Private Actor or Public Authority? How the Status of Communications Service Providers affects Human Rights

By Allison M Holmes*

Abstract

Communications data retention, regarding the who, where, how and when of internet and mobile telephony communications, is a law enforcement tool which has recently been at the forefront of public debate in the United Kingdom. This data is collected and retained by the private sector, specifically Communications Service Providers (CSPs), and is later accessed by relevant law enforcement agencies. Such a system of retention effectively imposes the role and duties of a public authority on a private company. These companies act as intermediaries who operate enforcement mechanisms via the network infrastructure. Despite this, CSPs are treated as private actors in the relevant statutes. This impacts directly on human rights, particularly privacy, as private actors are turned into the instruments of privacy intrusions. The private status of CSPs limits the protections guaranteed to individuals, given that the provisions of the Human Rights Act 1998 provide for the conduct of public authorities but, in general, do not apply to private companies. Private companies which exercise functions of a public nature however, may fall under the remit of the HRA. It is argued that the communications data retention regime, particularly following the passage of the Counter-Terrorism and Security Act 2015 which placed additional obligations on CSPs, and the powers under the Investigatory Powers Act, have, by implication, altered their status, making them 'functional public authorities'. Following on from that, it is contended this regime offers insufficient protections; the human rights of individuals affected by the retention policies and practice would be better served by clarifying relevant legislation to ensure that CSPs are performing functions of a public nature when complying with statutory retention requirements.

Introduction

Communications data retention, regarding the who, where, how and when of internet and mobile telephony communications is an effective and accepted law enforcement tool which has recently been at the forefront of public debate in the United Kingdom. The communications data broadly

falls into three categories encompassing subscriber data,[1] service data,[2] and traffic data,[3] and can be broadly characterized as data which pertains to the context of what is said but not the content of the communication itself. This data plays a key role in current law enforcement and national security operations. Indeed, in 2014 a study found that 'communications data has played a significant role in every Security Service counter-terrorism operation over the last decade and has been used as evidence in 95% of all serious organized crime cases handled by the Crown Prosecution Service'.[4] The data offers significant benefits for those involved in the detection and investigation of crime. It is relied upon to provide both inculpatory and exculpatory evidence, reveal a suspect's movements, reveal links between suspects, enable the discovery of other key offenders, determine the last known whereabouts of victims, highlight inconsistencies in accounts by suspects, and corroborate the testimony of victims.[5]

Communications data is collected and retained by the private sector, specifically, communications service providers (CSPs),[6] for later access by approved public authorities. CSPs are companies which run public telecommunications services for both internet and telephone communications. The definition of CSPs is broad, and potentially includes companies such as Virgin and BT which are primary providers of broadband and telecom services and companies like Google or Yahoo which facilitate e-mail communications. It may further be extended to websites and applications which are not traditional communications suppliers, but which provide

*Kent Law School, University of Kent, Canterbury, CT2 7NZ. Special thanks to Professor Dermot P Walsh MRIA and Dr. Sinéad Ring for reviewing a draft of this article and to the anonymous reviewer for their comments.

[1] This is information held or obtained by a CSP in relation to a customer, including their name, address, and telephone number.

[2] This consists of the use made by any person of a CSP and for how long, for example, an itemized phone record showing the date, time, and duration of calls and to what number each was made.

[3] Traffic data is data comprised in or attached to a communication by means of which it is being or may be transmitted, e.g. who the user contacted and at what time, the location of the person contacted, and the location of the users.

[4] Regulation of Investigatory Powers Act Consultation: Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice (2014). Noted in this are several examples of cases where this information was used. This included: Operation Frant where telephone evidence of cell site data and call logs revealed participants of a drug ring binging high grade heroin into London; Operation Backfill where internet data was used to identify perpetrators of armed robberies; and Operation Notarise which led to the arrest of over 600 suspected paedophiles. See also: Anderson, D A Question of Trust (Independent Reviewer of Terrorism Legislation June 2015) Annex 10 339-341.

[5] May, Report of the Interception of Communications Commissioner March 2015 (HC1113, 2015) para 7.65.

[6] For the purposes of this paper, CSPs will be defined as providers of a public telecommunication system, where that system exists for facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy (Investigatory Powers Bill 2016 s 233(2)). This includes where the service participates in the management or storage of communications transmitted or that may be transmitted.

communications over the top of these services which might be caught under this definition, such as Facebook and Whatsapp. CSPs are the dominant instruments through which all communications now occur; it is essentially impossible to communicate electronically without utilizing one of these services.[7] The prevalence of mobile telephones and the internet has resulted in an expansive increase in the amount of data generated by even the most innocuous of transactions. This data is far more encompassing and revealing than that derived from traditional communications systems.[8] For example, '[t]he frequency and times of communications reveal the strength and type of people's relations. The number of people two parties know in common is an indication of the social cohesion of their groups. The co-locations of mobile devices at day or night is an indicator of friendship or intimate relations'.[9] The scale and scope of communications data ensures it can provide a comprehensive account of a large portion of a person's life.[10] Further, the common roles associated with CSPs have been altered. Traditionally, these companies were seen as intermediaries, merely connecting two parties. Whilst this remains a key function, their role has expanded. CSPs provide not only communications, but also opportunities for social interaction, research, purchases, education, and so on. This growth in personal data retention has not been accompanied by concurrent developments in the law which address the privacy issues posed by the enhanced data capture.

At issue herein is the collection and retention of this communications data by CSPs for future use and access by law enforcement agencies. While both retention and access have implications for human rights, it is the former only which will be the focus in this paper, as collection and retention present distinct concerns for CSPs which have not been adequately addressed by legislation. In this context, retention is the storing of all communications and transactions for a set period, which is longer than would typically be used for billing and engineering purposes,[11] to facilitate future access for public authorities. The retention requirements placed on CSPs

[7] As of 2016, 89% of households in Great Britain had internet access. 71% of adults in the UK use smart phones and 70% of adults use internet 'on-the 'go'. See: Prescott C, 'Internet access - households and individuals: 2016' (Office of National Statistics 2016).
[8] See for example the ability of location data to track an accurate picture of your movements in: 'Tell-All Telephone' Die Zeit (Zeit Online 31 Aug 2009 2009). There is no historical equivalent to this other than targeted surveillance.
[9] LSE Policy Engagement Network, Briefing on the Interception Modernisation Programme (London School of Economics and Political Science, 2009).
[10] This was acknowledged by the CJEU in the AG opinion Cruz Villalon in the case of Digital Rights Ireland Case C-293/12 (2013) ECLI-845.
[11] Whitley E and Hosein I, 'Policy discourse and data retention: The technology politics of surveillance in the United Kingdom' (2005) 29 Telecom P 857.

