[108] *Malone* v *UK* (App no. 8691/79) [1984] ECHR 10, para 66, reiterated in *Zakharov*, n. 1, para 228

law required should be legislative in form,[109] rather than common law based as English courts have emphasised[110] had been accepted previously - at least by the ECtHR.[111]

The ECtHR has set down qualitative requirements in respect of any such law: accessible; sufficiently clear as to be circumstances under which interference may be justified; and consistent with the rule of law. Situations where the law is confused are problematic.[112] It specified in *Zakharov*:

> The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse.[113]

In numerous surveillance cases, the ECtHR has focussed on this element, rather than considering the proportionality of the measure, perhaps because of the sensitivity of the area.[114] Further, as can be seen in the quotation from *Zakharov*,[115] there are links, perhaps overlap, between the requirement of lawfulness and 'necessary in a democratic society'.[116] Somewhat unusually, the ECtHR has introduced substantive procedural elements into the test for foreseeability/accessibility. While some have criticised this approach for blurring the boundaries between Article 8 and the right to a remedy,[117] this remains a consistent part of the ECtHR's approach in this area. Such procedural elements constrain State action and also allow individuals to understand at a general level when they might bring themselves within the scope of such measures (and to act accordingly[118]).

There must be clear, detailed rules specifying the conditions subject to which interferences are legitimate.[119] The minimum safeguards as regards interception of phone calls[120] are: the nature of the offences which may give rise to the intrusion; a definition of the categories of people liable to be affected; a limit on the duration of telephone tapping; 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 recordings may or must be erased or the tapes destroyed. While rules can be set down in secondary legislation and

---

[109] *Weber & Saravia v. Germany* (App no. 54934/00), judgment 29 June 2006, (2008) 46 EHRR SE5, [2006] ECHR 1173, para 90; *Khan* v. *UK* (App no. 35394/97) ECHR 2000‑V; Emmerson, n.2, para 7-28; c.f *Murray* v *UK* (1995) 19 EHRR 193

[110] *Wood* n. 51

[111] *Huvig* v France (1990) 12 EHRR 528; *Kruslin* v *France* (1990) 12 EHRR 547; *Murray* n. 109*;* c.f. *Hewitt and Harman* v. *UK* (Comm. Dec) (1992) 14 EHRR 657; for criticism of this position see P. de Hert, 'Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11' (2005) 1 *Utrecht Law Journal* 68, p. 78

[112] *Khan* v. *UK* n. 109, para 27; *Vukota-Bojic* n. 103, paras 71-73

[113] *Zakharov*, n.1, para 236, and see para 230 on safeguards against abuse

[114] M. H. Murphy 'A Shift in the Approach of the European Court of Human Rights in Surveillance Cases: a rejuvenation of necessity?' (2014) 5 EHRLR 507, pp.510-11

[115] *Zakharov*, n.1; also *Kennedy* v. *UK* (2001) 52 EHRR 4, para 155

[116] E.g *Kvasnica* v *Slovakia* (App no. 72094/01), judgment 9 June 2009, para 84

[117] I. Cameron, *National Security and the European Convention on Human Rights* (The Hague: Kluwer Law International, 2000) p. 34

[118] *Sunday Times* v *UK* (Application no. 6538/74), judgment 26 April 1979, [1979] ECHR 1

[119] *Weber and Saravia*, n. 109

[120] *Weber and Saravia* n. 109, para 95; *Zakharov* n. 1, para 231

codes,[121] any such documents must be publicly available[122] and legally binding.[123] In principle, the same points about lawfulness will arise in relation to the Charter. Here, however, while the Opinion of the Advocate General in *Watson/Tele2* suggested that any such laws or codes must be binding on the relevant authorities,[124] the judgment did not pick up this issue. As noted[125], however, the Charter must provide at least the protection of the ECHR, which supports the position of the Advocate General.[126]

This requirement of lawfulness gives rise to problems for the ANPR regime. The assertion in the Home Office Document that '[t]he DPA and RIPA provide the framework to support Article 8 ECHR'[127] is at best questionable. The DPA, as we have noted, safeguards how data is processed but does not provide a legal base; it does not authorise or require the acquisition of data through this type of activity. It does not fulfil all the functions the ECtHR has ascribed to 'law', specifically it gives no indication of when and to whom intrusive measures might apply. So while it might provide some safeguards against abuse, on its own it is not enough. A similar point could be made about PoFA. Further, there are no sanctions for non-compliance with the PoFA code. Any common law basis for police action is very broad and vague, probably beyond acceptable limits for allowing individuals to predict its application.

