The Investigatory Powers Act 2016 and Connected Vehicles: A New Form of Panspectric Veillance Looming?

MARSON, James <http://orcid.org/0000-0001-9705-9671>, WHITE, Matthew and FERRIS, Katy

The Investigatory Powers Act 2016 and Connected Vehicles: A New Form of Panspectric Veillance Looming?

Connected and autonomous vehicles (CAVs) currently exist in varying states of readiness to, at one end of the spectrum, assist the driver in normal driving activities and at the other operate in fully autonomous mode, requiring no driver input at all. In facilitating these features, CAVs create, give access to and allow communication of the data produced. The further along the autonomous scale CAVs progress, the greater the data generated, which are being harvested by original equipment manufacturers (OEMs), often unwittingly by the end-user. The operation of the Investigatory Powers Act 2016 gives government agencies power to compel the retention and access to these data. Here we argue that the definitions within the Act result in CAV OEMs being subject to retention notices of the data generated by these vehicles. This issue, its extent and potential for abuse, and the lack of protection for those associated with the use of CAVs, hitherto unexamined in the legal academic literature, is the focus of this paper.

Keywords: Breach of human rights; Communications data; Connected and autonomous vehicles; Investigatory Powers Act 2016; Privacy, Retention notices.

INTRODUCTION

Connected and autonomous vehicles (CAVs) are anticipated to be the greatest disruption to travel seen in at least a generation.[1] Through the use of a variety of on-board sensors and cameras, CAVs are able to drive independently. These vehicles collect, process and produce data from the vehicle's cameras, LiDAR[2] and RADAR[3] sensors, along with the neural networks and emerging vehicular clouds where 'vehicles can communicate with one another, form self-organized vehicular ad-hoc networks, collect real-time sensing data, conduct intensive computation, and disseminate information.'[4] Whilst the true 'full self-driving' features of CAVs are only beginning to be tested through access given to a restricted group of members of the public (based on their safety records),[5] the data generated by CAVs to enable their (current) semi-autonomous[6] features have already led to concerns being raised relating to

[1] See for instance S. A. Cohen and D. Hopkins, 'Autonomous Vehicles and the Future of Urban Tourism' (2019) 74 *Annals of Tourism Research* 33.
[2] A system of laser pulses which build a three-dimensional model of the environment around the vehicle.
[3] To enable the car to 'know where it is' and avoid the hazards of traffic.
[4] For a discussion regarding the complexity in constructing a v-cloud see J. Kang, E. Bertino, D. Lin, and O. Tonguz, (PDF) 'From Autonomous Vehicles to Vehicular Clouds: Challenges of Management, Security and Dependability' (2019) Paper presented at Conference: IEEE 39th International Conference on Distributed Computing Systems at: Dallas, Texas (April 2019). Available from: https://www.researchgate.net/publication/332130832_Survey_-_From_Autonomous_Vehicles_to_Vehicular_Clouds_Challenges_of_Management_Security_and_Dependability.
[5] https://www.businessinsider.com/tesla-full-self-driving-elon-musk-beta-update-safety-score-2021-9?r=US&IR=T.
[6] This term is quite widely used in discourses around CAV development but it is, of course, a misnomer. Any vehicle which is not fully autonomous is not 'autonomous' as it requires constant supervision from the driver/person in charge to take control at any point during the journey.

users and non-users' privacy,[7] and these are advancing with each further step along the autonomous vehicle, Society of Automotive Engineers (SAE), scale.[8]

The Investigatory Powers Act (IPA) 2016 aimed to bring communications data retention within a single, clear piece of legislation.[9] Section 87 of the IPA 2016 enables the Secretary of State, subject to approval, to issue to telecommunications operators and communication service providers (CSPs) a notice compelling them to retain, for a period of up to 12 months,[10] communications data. These data may be retained for a purpose as outlined in s. 61(7) which includes (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (d) in the interests of public safety; and (g) for the purpose of preventing (or mitigating against) death or injury or any damage to a person's physical or mental health.[11] Consequently, intelligence agencies and law enforcement bodies are able to conduct targeted interception of communications,[12] and in certain instances without a warrant.[13] It should be noted from the outset that the obligation to retain is not exclusive[14] to the Secretary of State and Judicial Commissioner,[15] but also a variety of relevant public authorities under the guise of the state. The Government sought to introduce authorisations through an Investigatory Powers Commissioner (IPC)[16] to ensure independence in the process. This, however, overlooks the fact that the IPC is also the reviewer and auditor of said authorisations.[17]