under the relevant instruments require data to be kept on all service users, installing a blanket measure which occurs irrespective of individual suspicion or judicial authorization. Whilst the value of this data for law enforcement is clear, its value to the CSPs is negligible. Despite the clear value to the public interest, the retention of communications data is not treated as a public function. In discharging these functions, CSPs are regarded as private actors in the relevant statutes. This impacts directly on human rights, particularly privacy, [12] as private actors are turned into instruments of privacy intrusions without the subsequent protections offered under the Human Rights Act. It is argued that this interpretation of CSPs as private actors is incorrect. This paper will examine the status of CSPs in the retention of communications data with the aim of demonstrating how those functions can be interpreted as 'functions of a public nature' thereby placing the CSPs within the scope of the Human Rights Act 1998.

Functions of a Public Nature

The Human Rights Act 1998 (HRA) was intended to 'bring rights home' to the public, making the rights set out in the European Convention on Human Rights (ECHR) enforceable in a direct and readily accessible manner.[13] In doing so, the HRA rooted the provisions of the ECHR in domestic statute, thereby providing individuals with effective remedies in UK courts for a breach of their Convention rights. However, the HRA does not provide for blanket protection for all interferences with human rights. It is restricted primarily to breaches which occur consequent on the actions of 'public authorities'. Specifically, Section 6 HRA states that '[i]t is unlawful for a public authority to act in a way which is incompatible with a convention right'. Critically, Section 6(3)(b) provides that a 'public authority' can include 'any person certain of whose functions are functions of a public nature', and section (6)(5) notes that, 'in relation to a particular act, a person is not a public authority by virtue of only subsection 3(b) if the nature of the act is private'. Taken together, these two subsections provide that any person or body whose functions are of a public nature will be a public authority, other than in relation to those

[12] Mere retention has been held to be a violation of Article 8. See Weber & Saravia v Germany App no 54394/00 (ECHR 29 June 2006); Liberty & Ors v GCHQ & Ors 2014 UKIPTrib 13_77-H 5 Dec 2014; Digital Rights Ireland ibid.

[13] See Bamforth N 'The true "horizontal effect" of the Human Rights Act 1998' (2001) LQR 34; Miles J 'Standing under the Human Rights Act 1998: theories of rights enforcement and the nature of public law adjudication' (2000) CLJUK 133; Bamforth 'The application of the Human Rights Act 1998 to public authorities and private bodies' (1999) CLJUK 159.

particular acts which are of a private nature. These provisions allow for the requirements of the HRA to be enforced against private bodies in cases where they are performing 'functions of a public nature'.[14] For the purposes of this article, these bodies will be referred to as 'functional public authorities'.

While the expanded definition of a public authority extends the scope of the HRA, the statute is unclear as to what precisely is meant by 'functions of a public nature'. It is therefore important to define this term to determine when the actions of a private body are covered by the provision.

i. Parliamentary Interpretation

During the debates preceding the passage of the HRA 1998, both Houses of Parliament discussed specifically what the provisions under section 6 were designed to capture. The general proposal was that the definition of public authority should have a broad scope. 'In the course of parliamentary debates on the passage of the Human Rights Act, it was clear that private bodies delivering privatized or contracted-out public services were intended to be included within the scope of the Act through the 'public functions' concept'.[15] In the White Paper on the Human Rights Bill, the definition of a public authority was stated in wide terms:

> Examples of persons or organizations whose acts or omissions it is intended should be able to be challenged include central government (including executive agencies); local government; the police; immigration officers; prisons; courts and tribunals themselves; and, to the extent that they are exercising public functions, companies responsible for areas of activity which were previously within the public sector, such as privatized utilities.[16]

This view was supported by the Lord Chancellor (Lord Irvine of Lairg) in his statement on the Bill wherein he noted that '[c]lause 6 is designed to apply not only to obvious public authorities such as government departments and the police, but also to bodies which are public in certain respects but not others. Organizations of this kind will be liable under Clause 6 of the Bill for

[14] For further discussion of 'functional public authorities' see: Quane, H 'The Strasbourg jurisprudence and the meaning of a "public authority" under the Human Rights Act' (2006) PL 106; Sunkin, M, 'Pushing forward the frontiers of human rights protection: the meaning of public authority under the Human Rights Act' [2004] PL 643; Oliver, D, 'The frontiers of the State: public authorities and public functions under the Human Rights Act' (2000) PL 476; and Oliver, D, 'Functions of a public nature under the Human Rights Act' (2004) PL 329.
[15] Palmer S, 'Public, Private, and the Human Rights Act 1998: An Ideological Divide' [2007] Cambridge L J 559, 562.
[16] Home Office, Rights Brought Home: The Human Rights Bill (White Paper, CM 3872, 1997) at para 2.2.

any of their acts, unless the act is of a private nature'.[17] Subsequent contributions to the Parliamentary debates also noted the importance of the broad classification of public authorities and denounced the idea of creating a definitive list of which types of private bodies exercising public functions would be caught by the provision. Indeed, they believed an exhaustive list of this sort would be unnecessarily limiting and ill-suited to adaptation over time. Instead, the favoured approach to determining what constituted 'functions of a public nature' was to leave the issue for the Courts to decide on a case-by-case basis:

> The drafters of the Bill have wisely included a broad, inclusive definition of what constitutes a public authority. They have done so because it is only possible on a case-by-case basis, looking at the particular body, the nature of the functions and the circumstances in which they are discharged, for the courts to come to a conclusion as to whether the activity falls on the side of a public function.[18]

As a result, the determination of what constitute 'functions of a public nature' for the purposes of the Act has been left to the Courts. However, as will be shown below, the Courts have failed to incorporate the broad interpretation advocated by Parliament.

ii. Judicial Interpretation

Several cases have considered the meaning of 'functions of a public nature' and attempted to determine whether a private company is caught by the provisions of section 6. The majority of these decisions relate to the provision of housing and care; however, the precedent set is instructive for defining functional public authorities.