RIPA remains as a possible legal base but there are two difficulties with seeking to ground ANPR in it. The first is that ANPR does not fit clearly into the categories of surveillance[128] that are regulated by RIPA Part II. Part II covers covert surveillance - that is, surveillance carried out in a manner to ensure that persons who are subject to the surveillance are unaware that it is taking place.[129] While some specific operations with ANPR cameras located in unmarked cars might satisfy this test, it is much less likely that static cameras do so. Even if the police are unwilling to publicise locations, the cameras are potentially visible to the road user, even if – as street furniture – they are part of the background and thus practically invisible. The PoFA Code describes ANPR, moreover, as overt surveillance. It has been questioned whether the definition of covert surveillance works in the context of mass surveillance, where individuals may be aware that the techniques exist – and so do not satisfy a strict view of RIPA – but are unaware that the techniques are being used in their respective instances.[130] In any event, to fall within RIPA, covert surveillance must be one of the following: directed surveillance; intrusive surveillance; or the use of CHIS, the last of which is clearly not relevant here. ANPR does not fit these categories. Directed surveillance is for the purposes of a specific investigation, rather than general monitoring; intrusive surveillance relates to activities taking place on residential premises[131] or in any private vehicle. It would be an expansive view of this latter element that might cover ANPR, especially as the use of trackers has been expressly excluded. The second aspect is that surveillance can be carried out even in the absence of

[121] *Kennedy* n. 115
[122] *Liberty* v. UK (App no. 58243/00), judgment 1 July2008, (2009) 48 EHRR 1; *Zakharov*, n. 1, para 241,
[123] In *S and Marper*, n. 80, the Court noted that the rules were non-statutory guidelines, but discussed proportionality rather than deciding the case on legality
[124] *Tele 2/Watson* n. 1, opinion para 150
[125] See n. 46
[126] See S. Peers and S. Prechal 'Article 52' in Peers et al (eds) *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing: Oxford, 2014), para 52.42
[127] Home Office, *The Use of ANPR by Law Enforcement Agencies: Lawful Interference with the European Convention on Human* Rights, December 2014, para 1.4
[128] Surveillance is defined at s. 48(2) RIPA
[129] Section 26(9)(a) RIPA
[130] Mackay n. 2
[131] Note the Article 8 ECHR covers business premises

authorization under Part II.[132] The regime has been criticised in this regard,[133] being described as 'no more than a voluntary code'.[134] This is a weakness indeed when we consider the requirement of lawfulness, especially as regards the binding nature of the law. As noted above, the IPA only partially covers use of ANPR data; it would not constitute relevant 'law' in this context.

It has been suggested[135] that the Criminal Procedures and Investigations Act 1996 (CPIA) justifies the retention of data. This argument is weak. The CPIA was introduced to allow the review of evidence after trial so as to avoid miscarriages of justice. It does not deal with creation, storage or access and cannot relate to individuals not of interest to the police. Furthermore, this obligation to retain evidence has not been found to be sufficient justification for retention of data in other contexts (communications data, biometric data)[136] and concerns have been expressed about using CPIA justifying keeping biometric data on a 'just in case basis'.[137] The Anti-Social behaviour, Crime and Policing Act 2014 clarified that, once CPIA no longer applies, the sample must be destroyed, and it must not be used other than for the purposes of proceedings for the offence in connection with which it was taken.[138] It therefore undermines the possibility of relying on CPIA as a general justification for retention of data.