[7] See the report (in German) regarding Tesla not providing the purposes for the use of personal data, its continuous monitoring of its environment, a lack of data minimization and the cross-border transfer of data without adequate protection. The report continues, at p.7, that the cameras on the Tesla Model 3 evaluate and record vehicle license plates and performs facial recognition. Available at https://www.heise.de/news/Studie-zum-Datenschutz-Elektroautos-von-Tesla-duerften-nicht-zugelassen-werden-4934095.html.

[8] The SAE International Standard J3016 identifies the levels of automation of vehicles. At level 0, the driver controls all aspects of driving. Level 1 includes steering and acceleration/deceleration assistance systems aiding the driver. At level 2, partial automation provides steering and acceleration/deceleration using information from the driving environment. The driver is expected to intervene and respond when requested at Level 3, but all other aspects of driving is taken by the CAV. Level 4 denotes high automation where the automated system takes all aspects of driving. Level 5 refers to an automated driving system where all tasks in all roadway and environmental conditions are taken by the system. It denotes a full automation system.

[9] Home Office, *Draft Investigatory Powers Bill* (Cm 9152 2015) [26].

[10] Section 87(3) of the IPA 2016.

[11] None of which are defined in the Act.

[12] We note retention powers and interception are mentioned closely here. For clarity, of course retention and interception are two different things. However, interception under the guise of retention is possible, for example s. 46 of the IPA 2016 could allow such interception.

[13] Not all interceptions require an (immediate) warrant, for example urgent warrants. However, the state authorities with the power to issue warrants include the Metropolitan Police Service; British Transport Police; GCHQ; Ministry of Justice; Home Office; HM Revenue & Customs; Department of Transport; and the Serious Fraud Office.

[14] It is not exclusive because Part III allows other public authorities to obtain communications data. The public authority could request that the telecommunications operators obtain and keep records for them to have access to at a future point. The explanatory notes for the IPA 2016 maintain that s. 61(5)(a) allows a relevant public authority to request communications data on a forward-looking basis in respect of a known subject of interests.

[15] At s. 61(1) of the IPA 2016, a designated senior officer (DSO) of a relevant public authority may also obtain communications data for specific investigations/operations or for testing, developing or maintaining ways relating to the availability or obtaining communications data. A DSO is defined in s. 70(3) of the IPA 2016, as a person holding office, rank or position in relation to the authority. This would include, for example, a superintendent of a police force.

[16] Regulation 3 of the draft Data Retention and Acquisition Regulations 2018 SI 2018, which inserts s. 60A into the IPA 2016.

[17] See s. 229(1)(b) of the IPA 2016.

As will be demonstrated throughout this paper, the IPA 2016 contains many examples of imprecise definitions of many significant aspects of its content, thereby expanding its reach to affect a wide group of devices such as phones, computers, refrigerators and CAVs. Whether this is intentional or otherwise will be tested latterly by the courts, however, to begin with just one example, a significant difference between IPA 2016 and the (previous incarnation) Data Retention and Investigatory Powers Act (DRIPA) 2014 is the omission of the word 'public' in telecommunications operators, which thereby extended the application of the data retention obligations to private sector entities including hosted services offering communications to businesses, or those running cloud-based communications services on behalf of businesses.[18] Indeed a conclusion may be drawn that the government was slowly reintroducing, by stealth, the wide reaching application of its failed Draft Communications Data Bill.[19]

Collectively the generation of data and their intrinsic link to those people who use and, in some cases, come into contact with these items, along with their collection and potential for (ab)use requires examination. In the academic literature, so far these discussions have been largely restricted to the ethics of the use of the data produced, along with some discussion of drivers' privacy.[20] What is clear from the application of the IPA 2016 and the emerging use of CAVs is the potential infringement of individuals' human rights through creating what has been termed by Portela and Cruz-Cunha 'panspectric veillance.'[21] Here people are, unbeknown to them, subject to surveillance. CAVs produce vast quantities of data,[22] and there is increasing evidence of data breaches occurring with the transmission of these data (despite promises of the adoption of privacy-by-design features being embedded in the vehicles).[23] Given the latitude in definitions, the extent of the (at least somewhat unconstrained)[24] powers, and the limited safeguards present in the IPA 2016, the state is able to access ever more data about people, their movements, their connections, their habits and their interests than ever before.