The first case to deal with the term 'functions of a public nature' was Poplar Housing Regeneration Community Association Ltd v Donoghue.[19] In this case, the local authority was under a statutory duty to provide or secure the provision of housing for certain homeless people, a task which they delegated to Poplar, a private housing association. Poplar sought to evict a tenant they believed to be intentionally homeless; the tenant argued that such action was a breach of her Article 8 rights. In their submission, Poplar argued they were neither a standard public authority nor a body performing functions of a public nature and therefore their actions did not fall under the scope of the HRA. Lord Woolf CJ in the Court of Appeal identified three factors

[17] HL Deb 3 Nov 1997, Vol 582, Col 1227-1312.
[18] Ibid by Lord Lester of Herne Hill.
[19] (2001) 4 All ER 604

which would lead to the interpretation that a function is one of a public nature: statutory authority for the action; the extent of control over the function exercised by the public authority, and; a close relationship between the acts and the activities of a public body.[20] 'The more closely the acts that could be of a private nature are enmeshed in the activities of a public body the more likely they are to be public'.[21]

Close ties between the body and the public authority form the foundation of an institutional relational approach to defining 'functions of a public nature'. This approach emphasizes the institutional arrangements between the entities. In this case, Poplar was so closely assimilated to the local authority that it could not be said that is was performing a private function. This approach broadly classifies 'functions of a public nature' through an examination of the public body, its relationship with other bodies, both public and private, and its position in statutory arrangements.[22] However, the institutional approach is insufficient to explicitly define 'functions of a public nature'. It provides for a simplistic view of the issue, attaching significance to what the body 'is' rather than what the functions are. It limits the applicability of the provisions of section 6(3)(b) and is in direct contrast to the approach favoured by Parliament during Hansard wherein the Lord Chancellor stated that in the interpretation of 'functions of a public nature', 'the focus should be on their functions and not on their nature as an authority'.[23] Following the Poplar case, the Court retained elements of the institutional approach in their interpretation but expanded the test for 'functions of a public nature' to also assess the function of the body in line with the Parliamentary interpretation.

Specifically, the case of Parochial Church Council of the Parish of Aston Cantlow, etc. v Wallbank[24] confirmed elements of a functional approach to interpreting the status of a private body. Aston identified relevant factors that should be considered, mainly: the extent to which the function is publicly funded, whether the body is exercising statutory powers; and whether the

[20] Ibid at para 65.
[21] Oliver supra note 14 at 330.
[22] Oliver, supra note 14 at 481.
[23] Lord Chancellor, supra note 17; this line of reasoning is echoed in ECtHR judgment Costello Roberts v UK App No 13134/87 (1993) 19 EHRR 112.
[24] [2003] UKHL 37

body is taking the place of a central government or local authority in providing the function or is providing a public service.[25]

The case of Aston was followed by YL v Birmingham City Council[26] which remains the precedential foundation for the determination of 'functions of a public nature'. The House of Lords looked at three key areas in deciding the case. First, they assessed whether the private actor was profiting from the provision of the services delegated to it by the local authority. 'In particular, their Lordships believed that the performance of functions for commercial gain 'pointed against those functions being public'.[27] The motivation for the provision of services in this case was commercial, undertaken by a for-profit company; the fact that the profit came from the local authority rather than a private individual was insufficient to classify the actions as public. Second, the Court noted the contractual arrangement between the local authority and the care home. Lord Woolf in Poplar addressed the issue of contractual obligations, stating: '[a] public body in order to perform its public duties can use the services of a private body. Section 6 should not be applied so that if a private body provides such services, the nature of the functions is inevitably public'.[28] Finally, the Court noted the significance of any statutory or coercive powers the body possessed.[29] The existence of these powers would lend themselves to the assertion that the private body was performing functions of a public nature.[30]

The reasoning of the House of Lords in YL was subsequently interpreted and applied in the case of R (Weaver) v London and Quadrant Housing Trust.[31] This case concerned the provision of social housing by the Trust. The applicant alleged that the termination of his tenancy was a violation of his Convention rights under the HRA, which the Trust was obligated to respect by virtue of their status as a functional public authority. The Court agreed, identifying several

[25] Ibid at para 12.
[26] [2007] UKHL 27
[27] Williams A, 'Public authorities: what is a hybrid public authority under the HRA?' in David Hoffman (ed), The Impact of the UK Human Rights Act on Private Law, (Cambridge University Press 2011) 51.
[28] Poplar, supra note 19 para 58.
[29] These would include for example a private run prison or mental health facility where the subject was detained involuntarily.
[30] This was confirmed in the case of R (on the Application of A) v Partnerships in Care Ltd (2002) 1 WLR 2610 wherein a private mental hospital was found to be performing a function of a public nature because the hospital had coercive statutory power to detain the patient under the Mental Health Act 1983 and was under statutory duties under the Registered Homes Act 1984 to provide adequate staff and facilities.
[31] [2009] EWCA Civ 587; See also Barr & Ors v Biffa Waste Services Ltd (No 3) [2011] EWHC 1003 which similarly confirmed the principles of YL for defining a functional public authority.

factors relevant to defining the Trust's functions as public. First, there was a significant element of public subsidy for the provision of the housing by the Trust.[32] Second, the Trust was assisting the local authority in completing its statutory duties.[33] Third, the provision of subsidized housing was the opposite of a commercial activity and could only be described as governmental in nature.[34] Finally, the Trust was acting in the public interest in the provision of its service.[35] Therefore, it was held that the Trust was performing 'functions of a public nature' which must be compatible with the HRA.

The preceding discussion demonstrates the lack of clarity concerning the determination of functional public authorities for the purposes of the HRA. The reasoning and analysis underpinning the case law incorporate subjective elements in determining when a private body may be caught by the provisions. Broadly speaking however, there are a few consistent criteria which may be used to determine whether a private actor is a functional public authority. These include: the extent to which its action is publicly funded or subsidized; whether its actions are governed by statutory authority or contractual arrangements; whether the entity in question possesses any coercive powers over the individual; whether the body is acting in its own commercial interest; and whether there is a public interest in performing the function in question.

iii. Future Interpretation

The judicial interpretation of 'functions of a public nature' is criticized for being too narrow in its scope. In response, several proposals have been advanced to clarify the position of section 6(3)(b). The Joint Committee for Human Rights (JCHR) published reports on the Meaning of a Public Authority in 2003[36] and 2007[37] identifying key factors in the determination that a private body is a functional public authority. It suggested: the determination should be made without reference to the nature of the organization involved; the previous role of the Government in exercising the same function should be persuasive; there should be an element of public funding; the function should serve a public rather than commercial interest; and the focus should be on the