There may also be problems about clarity of the regime. Insofar as it is possible to rely on the statutory framework, it consists of overlapping systems with different enforcement mechanisms. This is potentially confusing. In all, any framework is undermined by the lack of coherence of piecemeal legislative responses, arguably with different rationales.[139] Further, the fact that there is no authorisation regime setting down conditions of access and use makes it difficult for individuals to foresee the applicability of the regime, even if the bulk collection of ANPR data is acceptable at a level of principle. There are insufficient specific safeguards – as suggested by *Weber & Saravia* and subsequent cases- to prevent arbitrary behaviour.[140] The ANPR system would seem to fail on these rule-of-law criteria.

'legitimate aim'

This aspect raises few problems. The European courts seem unwilling to challenge States' claims,[141] sometimes inferring the legitimate purposes on behalf of governments.[142] Here, the data is used for the fight against crime. The investigation of crime is a legitimate public interest

[132] Walker, n. 16, para 2.64
[133] Akdeniz, Taylor and Walker 'Regulation of Investigatory Powers Act 2000' [2001] Crim LR 73
[134] McKay, n. 2, para 1.37
[135] Freedom of Information Act Request: 'Automatic Number Plate Recognition (ANPR) governance arrangements, board papers', available at: https://www.whatdotheyknow.com/request/289438/response/730763/attach/html/15/18%2019%20Email%20ICO%20to%20ANPR%2023042015%201714.pdf.html, accessed 8th February 2017
[136] Hansard, 10 October 2011, Column 104
[137] Commissioner for the Retention and Use of Biometric Material, Annual Report 2014, November 2014, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387573/BiometricsAnnualReport201314Print.pdf, accessed 8th February 2017, pp 59 et seq
[138] Explanatory Notes to Anti-Social Behaviour, Crime and Policing Act 2014, para 62
[139] Parsons et al 'ANPR: Code and Rhetorics of Compliance' (2012) 3 *European Journal of Law and Technology* (online publication)
[140] Contrast codes on interception of communications in Kennedy n. 121 and *R.E* v *UK* (App no. 62498/11), judgment 27 October 2015 where codes had not yet come into force
[141] *Hewitt and Harman* v. *UK* (No. 2) (App. no. 20317/92), dec. 1 September 1993
[142] E.g. *Surikov* v. *Ukraine* (App no. 42788/06), judgment 26 January 2017, para 82

in both EU[143] and ECHR systems, although the multiplicity of possible uses for the ANPR data may give rise to concerns about 'purpose creep', where data obtained for one purpose is used for another. The nature of the public interest is also a relevant factor for assessing proportionality, and the distinction between crime and serious crime may be significant in that context. Further, the scope of activities that could fall within the prohibited behaviour must be sufficiently clear to satisfy the foreseeability requirement.[144] While the definition of offences is in principle a matter for States, it is also possible that the Court of Justice might start filling in the meaning of 'serious crime': a reference on the meaning of 'serious crime' has been made, albeit in a different context.[145]

'necessary in a democratic society'

'Necessary in a democratic society' for the ECtHR means that the interference meets a "pressing social need" but also that it is proportionate to the aim pursued.[146] It is not found in the Charter or its jurisprudence. While not meaning 'indispensable', necessity expects more than 'useful', 'reasonable' or 'desirable'.[147] Further, the reasons adduced to justify the measures must be 'relevant and sufficient.[148] The level of review takes into account all the circumstances, and the intensity of review may vary. The ECtHR has been deferential to State concerns about national security, but measures such as powers of surveillance are more closely scrutinised.[149] Given the importance of data protection for the effective exercise of privacy rights, the margin of appreciation is limited in this context too.[150] Another aspect is whether the measure is appropriate for achieving the aim, a question which goes beyond just a logical connection. There must be some degree of success or effectiveness,[151] although it is debateable the extent to which any such effectiveness has been required to be clearly evidenced.[152] A proportionality assessment may also return to some of the issues relevant for the lawfulness assessment. While some commentators have been critical of the ECtHR's approach,[153] especially its earlier jurisprudence, more recent case law in this area shows a greater willingness on the part of the ECtHR to engage with a proportionality assessment.[154]

The Court of Justice will consider whether the essence of the right has been destroyed and whether an instance of interference is proportionate. While the essence test may show another formal distinction between the tests applied by the two courts,[155] it is a high barrier to cross and the Court of Justice has not often found this test satisfied even in some cases involving mass surveillance.[156] An infringement was found in *Schrems*, however, in relation to the content of communications.[157] In terms of proportionality, there are similarities to the approach