Our aim is to raise the potential problems that the IPA 2016 presents for individuals' privacy, especially in the context of CAV use, how the definitions within the Act are sufficiently expansive to encompass CAV OEMs as being susceptible to data retention notices, and their culmination in the breaches of individuals' privacy through the IPA 2016 and CAVs. We conclude that caution might have to be exercised by users in the deployment of CAVs, and that

[18] For commentary see N. Brown, 'A Quick Overview of the Draft Investigatory Powers Bill' (4 November 2015) <http://www.scl.org/site.aspx?i=ed44789>; and J. Cobbe, 'Casting the Dragnet: Communications Data Retention under the Investigatory Powers Act' (2017) Available at <https://www.academia.edu/33709047/Casting_the_Dragnet_Communications_Data_Retention_under_the_Investigatory_Powers_Act>.

[19] Clause 1, and 28 of the Draft Communications Data Bill.

[20] See, for example, D. J. Glancy, 'Privacy in Autonomous Vehicles' (2012) 52(4) *Santa Clara Law Review* 1171.

[21] I. M. Portela, and M. M. Cruz-Cunha, 'What About the Balance Between Law Enforcement and Data Protection?' in I. M. Portela, and M. M. Cruz-Cunha (eds) *Information Communication Technology Law, Protection and Access Rights: Global Approaches and Issues*, (IGI Global 2010).

[22] As of February 2020, Tesla vehicles had amassed a combined 3 billion miles of real-world data: https://lexfridman.com/tesla-autopilot-miles-and-vehicles/.

[23] See for example the European Data Protection Board, 'Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications' (2020) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf; and Resolution on data protection in automated and connected vehicles; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.

[24] We use this term when considering, for example, that the Secretary of State/Judicial Commissioner permit blanket and indiscriminate surveillance. The IPA 2016 does not prevent this.

the IPA 2016 itself should be reconsidered to avoid breaches of the European Convention on Human Rights (ECHR) and individuals' privacy generally.

LEGISLATING PLAINLY, PRECISELY AND WITH A CLEAR TARGET

This paper critiques the extent and application of the IPA 2016 with the increasing prevalence of CAVs, the data they produce and are thus available for retention purposes. The definitions within the IPA 2016 and the applicability to CAV OEMs will be considered later, but we begin here with a general outline of the problem of legislating with definitional certainty and law's race to keep up with technological change. From the outset it must be acknowledged that there is great skill in the drafting of well-written and clearly articulated legislation. Indeed, as noted by Dickerson, it embodies the most rigorous form of writing outside of mathematics.[25] Further, as discussed in this journal by Watson-Brown,[26] plain English being used in legislation is of supreme importance in legal drafting, yet often remains definitionally elusive. He rightly notes the distinction between simplicity of language and effective communication, ensuring that

> effective communication [does] not reduce important matters to simple statements for the sake of simplicity. It is desirable that a complex issue becomes more understandable but the issue covered by the policy expressed in legislation should not be abandoned for the sake of simplicity.[27]

This led to Watson-Brown's critique of Coode's formula for legislation,[28] a formula which should consist of the description of the legal subject, enunciation of the legal action, and when the law is not of universal application, the following dimensions should be added to the formula: the description of the case to which the legal action is confined. And finally, the conditions on performance of which the legal action operates. However, Watson-Brown, at page 18, observes that such a formulaic approach leads to materials which are difficult to understand, with the reader being 'confronted with a series of conditional propositions before knowing who is to do what.' The IPA 2016 is, by necessity, a complex piece of legislation. It facilitates the retention of data, the requests for and interception of communications data, allows for the bulk warrants for communications data and equipment interference. Yet many of its definitions and powers are not completely defined and are open for interpretation. Given the scope for increased surveillance, which was the purpose of the Act, clarity of definitions to articulate the extent of the powers, especially those which operate extra-territorially and may cause jurisdictional problems, are of the upmost significance. It is also the breadth of the IPA 2016 which impacts on the clarity and increasing scope of the legislation. It was in the Regulation of Investigatory Powers Act 2000, to DRIPA 2014 and most recently the IPA 2016, where the obligation to retain has expanded from telephone companies and Internet Service Providers (ISPs) to include websites, cloud-based services, controllers of networks, devices, apps, software, hardware and internet of things (IoT) objects. The obligation to retain could be interpreted to apply to almost anything that communicates, and its application to normal and seemingly mundane items, especially those which people have frequent contact with – their