[32] Ibid at para 68.
[33] Ibid at para 69.
[34] Ibid at para 71.
[35] Ibid at para 71.
[36] Joint Committee on Human Rights, The Meaning of a Public Authority under the Human Rights Act, (2003-04, HL 39, HC 382).
[37] Joint Committee on Human Rights, The Meaning of a Public Authority under the Human Rights Act, (2006-07, HL 77, HC 410).

nature of the function being performed.[38] Following these reports, two Bills were proposed in 2008 and 2009 which sought to clarify the position, however, neither proceeded past the initial stages. Instead, Parliament has imposed explicit statutory provisions declaring that the private entities involved are performing functions of a public nature.[39]

Such a provision on the face of a relevant statutory measure brings clarity to the status of the body in question. In the absence of a general requirement to include such a provision, however, the issue will continue to be dealt with on a case by case basis. Certainly there is no explicit statutory provision clarifying the status of CSPs in the retention of communications data. It follows that the question of whether they qualify as 'functional public authorities' for the purposes of section 6 in this context will ultimately be a matter for the courts. In making that determination, the courts must pay close attention to the statutory provisions on data retention as they relate to CSPs and how these provisions relate to the factors identified in the established case law.

CSPs and 'functions of a public nature'

In determining whether CSPs perform 'functions of a public nature', it is useful to first establish the precise remit of their actions. The Data Retention and Investigatory Powers Act 2014 stipulates that CSPs, when placed under a notice by the Home Secretary,[40] are required to retain communications data, including that information linked to subscriber information (names, addresses, and identifying information of account holders), service use data (dates, times, durations, and end points of communications), and traffic data (locations of the user and recipient of communications). This information must be stored for a period of up to 12 months by the CSP, preferably in a database separate from those used by the CSP for business purposes, in order to facilitate access by law enforcement and national security aims.

The procedures requiring data retention for law enforcement and national security objectives must be distinguished from those which allow for retention for the business purposes of the company. Retention for these purposes is provided for the in the Data Protection Act (DPA) 1998 and the Privacy and Electronic Communication Regulations (PECR) 2003. These

[38] Ibid
[39] See Health and Social Care Act 2008 s 145.
[40] Data Retention and Investigatory Powers Act 2014 s 1.

instruments provide a traditional regulatory framework for the business operations of companies which collect and process personal data.

These instruments establish safeguards for the retention of data and provide that such data may only be retained when it satisfies specific requirements. Data may be retained only as long as necessary for business purposes and following that period it must be anonymized or deleted.[41] Similarly, the data can only be used for legitimate commercial reasons for which the company has received the users consent; any other use is in violation of the DPA and PECR and gives rise to liability.[42] The same is true for any unwarranted disclosure of data.[43] These instruments do not provide for a mandatory data retention regime; it remains at the discretion of the company to retain data subject to these limitations. It must also be noted that, under these provisions, the security, intelligence, and law enforcement agencies can only access data which is legitimately retained. They cannot compel companies to retain more data than is necessary for these purposes, nor can they require the retention of data for longer periods to facilitate investigations. This leaves a gap in the capabilities of law enforcement in respect of communications data.

It is not in itself sufficient that companies are required by statute to collect and retain data beyond their ordinary business purposes which could be subject to the DPA and PECR.[44] This does not necessarily allow CSPs to fall under the heading of 'functional public authority'. However, the aims of the collection and retention processes, along with the judicial reasoning provided for in YL, discussed in the following analysis, provide for a strong case that these CSPs are in fact exercising a 'function of a public nature'.[45] The primary function of this retention is

[41] Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426 s 5.
[42] Ibid
[43] Ibid
[44] It must be acknowledged that often companies are required by regulations to collect and retain some forms of data for potential future use by law enforcement. Notably, s 6 of the Wireless Telegraphy Act 1967, amended by the Communications Act 2003, required television dealers collect personal information to facilitate the notification of sale and hire televisions sets, until repealed by Schedule 21 of the Enterprise and Regulatory Reform Act 2013. Similarly, regulatory regimes which have traditionally governed telecommunications and internet companies have utilized self- or co-regulatory regimes to govern service providers (see: Koops B, Lips M, Nouwt S, Prins C, Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners (The Hague 2006)). However, the legislative framework governing CSPs does not fall under the remit of self- or co-regulation. Rather, state intervention is required to ensure companies satisfy these requirements and perform functions which otherwise they would be unwilling or unable to do. See: Ofcom, 'Identifying Appropriate Regulatory Solutions: Principles for Analysing Self- and Co-Regulation' (10 Dec 2008).
[45] A similar argument has been developed regarding the Internet Watch Foundation, where it can also be argued that the IWF is performing 'functions of a public nature' in accordance with these principles. See: Laidlaw E, 'The

to facilitate law enforcement. Using traditional telecommunications systems, such collection of data would have been under the purview of law enforcement and permitted public authorities.[46] By requiring the retention of this data by CSPs, functions are executed under the guise of private actions which can be utilised solely by the state. When coupled with the principles established in the relevant case law, CSPs can be said to satisfy the requirements of a 'functional public authority', namely: providing a service with a social benefit, being publicly funded, possessing statutory underpinning, and carrying out a governmental function. The following tracks the legislative developments which lead to this conclusion and the subsequent impact on human rights.

Anti-Terrorism Crime and Security Act

As a result of the capability gap between data retained by CSPs during their ordinary business dealings and data desired by law enforcement, the Anti-Terrorism, Crime, and Security Act (ATCSA) 2001 was enacted, under which a voluntary code was introduced to allow CSPs to retain communications data for periods longer than necessary for business purposes in order to facilitate law enforcement and national security operations. The issue of whether such retention would place CSPs within the definition of a functional public authority was addressed during the deliberation of the ATCSA Code of Practice. Therein, the Home Secretary stated the Government's position that the retention of communications data by CSPs was 'a private function that arises out of the commercial service that the communication service providers provide',[47] and retention would be classified as such regardless of whether the data was retained for their own commercial functions or under the provisions of the Code of Practice. Any such requirements to comply with human rights obligations would have to be set forth in the Code itself.