[143] *Digital Rights Ireland Ltd* n. 77, para 41
[144] E.g *Zakharov*, n. 1, para 247
[145] Case C-207/16 *Ministerio Fiscal*, pending
[146] *Handyside* v *UK* (App no 5493/72), judgment 7 December 1976, (1976) 1 EHRR 737, [1976] ECHR 5, paras 48-49
[147] *Handyside*, n. 146, para 48
[148] *Peck* n. 51, para 76
[149] *Klass* v *Germany* (App. no. 5029/71), judgment 6 September 1978, para 42
[150] *Surikov* n. 142
[151] In *S and Marper*, n. 80, the Court referred to the need for the justifications to be relevant and sufficient
[152] Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci (A/HRC/31/64), 8 March 2016, para 11
[153] P. de Hert, n. 111, p. 80
[154] See e.g *Zakharov* n. 1; *Surikov* n. 142; Murphy 'A shift in approach', n. 114, pp. 414 *et seq*
[155] A third difference might be the 'margin of appreciation': see Peers, n. 126, paras 52.68- 52.69
[156] See e.g. *Digital Rights Ireland* n. 77 paras 39-40
[157] *Schrems*, n.1

taken by the ECtHR. Any room for national discretion was in this context limited. In reaching this conclusion, the Court of Justice emphasised the importance of data protection to ensuring respect for private life,[158] impliedly reflecting early concerns about the power of the state being enhanced by databases. Since *Digital Rights Ireland*, the Court of Justice has been willing to engage in extensive analysis of the proportionality of State measures in the context of national security and the fight against terrorism considering critically both the idea of 'necessity' and the level of safeguards provided by the system; the issue of appropriateness has received less attention.

In the context of ANPR, the case law of both European courts on mass surveillance[159] are relevant. ANPR collects and retains the data of all vehicles, which can be linked back to individuals, whether or not those vehicles are wanted in connection with a particular offence. The system is therefore indiscriminate, rather than suspicion-based. Such a system requires particularly strong justification (especially with the retention of data for increasingly long periods) given both European courts have been critical of systems of mass surveillance in the context of communications.[160] As noted, it may be that GPS and passenger name records in relation to international flights are less intrusive than communications surveillance, but this does not mean that such intrusions have no weight[161] especially where a detailed individual picture may be generated.[162] While data retention and data mining may be appropriate, perhaps identifying persons of interest hitherto unknown, problems arise when considering necessity/proportionality. Of particular concern is the fact that the data collected and retained is 'general and indiscriminate', so that in the view of the Court of Justice, even a relatively serious objective (the fight against serious crime and terrorism) could not be justified. While some note that it may be possible always to find some examples of cases that have needed retained data to solve them,[163] the Court of Justice has side-stepped this type of argument. In an indiscriminate system, there is no link between the data retention and the threat posed by a specific individual and, in its view, therefore goes beyond what is 'strictly necessary'.[164] While bulk powers may be acceptable where they distinguish quite finely between categories of people (or perhaps activities), blanket bulk powers are not.[165] Even where bulk powers might be acceptable, stringent safeguards to prevent abuse would be of central importance in determining whether such powers were proportionate.

The position appears less emphatic in the jurisprudence of the ECtHR. In the chamber decision in *Szabó*,[166] the ECtHR appeared to accept that mass acquisition of data may be necessary for the fight against terrorism, but on the facts in issue there were inadequate safeguards. A concurring opinion, however, expressed a strong view that the Grand Chamber in *Zakharov* imposed a requirement for a more specific level of suspicion even in the context of serious

[158] *Digital Rights Ireland* n. 77, para 48; also *Tele2/Watson* n. 1, para 83

[159] 'Mass surveillance' is not a term derived from law and its precise boundaries have been the subject of much discussion: see European Commission for Democracy through Law (Venice Commission) (2015), p 12; Fundamental Rights Agency, Surveillance by intelligence Services: fundamental rights safeguards and remedies in the EU, 2015, p. 17

[160] *Digital Rights Ireland* n. 77, *Tele 2/Watson*, n. 1; *Zakharov*, n. 1

[161] *Vukota-Bojic*, n. 103, para 76.