[25] R. Dickerson, 'Legislative Drafting: A Challenge to the Legal Profession' (1954) 40 *Indiana Law Journal* 635, 635.
[26] A. Watson-Brown, 'In Search of Plain English—The Holy Grail or Mythical Excalibur of Legislative Drafting' (2011) 33(1) *Statute Law Review* 7.
[27] ibid, 9.
[28] G. Coode. 'On Legislative Expression; or, the Language of Written Law' (1845) available: http://metaphysicspirit.com/books/Legislative%20Expression.pdf.

mobile telephone and their car (for instance), has implications for their privacy and wider human rights.

This brings us to an issue Moses,[29] among others, has examined, the reasons and responses to law's race to keep up to date with technological change. Laws in this area can move quickly, and developments have been identified above, but ultimately technology and its increasingly data driven and connected nature can supersede the laws which interact, affect and/or govern it. Due to the perception that law may struggle at times to realise the implications of future changes, suggestions have been advanced around improved statutory drafting techniques and technology-neutral legislation which operates effectively in different technological contexts. Yet technological-neutral drafting is likely to be successful for existing technologies and less so for changing technological environments. This debate is not new. In the jurisprudence of the United States, such discussions were raised in respect of the legal problems affecting emerging technologies in the rail industry in 1858,[30] and human interactions with computerised automated systems has been discussed by Teubner.[31] Yet it is the reason for the legal problems and how they arise in respect of technological change, understood from the perspective of legislating, which requires examination. In respect of the analysis we provide of the IPA 2016 and its extension through the data captured by CAVs, a legal problem which shadows technological change is the possible over-inclusiveness of existing legal rules as applied to new practices. For context, the IPA 2016 was established, following the conclusion of three independent reviews in 2015, to realise a consolidation of powers held by various security and intelligence agencies in relation to the gathering of communications and content data, the regulation of these powers, and to update the law to be fit for purpose in an increasing digital age. It gave government agencies powers to require technology and communications businesses (quite broadly defined, as will be demonstrated) based within the UK and extra-territorially to retain personal data of customers.[32] Thus, businesses could be required to assist UK agencies with reference to the execution of bulk equipment interference – interception – warrants. This was the target or goal of the legislation, yet as we are arguing in this paper that the CAV OEMs are now subject to the retention powers within the IPA 2016, it is far from certain that the drafters had in mind the inclusion of data from a new technology (and one which produces data as a (mere) by-product of its functionality).

It is arguable, therefore, that the IPA 2016 was not formulated with new technologies in mind, despite the increase in its scope, and it is further arguable that the increasing use and adoption

[29] L. B. Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) *Journal of Law, Technology & Policy*, 239.

[30] E. L. Pierce, A Treatise on American Railroad Law' (1857) available: https://books.google.td/books?id=8i00AQAAMAAJ&printsec=frontcover&hl=fr&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[31] G. Teubner, 'Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law' (2006) 33 *Journal of Law & Society*, 497.

[32] Thereby achieving the same goal albeit using a different power. Section 61(4)(c)(i) allows an authorised officer to, where they believe a telecommunications operator is *not already in* possession of but *maybe or is capable of obtaining any communications data* (authors' emphasis), by notice, require them to obtain data that is not already in their possession and disclose data subsequently obtained by them. Moreover, s.61(5)(a) allows authorisations for data that did not exist at the time of the authorisation. This could require telecommunications operators to generate and *retain* material they may normally would not. The explanatory notes for the IPA 2016 maintains that s.61(5)(a) allows a relevant public authority to request communications data on a forward-looking basis in respect of a known subject of interests.