While the provisions of ATCSA did place additional requirements on CSPs to retain data, it is argued that in the specific instances of this case, the Government were correct in their assertion

---

Responsibilities of Free Speech Regulators: An Analysis of the Internet Watch Foundation' [2012] Intl J L & Tech 312; and McIntyre TJ, 'Intermediaries, Invisibility, and the Rule of Law' (March 2008) BILETA Conference Paper.

[46] Collection of data and access by public authorities was governed in a piecemeal fashion by several statutes including: Regulation of Investigatory Powers Act 2000; Police and Criminal Evidence Act Schedule 1; Wireless Telegraphy Act 2006 s 48; and the Telecommunications Act 1984 s 94.

[47] Joint Committee on Human Rights, Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-Terrorism, Crime, and Security Act 2001, (2002-03, HL 181, HC 1272) 6.

that these requirements did not meet the threshold of 'functions of a public nature'. Two details are key to this conclusion. First, while there was an obligation to retain the data under the Code of Practice, such an obligation was 'voluntary'; CSPs were under no direct statutory requirement to retain any particular data for any set period of time. The voluntary nature of these agreements lends itself to the conclusion that the retention was a private function. Second, where CSPs did retain data, they only retained that which they already generated and collected for business purposes. No additional categories of data were collected and retained; rather all the data had a clear commercial value for the CSP. It is unlikely that the future use of retained data by law enforcement would be sufficient to satisfy the requirement that the function be in the public interest.

It is important to note the specific requirements of ATCSA as it related to these retention regimes and distinguish them from later legislation. It is these further developments in the law which expanded retention outside the scope of purely business functions, and therefore engage s 6(3)(b) HRA.

The Data Retention Regulations of 2007 and 2009

Data retention was expanded at the supranational level in 2006 when the European Parliament and the Council adopted Directive 2006/24/EC on the retention of data generated or processed in the provision of publicly available communication services or public communications networks.[48] The purpose of this Directive was 'to harmonize the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law'.[49] The Data Retention (EC Directive) Regulations 2007 and the Data Retention (EC Directive) Regulations 2009 gave domestic effect to this Directive requiring the retention of certain categories of data generated by CSPs. These Regulations permit retention if notice is given by the Secretary of State to the relevant service provider, despite the provisions of the PECR and DPA which previously governed this data and limited the scope of its use in the commercial sense. Any such notice allows for CSPs to derogate from requirements under the

[48]Directive 2006/24/EC of the European Parliament and the Council on the retention of data generated or processed I connection with the provision of publicly available electronic communications networks (2006) OJ L105/54. This Directive amended Directive 2002/58/EC which was given domestic effect in the PECR 2003.
[49] Ibid at Recital 21.

DPA and PECR which govern private retention, for listed categories of data and data retention periods.[50] Once provided with the notice, CSPs are under a positive duty to retain the data stated in the notice and a failure to do so may result in civil proceedings being initiated by the Secretary of State.[51] While these provisions place the CSP under a duty, the retention required does not extend beyond that data which is required in the ordinary course of business. The mere fact that a CSP is under an obligation to retain the data does not in itself satisfy the criteria for declaring it a public function as the data retained possesses potential commercial value. However, subsequent developments in the legislation have distinguished this retention which is ancillary to business purposes from that done in the public interest.

Data Retention and Investigatory Powers Act (DRIPA) 2014

The Data Retention Directive 2006/24/EC was challenged before the European Court of Justice in the case of Digital Rights Ireland. This case questioned whether the Directive was compatible with, among others, Articles 7 and 8 of the Charter of the European Union concerning privacy and the processing of personal data, and Article 8 of the ECHR. In its judgment, the Court examined whether the Directive's provisions satisfied the requirements of necessity and proportionality in instituting the expansive and indiscriminate retention of personal data. The court held that it did not, emphasizing that the retention captured data of all persons regardless of any link to serious crime;[52] no provisions were made for privileged or sensitive communications;[53] the retention was not subject to any prior judicial review;[54] and the Directive allowed for overly expansive retention periods.[55]

Following the invalidation of Directive 2006/24/EC, the Government acted quickly to pass the Data Retention and Investigatory Powers Act (DRIPA) to clarify the scope of data retention in the UK, ensure that retention would continue, and confirm that adequate safeguards existed so retention would not fall foul of relevant human rights obligations. DRIPA effectively replicated the provisions of the Data Retention (EC Directive) Regulations 2009, placing on statutory footing the requirement that CSPs retain data. Specific implementing measures and detailed

[50] Data Retention (EC Directive) Regulations 2009, SI 2009/859 s 5.
[51] Ibid at ss 10(5) – 10(6).
[52] Digital Rights Ireland, supra note 10 at para 58, 59.
[53] Ibid
[54] Ibid at para 62.
[55] Ibid at para 63, 64.

obligations were enumerated in the Data Retention Regulations 2014 following the passage of this Act.[56] The Act does not require the retention of any new categories of data; the data retained is still that which is generated through the ordinary commercial actions of the company. However, the value of this data to the company, due to technological developments and changes in business models is negligible. Algorithmic processing allows for quicker processing of the data for use in applications such as targeted advertising which thereby require shorter retention periods. Business models no longer rely on usage or call logs for billing purposes making the retention of specific traffic and user data unnecessary. Additional requirements placed on CSPs under DRIPA regarding storage, security, and potential uses of the data further diminish its commercial value. These developments lend themselves to the conclusion that, while the precise provisions regarding data retention may not have been substantially altered between the previous retention regulations and the 2014 Act, social and technological developments have contributed to a change in the status of their functions. Traditional retention is therefore no longer necessarily in the best commercial interests of these companies. Following the established case law, it can be argued that CSPs under DRIPA satisfy several of the recognized criteria to be classified as performing 'functions of a public nature': they are under statutory authority; the service is done in the public rather than private interest; and the primary objective of the retention is to perform a public function.