[162] Parsons, n. 139

[163] Feiler, n. 104, at 7.3.3

[164] *DRI* n. 77, para 56; *Tele 2/Watson* n. 1, paras 96, 105

[165] *Tele2/Watson*, n. 1

[166] *Szabó*, n. 1

crime.[167] Previous cases, for example *S and Marper*[168], took a similarly strong line against blanket and indiscriminate State acts. If indiscriminate acquisition of data remains in principle possible, the safeguards are of central importance to proving that the resulting intrusion is necessary in a democratic society.

The general retention of ANPR data may be disproportionate in the light of both courts' jurisprudence. ANPR affects all road users in England indiscriminately. Further, the objectives for which ANPR data is used cover a wide range and, crucially, include low-level offences (e.g. untaxed or uninsured cars) suggesting that even if location data is less intrusive than communications data, the justification for intrusion is less strong. There is little evidence that the acquisition or retention of this data is 'strictly necessary', rather than 'useful', insofar as it is effective at all.[169] There is no discrimination in the system between retention of data relating to those of interest to the police, nor of distinguishing between offences of different levels of seriousness.

It is open to question whether the decision to install ANPR cameras and the choice of location/intensity are activities requiring justification. Such choices are clearly caught in the context of locational privacy; less obviously so in relation to an analysis based on systemic storage of data. It may, however, be difficult or artificial to distinguish between acquisition/monitoring and storage where the acquisition method is the creation of a photographic record.[170] Certainly, the PoFA Code suggests that any 'decision to use any surveillance camera technology must, therefore, be consistent with a legitimate aim and a pressing need' and designed to meet the stated purpose and deployed only for the necessary time; essentially a proportionality analysis.[171] The phraseology – especially the word 'use' – blurs the issue of acquisition and storage whilst making it clear that 'use' needs to be justified. While PoFA may suggest useful constraints on ANPR use, it cannot be seen as an adequate safeguard in human rights terms because it is not binding. Additionally, PoFA also does not directly consider location. The Information Commissioner's Code on CCTV, which is binding, suggests that data controllers consider whether the location for CCTV cameras is appropriate for purpose and does not intrude on private property. It does not directly address the locational privacy concerns arising from accumulation of data and an intensity of cameras. The Information Commission has taken action against the use of ANPR, notably against the Royston 'ring of steel'.[172] While demonstrating that ex post enforcement mechanisms exist,[173] the Data Protection Act in terms of ex ante safeguards requires internal review only. The installation of ANPR cameras can in this context be contrasted with the collection of communications data. There, although the collection of data is potentially widespread, it must be triggered by a notice to the telecommunications operator. ANPR is distinctive in having no link to governmental or external oversight at this stage. It is questionable whether this is sufficient.

---

[167] *Szabó* n. 1, para 20

[168] *S and Marper,* n. 80

[169] Big Brother Watch noted that the levels of crime in Royston did not increase after the dismantling of the 'ring of steel', see https://www.bigbrotherwatch.org.uk/2014/08/loss-roystons-ring-steel-hasnt-caused-crime-wave/, accessed 27th February 2017

[170] Laws in *Wood*, n. 51

[171] PoFA Code, n. 8, para 2.4.

[172] See n. 97

[173] The text of the notice, 24th July 2013, no longer seems to be available. Press reports state that the ICO found the collection of the information to be unlawful, breaching principle 1 of the Data Protection Act, and excessive, breaching principle 3

The *Tele2/Watson* case considered the adequacy of safeguards around access to data and examination of the data. In this there are similarities with the ECtHR's approach. Indeed, that court recently noted "a certain level of consensus" about the level of safeguards, based on acceptance of data protection principles.[174] Again objective criteria must be established which limit access, and following *Tele2/Watson*, access to a person's data should be granted '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'[175], with further access to people indirectly connected to such activities being allowed in exceptional circumstances (such as terrorist activities).