of CAVs in private ownership was not foreseen in the drafters' intentions,[33] but the result of the introduction of CAVs has meant their, perhaps inappropriate, inclusion in the realm of this legislation. Essentially, this pre-existing law is being applied to a new context and perhaps beyond the target of the original intentions of the drafter. The technological change with the advancing CAV mode of transport, not only in terms of increasing adoption and new government initiatives to increase the numbers of electric (and therefore more likely to also be connected) vehicles, replacing those using internal combustion engines, with the increasing sophistication of the CAVs as they move up the SAE scale to full autonomous modes (and create more data), aggravates the targeting of legislation. The new sources of data, from cameras inside and external to the vehicle, to communications between the vehicle and other vehicles to the vehicle and infrastructure, may have lost the clear connection between the IPA 2016 and the intended businesses which would come within its defined jurisdiction. The problem with technological changes and older legislation, particularly in respect of protecting privacy rights, has been widely discussed by authors including Bernstein[34] in the realm of protecting identity interests.

We return to these issues throughout the remainder of the paper, identifying the definitional problems within the IPA 2016, in particular how they apply to CAVs, and the over-inclusiveness of the Act. Whether the IPA 2016 was enacted to encompass future technologies is not certain, and whether the definitions in the Act were intentionally broad to allow as comprehensive an application as possible is, again, a matter of speculation, but clearer and more precise drafting could have prevented unintentional application in new technologies and contexts. It is the loose definitions and emerging technologies which can upset the balance of legislation written at a point in time and not foreseeing application in new circumstances.

THE INVESTIGATORY POWERS ACT 2016 AND ITS APPLICATION TO CAV OEMS

A crucial matter to be determined from the outset is the extent to which the bodies identified as telecommunication operators or those providing a telecommunications service encompass organisations in possession of CAV data. This is vital to CAV OEMs and their partners (and of course the users and those affected by these vehicles) in identifying whether they could be required to retain, and latterly make available, the data produced by their vehicles. Section 261 of the IPA 2016 contains definitions relevant to telecommunications. At s. 261(10), a telecommunications operator is a body that offers or provides a telecommunication service to persons in the UK or controls or provides telecommunication systems which is wholly or partly in or controlled from the UK. The fact that a telecommunications service is offered to a person in the UK highlights the extra-territorial application of IPA 2016, as it is not the location of the service that is important, but the location of the person to whom the service is offered.[35] The definition of a telecommunication service[36] is not dependent on whether the person/body who provides the service also provides a telecommunication system. Further, albeit not within the definition itself, but of terminology within the definition, is that of 'communications.' Its singular is defined in s. 261(2)(a) as anything comprising speech, music, sounds, visual images

[33] CAV vehicle sales in the UK in 2016 accounted for almost 90,000 of the 2.7 million units sold: https://www.smmt.co.uk/2017/01/uk-new-car-market-achieves-record-2-69-million-registrations-in-2016-with-fifth-year-of-growth/

[34] G. Bernstein, 'Accommodating Technological Innovation: Identity, Genetic Testing, and the Internet' (2004) 57 *Vanderbilt Law Review*. 965.

[35] *CG v Facebook Ireland Ltd & McCloskey* [2016] NICA 54.

[36] Section 261(11) and (12) of the IPA 2016.

or data of any description, and s. 261(2)(b), signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus. Therefore, communications have a wide-ranging meaning which would cover the interaction between vehicles and vehicles and their surrounding physical infrastructure. CAVs, using Tesla as an example, through the telematics log data, provides the vehicle's performance, usage, operation and condition, including its Vehicle Identification Number, speed, odometer readings, battery use management information, battery charging history, electrical system functions, software version information, infotainment system data, safety-related data and camera images, braking and acceleration data, security, e-brake, accidents, short video clips of accidents, information regarding the use and operation of Autopilot, Summon, and other 'autonomous' features; and other data to assist in identifying issues and analysing the performance of the vehicle.