First, under DRIPA, CSPs are performing a duty which is imposed on them by statutory authority. Section 4 DRIPA provides that it is the duty of public communications providers to retain relevant communications data if provided with a notice by the Secretary of State. This notice will include the company to which it relates, which services the data must be retained for, the data to be retained, the periods of retention, and any additional requirements or restrictions pertaining to the data.[57] While the Secretary of State must take reasonable steps to consult with a CSP before issuing such a notice,[58] this requirement may be waived if necessary.[59] Further, this consultation does not require the Secretary of State to find the CSPs input or objectives persuasive. Nor does the CSP have any ability to challenge a notice which requires them to retain data, regardless of any potential costs or hardships it might place on the company. Rather,

[56] Data Retention Regulations 2014, SI 2014/2042.
[57] Home Office, Retention of Communications Data (Code of Practice, 2014) at para 3.3.
[58] Ibid at para 3.9.
[59] Ibid at para 3.13.

s 10(5) states that CSPs provided with notices are under an obligation to comply with them and s 10(6) asserts that a failure to comply with these requirements are enforceable through civil proceedings by the Secretary of State for an injunction or for the specific performance of a statutory duty under s 45 of the Court of Session Act 1988[60] or for any other appropriate relief. The requirements of DRIPA are indicative that the obligations on CSPs are rooted in statutory duties rather than contractual obligations, indicating that the duties are 'functions of a public nature'.

Second, the requirements imposed by DRIPA indicate that the retention of data is done primarily to satisfy a public interest objective. Retention is used in the prevention, detection, and investigation of crime and the protection of national security interests. In 2015, there were over 700,000 pieces of data accessed by public authorities under this regime.[61] Communications data can be useful for a variety of purposes, from verifying alibis to tracking suspected drug dealers, human traffickers, and fraudsters. The value of communications data is clear. Its retention fulfils a public interest and necessitates statutory provisions to ensure that companies can retain it without violating the provisions of the DPA and PECR. Without these additional statutory provisions, companies would be obligated to delete the data once it was no longer required for business purposes, thereby diminishing the potential data pools that law enforcement and intelligence agencies would have access to in the execution of their duties. The importance of this data has frequently been noted by the Government: 'given the essential role communications data plays in assisting law enforcement agencies in protecting our citizens and bringing offenders to justice, the Government has for some years sought to ensure that it is retained and made available to appropriate public bodies lawfully, consistently, and efficiently'.[62] The retention of communications data by CSPs clearly fulfils a function which is in the public interest.

Third, the public interest dimension does not have to displace the private commercial interest in order to qualify as a public interest function for the purposes of the HRA. However, the specific requirements of DRIPA call into question the actual commercial value of the information retained. Technological developments have altered the needs for companies to retain data;

[60] S 45(b) Court of Session Act 1988 states that the Court may, on application by summary petition, order the specific performance of any statutory duty.
[61] May, supra note 5 Annex B.
[62] Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009, 3.

differing plans and services mean that billing procedures are no longer what they were when these provisions were originally envisaged. This means that companies often do not have the need to keep the same types of data; the value of the data will be subject to diminishing returns the longer it is required to be retained. This does not mean that retention has no value; but rather companies are focused on retaining categories of data which allow for profit rather than the traditional types required by statute. This issue was taken into consideration in the drafting of DRIPA. Lord West, for example, noted the problem in his contribution to the Parliamentary debates on the Bill:

> I was made aware that changes to communications technology meant that a record of communications information would no longer be held by communications service providers and that technology was changing the types of data that were available. This information was held purely as it was needed for the companies' billing procedures – that is why they kept it - and, as such was available for use by properly authorized state officials, in particular for prosecution of serious crimes and terrorism cases. New technologies and methods of communication meant that firms were beginning to, and going to, charge differently.[63]

If companies no longer need to retain the data, it would seem to follow that the company is discharging a public, as distinct from a private, function in retaining it.

Even where the data retained does have some value to the company, the actual retention requirements diminish its commercial viability. Due to the nature of retention notices and requirements concerning data security and integrity, 'it will often be the case that dedicated systems will be constructed within a CSP for the retention of communications data'.[64] This is significant in that it essentially compels CSPs to create a database solely for the data it retains pursuant to a notice under DRIPA. The 2014 Regulations acknowledge that there will be substantial costs incurred by the CSPs in complying with notices under DRIPA.[65] As such, the Government may provide contributions to the costs of developing, maintaining, testing, and operating these systems incurred by the CSPs in complying with statutory obligations.[66] This is particularly beneficial for CSPs who have to employ staff specifically to manage compliance with the requirements of the notice. Neither the creation of these databases nor the hiring of

[63] HL Deb 26 Jan 2015, Vol 759, cols 27-34, 39.
[64] Retention Code, supra note 48 at para 3.21.
[65] Ibid at para 5.1.
[66] Ibid at para 2.14.

additional staff to facilitate the retention of communications data for policing and intelligence purposes represents a profitable function for the company. Indeed, based on the precedent which forms the basis of the definition for 'functional public authorities', this element of public funding is indicative that the CSP is performing a 'function of a public nature'.

The lack of commercial justification for retention is further compounded by additional limitations placed on the access to and use of the communications data. In most cases, the data retained pursuant to a notice must be stored in a dedicated retention and disclosure system, separated by security measures from the CSPs business systems.[67] If data is retained subject to a notice, and would not be held for business purposes by the CSP, or should have been deleted under DPA and PECR standards, it must be protected from access by the company; the data may only be accessed and used subject to a lawful request.[68] This means that even though the data has been retained by the company, they may not have access to it. It further means that the retained data cannot be used for any additional business purposes which might be beneficial to the CSP, such as marketing or targeted advertising, when it is under the remit of the retention notice. In this regard, CSPs are essentially proxies for government retention and collection rather than the functions being ancillary to their ordinary business purposes. The dominant value of such retention therefore remains the public interest consideration. As such, it can be argued that such retention by CSPs is a public function.

Counter Terrorism and Security Act (CTSA) 2015

As demonstrated above, DRIPA satisfies several of the requirements necessary to classify a private actor as a 'functional public authority', namely, the statutory underpinning of the retention, the dominant public interest element, the lack of commercial value, and the element of public funding. This argument that CSPs are performing a public function in retaining communications data under DRIPA is even more persuasive when examined considering the provisions of CTSA 2015. The statutory duty to retain data on receipt of a notice under CTSA remains the same as under DRIPA. However, CTSA expands the categories of data to be retained, moving beyond those normally generated by or necessary for business purposes, to imposing a private obligation on providers to retain data relating to IP addresses. Specifically,

[67] Ibid at para 6.3.
[68] Ibid at para 8.6.