It is questionable whether the handling arrangements currently in place for access to and analysis of the ANPR data are adequate despite the data protection and PoFA codes. The Information Commissioner's code states that use of ANPR must be justified. Further, databases must be kept up-to-date and accurate (in particular to prevent mismatches). Data must be kept secure and retention periods must be the minimum necessary for the purpose for which the data was collected and immediately thereafter be deleted. These requirements provide some safeguards but, by comparison with the requirements from the surveillance jurisprudence, lack specificity and allow too much room for manoeuvre on the part of the processor. Moreover, retention periods determined by reference to a purpose are problematic in terms of bulk acquisition and retention of data. The access arrangements for communications data under the Data Retention and Investigatory Powers Act 2014 (DRIPA) were challenged in *Tele2/Watson*. The Court of Justice required independent supervision of access; indeed, it suggested that such independence would be found through prior authorisation by a judge or other independent body, where a request for access is made on the basis of a 'reasoned request'[176]. Such independent supervision is a safeguard against fishing expeditions, in that such a system could ensure that there was some form of justification for investigating a particular car/owner prior to that investigation taking place. Note that *Tele2/Watson* concerns a system that requires sign-off by a senior officer but involves the "Single Point of Contact", an officer separate from an active investigation, trained in surveillance and matters pertaining to human rights. The ANPR system has no equivalent level of protections, so is more vulnerable to challenge on this issue.

Finally, data must be deleted in a timely manner, in accordance with any internal rules or data handling codes. This seems not always to have been the case, at last as regards the Met. Case law makes clear that there are limits on how long any data can be retained. The nature of the offences sought to be prosecuted and the nature of the data affect the permissible retention period, as does the nature of the data held. Both the Data Retention Directive – which permitted two years' retention – and DRIPA which specified one year – were seen as problematic in terms of period of retention. The concern arises partly from the undifferentiated nature of the retention; it is one thing to retain data on suspicion or in relation to a prosecution, it is another thing entirely in relation to a person of no interest to the police. This is the trap into which ANPR falls. Even if a two year period in relation to terrorism or other serious offences is acceptable, which is dubious in the light of recent case law, the not very serious nature of some of the offences for which ANPR is used may weigh against such long retention. An extension

[174] *Surikov* n. 142, para 74
[175] *Tele2/Watson*, n. 1
[176] *Tele2/Watson*, n. 1, para 120.

would make any justification still harder; indeed the ICO has raised this point, questioning whether the operational case for such an extension has convincingly been made.[177]

Conclusion

This paper has argued that the ANPR system constitutes an intrusion into the private lives of road users based on both the ECHR and EU Charter. By contrast, English case law has not consistently recognised the concerns around privacy in a public space. ANPR has not been considered directly. Data retention triggers the application of the right to private life whether seen in Charter or Convention terms and must therefore be justified in accordance with the ECHR and the Charter. Beyond this is the question of locational privacy, the importance of which has not yet been directly addressed by any of the courts. It has been argued that if we look to the concerns that the courts have highlighted, then locational privacy should be protected. Even focussing just on systemic retention of ANPR data, the system needs to be justified. Here the ANPR regime runs into multiple problems: the inadequate basis in law; the bulk nature of the data retained; the lack of safeguards against abuse; and the disproportionate extent of the retention period. In short, the regime is fundamentally defective. It would seem far better to set up a legislative regime, with appropriate safeguards and oversight mechanism, rather than to allow the current system to continue – though bulk acquisition of ANPR data may remain problematic in the light of jurisprudence on blanket data gathering. Not only is the current position undesirable from the perspective of the road-user but the police use of ANPR data is exposed to legal challenge with potentially far-reaching consequences. Given that it is not just ANPR which may give rise to these issues, a broader review should be undertaken. All police surveillance in public space should be considered – such as that relating to the use of drones and BWV – to produce a coherent and appropriately calibrated system rather than one which is once again reactive, piecemeal and possibly still incomplete.

[177] Letter from ICO to Paul Kennedy (Chair, ANPR Users Group), dated 30 June 2015 on What Do They Know available at: https://www.whatdotheyknow.com/request/289438/response/730763/attach/10/10%20Letter%20ICO%20to%20ANPR%20Portfolio%2030602015.pdf, accessed 9th February 2017