Furthermore, Tesla is able to extract these data from the vehicle itself. It can gather this information either in person (such as during a service appointment) or via remote access. Remote analysis of data enables Tesla to dynamically connect to the vehicle in an attempt to diagnose and resolve issues with it. In so doing, it may access the personal settings in the vehicle (including the contacts, user's browsing history, navigation history, and radio listening history). Through this connection Tesla is able to view the current location of the vehicle. Given that devices, objects or things are caught under the definition of telecommunication system because of the conveyance of signals, CAV and associated hardware would fall under telecommunication operator however these definitions are approached.[37] Moreover, the obligation to retain could fall upon natural or legal persons owning devices, as a telecommunications operator includes one who provides or *controls* the telecommunications system. The magnitude of the implications of this inclusion cannot be overstated. Such technologies are already in place to some degree such as smart electricity meters,[38] TVs[39] and the list could continue to applications such as transportation and logistics, healthcare, personal and social settings[40] and the home.[41] The concern with smart objects is that they can accumulate a massive amount of data[42] which the characteristics of such traffic are currently unknown,[43] and could subsequently be retained, thus potentially turning homes and CAVs into the least technologically private place.

Any telecommunication operator, and by extension service, whether it be an app, software, website, webmail or creators of said services and so on could be compelled to make data retention capabilities possible. Section 253(5)(c) allows the removal of electronic protection to any communications data (as discussed later), coupled with s. 253(5)(b) the telecommunication operator could be obligated to retain by way of removing electronic protection and disclose it via s. 253(5)(e). This is all possible because s. 253(5) leaves open the possibility of other

[37] A position accepted by the organisation Big Brother Watch https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/03/Data-Retention.pdf.
[38] F. Mattern and C. Floerkemeier, 'From the Internet of Computers to the Internet of Things' in K. Sachs, I. Petrov and P. Guerrero (eds) *From Active Data Management to Event-Based Systems and More* (Springer, Berlin, Heidelberg 2010).
[39] John Ribeiro, 'Samsung faces complaint to FTC over Smart TV 'surveillance'' (26 February 2015) <http://www.infoworld.com/article/2889458/federal-regulations/samsung-faces-complaint-to-ftc-over-smart-tv-surveillance.html>.
[40] L. Atzori, A. Iera and G. Morabito, 'The Internet of Things: A Survey' (2010) *Computer Networks* 54:15 2787.
[41] ibid.
[42] Mattern and Floerkemeier, (n 38).
[43] Atzori et al., (n 40) 2800.

undefined obligations as it makes note of 'among other things' which could be used as a basis for issuing retention notices under Part 4 (again, whether the operator is present in the UK or not).[44] On the basis of the above definitions, we are confident that CAV OEMs would be considered a telecommunication operator and subject to retention notices. This is concerning when considering the data produced by CAVs, their attribution to individual drivers/person in charge of the vehicle, and their internal and external communications.

DATA AND DEFINITIONAL DILEMMAS

As an aim of this paper is to identify how the IPA 2016 might enable data from CAVs to be requested through a retention order from the state, it is important to first identify the definitional scope of what 'data' actually are. Part 4 of the IPA 2016 concerns the issuing of data retention notices, but also provides insight into which data are subject to notices. Section 87(1) of the IPA 2016 allows the Secretary of State to issue retention notices on telecommunication operators (as an individual, it cannot be applied to an object or device) to retain 'relevant communications data.' Section 87(4) details that telecommunications operators are not to retain 'third-party' data,[45] but s. 87(4)(d) allows these data to be required to be retained if it is used or retained for a lawful purpose. Section 87(11) concerns the retention of Internet Connection Records (ICRs) and s. 87(9)(b)(i) provides that retention notices can obligate data to be generated for the purposes of retention.

According to s. 87(11) of the IPA 2016, relevant communications data include the sender or recipient (human or not) of a communication, its time, duration, type, mode/pattern or fact of communication, the telecommunications system the communication has been transmitted to, from or through and its location. These five categories, Smith suggests, at face value appear to go wider than the data types found under the DRIPA 2014 (which implemented the Data Retention Directive[46] definitions) as amended by the Counter Terrorism and Security Act 2015.[47] Smith notes that the scope of relevant communications data 'sweeps up not only background interactions that smartphone apps make automatically with their supplier servers, but probably the entire internet of things.'[48] Smith continues that 'data such as the "type, method or pattern of communication" extend beyond the familiar sender/recipient, time and location.'[49] The application to CAVs and the plethora of communications externally, along with generated internal data which is capable of being communicated with the OEMs is equally applicable.