Part 3 CTSA allows the Secretary of State to require providers to retain communications data that will allow relevant authorities to link the unique attributes of an IP address to the person or device using it at a particular period of time.[69] The Act notes that this is necessary 'as there is no existing legal requirement for CSPs to keep a log of devices and addresses, it is not always possible for law enforcement agencies to identify through their enquiries who was using an IP address at any particular time'.[70] Liberty noted that '[i]n principled terms, this marks a significant shift in the relationship between the State, companies, and service users, co-opting companies into the surveillance process in a novel way and it grant[s] the State power to require companies to generate new information'.[71] Not only would companies not be legally entitled to retain IP address information under the PECR and DPA as it satisfies no business purposes, but even if they were they would be unlikely to do so, due to the additional cost and risk of public backlash as regards its impact on privacy. Consequently, IP address retention does not pose a viable commercial interest for CSPs.

In contrast, the public interest consideration is much stronger. In fact, in her introduction to the relevant section, then Home Secretary Theresa May acknowledged that the primary purpose for retaining the data was law enforcement.

> Companies generally have no business purpose for keeping a log of who used each address at a given point in time, which means that it is not possible for law enforcement agencies to identify who sent or received a message. The provisions will allow us to require key UK companies to retain the necessary information to enable them to identify the users of their services. That will provide vital additional capabilities to law enforcement in investigating a broad range of serious crime, including terrorism.[72]

This line of reasoning was followed throughout the debates. Emphasis was placed on the fact that failing to require companies to retain this information would result in less information for police and intelligence agencies.

> The provision would ensure that these data are available to law enforcement. It would improve the ability of the police and other agencies to identify terror suspects who may be communicating with each other via the internet and plotting attacks. It

[69]Counter Terrorism and Security Act 2015 s 21
[70] Home Office, IP Address Resolution Part 3 Factsheet (Counter Terrorism and Security Bill 2015).
[71] Ogilvie S, 'Liberty's response to the Home Office consultation on the Acquisition and Disclosure of Communications Data and the Retention of Communications Data Codes of Practice' (Liberty, Jan 2015) 22
[72]HC Deb 2 Dec 2014, Vol 589, cols 207-272, 214.

> would also help to identify and prosecute paedophiles, organized criminals, cyber-bullies and computer hackers, and to protect vulnerable people.[73]

IP address retention is tied to its value to the policing and intelligence services rather than its commercial value. Its substantial role in protecting the public interest, coupled with its low value for CSPs and lack of business uses; the statutory authority which requires its retention; and the element of public funding (along the same lines as retention under DRIPA), all indicate that the retention of this data by CSPs is a public function for the purposes of section 6(3)(b) HRA.

Investigatory Powers Act (IP)

Technological developments and enhanced retention capabilities led to criticisms that the current legislation which govern these regimes is no longer fit for purpose. A sunset clause attached to DRIPA placed its expiration on the 31st December 2016 resulting in proposals for a new Investigatory Powers Act which received royal assent in November 2016. As it stands, the IP Act replicates the current retention measures with the notable addition of the retention of Internet Connection Records (ICRs) and updated safeguards and oversight regimes. It is argued that the inclusion of a new category of data in the form of ICRs places the functions of the CSPs firmly under the scope of 'functions of a public nature' for the purposes of the HRA. These internet connection records are communications data which are broadly defined as records of the internet services that a specific device connects to.[74] These records may establish which websites, messaging applications, or other internet services are used; when they are used; how they are being used, including whether it is through applications on a mobile phone or other device; and demonstrate a certain device has accessed an online communications service.[75] The Government emphasized the need for the addition of this category of data in order to facilitate law enforcement, with the Home Office stating in their operational case that: 'Rapid technological change means that law enforcement's inability to access online CD is significant and will only get worse if it continues to be impossible to require communications companies to retain ICRs. More and more communications are taking place over the internet and as this happens it follows that an increasing proportion of CD will be unavailable when it is needed'.[76]

[73]James Brokenshire HC Deb 9 Dec 2014, Vol 589, Col 805-829, 823.
[74] Investigatory Powers Act 2016 s 62.
[75]Ibid.
[76] Home Office, Operational Case for the Retention of Internet Connection Records 4 November 2015.

The assumed value of ICRs to law enforcement demonstrates a departure point for the CSPs from services that possess a commercial value to those which are done in the public interest, thereby falling under the ambit of 'functions of a public nature'. Several factors are important to this conclusion. Representatives from various CSPs have acknowledged the lack of business value in retaining ICRs. Mark Hughes of Vodafone noted that: 'This is not an area that we make any money out of. We provide the very best service we can to assist law enforcement'.[77] The requirements under the IP Act regarding ICR retention place additional burdens on the CSPs beyond what the company would traditionally impose themselves. For CSPs to satisfy the requirement that they retain ICRs, they must institute a process called Deep Packet Inspection (DPI) which is not currently the industry standard. 'CSPs would have to upgrade their networks to enable them to capture communications data utilizing Deep Packet Inspection technologies to fulfil the requirements of creating and storing these Internet Connection Records'.[78] This process requires extensive capabilities and equipment to collect and store the data, imposing an additional financial burden on CSPs.[79]

In addition to the requirements placed on CSPs in collecting and retaining this new category of data, the IP Act places additional obligations on CSPs to secure and protect that data.[80] BT noted in oral evidence before the Joint Committee on the IP Bill: 'We are talking about collecting data for the first time – data that we have not collected before – and the key is to ensure that our customers and their rights are protected. The data has to be looked after very carefully, so we have to have a commensurate security wrap around them'.[81] Like the data retained pursuant to DRIPA and CTSA, the data under the IP Act must be kept separate from the data generated for business purposes[82] and may not be subsequently used by the CSP.[83] The increased burden that the retention measures under the IP Act place on CSPs are mitigated by the requirement that companies can 'receive an appropriate contribution in respect of their relevant costs' where relevant costs are those incurred by complying with a notice.[84] The overall effect of these

[77] Mark Hughes, Joint Committee on the Draft IP Bill Deb 14 December 2015, HC 144, Q 147.
[78] Written Evidence from Gareth Kitchen, Draft IP Bill, IPB0059.
[79] Written Evidence from David Walrond, Draft IP Bill, IPB0065.
[80] IP Act supra note 75 at s 92.
[81] Mark Hughes Joint Committee on the Draft Investigatory Powers Bill HC 651 Wed 9 Dec 2015, HC 651 Q 110.
[82] Home Office, Communications Data Draft Code of Practice (2016) para 16.3.
[83] Ibid at para 17.4.
[84] IP Act supra note 75 at s 249.

provisions is to remove the business value of the required processing and storage and instil an element of public funding; two further criteria which indicate that these are 'functions of a public nature' for the purposes of the HRA 1998.

The Human Rights Argument

Classifying the actions of CSPs as 'functions of a public nature' allows the retention of communications data to fall under the ambit of the Human Rights Act 1998 and the protections it guarantees. If CSPs are not seen as public authorities for the purposes of the HRA then they are not bound by the obligation to comply with Convention rights. This is particularly important due to the intrusive nature of retention and its impact on the right to respect for private life under Article 8 ECHR. Communications data enables privacy intrusions. In the Digital Rights Ireland case, Advocate General Cruz Villalon addressed the intrusive nature of communications data, noting such data makes it possible 'to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his identity'.[85] It occurs on a 'mass' scale, covering all users of a service or visiting a site. It is essentially impossible to communicate without generating the data caught by these instruments and its impact is therefore expansive. The European Court of Human Rights has confirmed that the mere act of retention and collection which potentially enables surveillance is sufficient to interfere with Article 8 rights.[86] It is therefore necessary to provide for protections in the relevant instruments to ensure these rights and to guarantee that individuals have recourse to a remedy when their rights are violated.

To this end, secondary instruments applicable to the investigatory powers instruments provide that privacy rights must be protected. However, the protection of human rights through secondary instruments has been deemed insufficient by the Joint Committee on Human Rights when examining the duties of functional public authorities. The Committee said, 'We accept that in a number of areas the protection offered by existing regulatory frameworks may provide some

[85] Digital Rights Ireland, supra note 10 at paras 72, 74.
[86] Weber & Saravia v Germany App no 54394/00 (ECHR 29 June 2006); Liberty & Ors v GCHQ & Ors 2014 UKIPTrib 13_77-H 5 Dec 2014; Amann v Switzerland App no 27798-95 (ECtHR 2000-II).

protection for human rights. However, without the application of the HRA, the protection offered will continue to be a diminished version'.[87]

The protection of human rights as regards data retention is effected by the provisions in the relevant legislation in DRIPA and CTSA, provisions under the DPA and PECR, and relevant secondary instruments such as the Retention Code of Practice. Many of these principles mirror HRA requirements for proportionality and necessity. Nevertheless, the provisions are not sufficient to protect human rights at the same level as the HRA. The Government has argued that it is not the retention that interferes with human rights obligations; rather it is the subsequent access of this information.

> In all the hubbub about this matter, sight seems to have been lost of the fact that what these proposals involve is simply the retention of records of communications – not even retention by the Government, but retention by the providers. What that would allow is properly authorized access by law enforcement agencies only to the communications of those whom they have reasonable grounds of suspecting as meaning to do us harm.[88]

Issues of access are required to satisfy human rights obligations because the retained data may only be accessed by relevant public authorities, a process which falls under the obligations of the HRA and its accompanying safeguards. However, the argument that the interference here only occurs once the data has been accessed is misleading. The European Court of Human Rights acknowledged this in Amann v Switzerland wherein it was held that the storing of data regarding the private life of an individual amounted to an interference with Article 8(1) ECHR.[89] Subsequently, the case of S and Marper v United Kingdom concluded that 'the mere retention and storing of personal data by public authorities, however, obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data'.[90] Further decisions have similarly focused on the potential threat and abuse caused by the collection and retention of data rather than the particular

[87] JCHR supra note 37 at 32.
[88] Lord Butler of Brockwell HL Deb 13 Jan 2015, Vol758, cols 651-747, 737.
[89] Amann supra note 83.
[90] S and Marper v United Kingdom App No 30562/04 and 30566/04 (ECHR 4 Dec 2008) 121.

access conditions,[91] an issue that is becoming increasingly significant as technologies saturate society and generate exponentially increasing pools of data.

The failure to classify CSPs as functional public authorities and thereby ensure that the collection and retention of this data is protected under the HRA diminishes individual protections. Currently, the only means of ensuring that retention meets human rights standards is through secondary instruments which require the Secretary of State to consider necessity and proportionality before issuing a notice.[92] While this imposes some requirements, it leaves demonstrable gaps in the human rights protections. Indeed, the JCHR has noted: 'While regulatory and inspection regimes clearly pay a very important role in ensuring the rights of services users and the quality of public services, they cannot be treated as a substitute for directly enforceable Convention rights'.[93] The lack of directly enforceable Convention rights means that individuals whose data is collected and retained have no recourse to challenge retention which is done for law enforcement or national security purposes. Indeed, the notice requirements placed on CSPs prevent them from even disclosing to individuals that their data is retained, even if individuals believe their data has been wrongly retained or retained in a manner inconsistent with the security, integrity, and destruction requirements of the relevant statute. Further, it is significant that individuals often have no choice in choosing to enter a relationship with a service provider and therefore no ability to prevent the data retention. 'While it is plausible to distinguish for HRA purposes between public and private regimes where those subjects are genuinely free to choose; it is much less so where the individual has no practical option but to accept the private provision'.[94]

By confirming the status of CSPs in exercising statutorily mandated retention as performing 'functions of a public nature; there would be stronger human rights protections, particularly by providing individuals with the right to a remedy and the ability to challenge the compatibility of retention requirements with the provisions of the HRA and ECHR.

Conclusion

[91] Case C-362/14 Max Schrems v Data Protection Commissioner (2015) OJ C351/14 and Digital Rights Ireland supra note 10.
[92] Home Office, supra note 79.
[93] JCHR, supra note 37.
[94] Sunkin, supra note 14 at 653.

Based on the current criteria as identified through relevant case law, CSPs are performing 'functions of a public nature' pursuant to s 6(3)(b) of the Human Rights Act 1998. The current statutory requirements, set forth in DRIPA and CTSA, provide that the powers of retention exercised by CSPs are done through statutory authority; are publicly funded; and accomplish functions that are primarily in the public interest, often at the expense of their own commercial benefit. The provisions under the IP Act demonstrate a further departure from retention for business purposes to a process principally satisfying a law enforcement and national security objective. As the current law stands, any decision on whether the retention and collection processes will satisfy the requirements of 'functions of a public nature' must be left to the Courts. It is argued that human rights requirements would be better satisfied if this qualification was placed on the face of the relevant statutes. Classifying CSPs as functional public authorities places an obligation on these companies to comply with the human rights provisions as established in the HRA 1998. In doing so, not only would the protections currently set out in secondary instruments remain, but there would be increased protections, particularly by guaranteeing individuals rights of challenge and redress. This protection is necessary due to the interference with private life that arises from the retention of data.