Although s. 87 of the IPA 2016 refers to 'relevant communications data', s. 261(5)(a) defines communications data as either entity or events data which is, or is capable of being, held or obtained, by or on behalf of the telecommunications operators. This includes data held by a telecommunications operator or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its intended destination,

[44] Section 253(8) of the IPA 2016.
[45] Explanatory notes for the IPA 2016, para 262.
[46] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[47] G. Smith, 'Never Mind Internet Connection Records, What About Relevant Communications Data?' (29 November 2015) <http://www.cyberleagle.com/2015/11/never-mind-internet-connection-records.html>.
[48] ibid.
[49] ibid.

describes how a person has been using a service or is about the architecture of the telecommunication system itself.[50]

Entity (which is a person or thing)[51] data refers to data about entities or links between them and telecommunications service/systems (although not individual events)[52] which includes phone numbers, service identifiers, physical address, or IP addresses.[53] Section 81(1) of the Regulation of Investigatory Powers Act 2000 defines person (on which the IPA 2016 is silent) as including any organisation and any association or combination of persons. Therefore, entity data can be summarised as data about an individual, any group of individuals or any object. This, consequently, and contrary to the explanatory notes, *can* provide information about individual events.

Events data is defined in s. 261(4) and can be summarised as identifying and describing events taking place on a telecommunication system or other device which consist of one or more entity engaging in an activity at a specific point, or points, in time and space.[54] This includes the sending or receiving of an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their device connected to; or the destination IP address that an individual has connected to online.[55] The explanatory notes also detail that entity data is generally less intrusive than events data, without explaining why.[56]

The breadth of the terms 'communication' and 'data' give an indication as to the significance of the powers available under retention. Combining these definitions highlights that the types of data that can be retained under Part 4 is broad.[57] However, in order to make sense of the relevant communications data issue, some insight can be gleamed from the Home Secretary, who presented evidence to the Joint Committee on the Draft Investigatory Powers Bill, of examples of what is considered to be communications data and content.[58] Although not a definitive legal source, it does give some insight into what is considered communications data. This includes, unique identifiers and location data, such as those linked to a customer's Broadband/mobile/CAV-based account as communications data and the identifiers associated with communications linked with said services. Further, communications data also consists of Wi-Fi access point identifiers, device identifiers when using mobile internet and any device identifiers of any other devices using the internet through that connection. Mapping of movements is possible through other device identifiers such as the International Mobile Subscriber Identity (IMSI) and the International Mobile Station Equipment Identity (IMEI) numbers, such as used by CAVs for their independent connected status.

[50] Explanatory notes for the IPA 2016, para 723.
[51] Section 261(7) of the IPA 2016.
[52] Explanatory notes for the IPA 2016, para 725.
[53] ibid, para 727.
[54] ibid, para 726.
[55] ibid, para 727.
[56] ibid, para 223.
[57] See for example Internet Connection Records. They are not defined, yet they fall under s. 87(11).
[58] Joint Committee on the Draft Investigatory Powers Bill, written evidence, Home Office, pp. 515-517; Similar to the types of data found in the Retention of Communications Data under Part 11: Anti-terrorism, Crime and Security Act 2001 Voluntary Code of Practice <http://www.opsi.gov.uk/si/si2003/draft/5b.pdf>.

This leads to the necessary discussion regarding location data/information[59] given that this also falls under communications data. Location data/information is regarded 'as any type of data that places an individual at a particular location at any given point in time, or at a series of locations over time.'[60] With the use of mobile phones, this may encompass 'geo-positioning other than latitude, longitude and altitude.'[61] In Recommendation AAA, the Intelligence and Security Committee of Parliament (ISC) regards approximate location data to be not as sensitive as communications data because the latter includes a more detailed class of information about a person's habits, such as preferences or lifestyle choices and websites visited.[62] However, as Scassa[63] and Uteck[64] have asserted, location data can be used to create a data picture of movements of identifiable individuals.[65] van der Hilst would go further than the General Data Protection Regulation (GDPR)[66] and argue that location could be considered 'sensitive personal data[67] or a special category of personal data because 'it can reveal information about a person's habits, (future) whereabouts, religion, and can even reveal sexual preference or political views.''[68] This highlights not only that location data can reveal very intimate details, it can be used to make future predictions based on current data possessed.[69]

Location data is, of course, a fundamental feature of CAVs. It includes rich data about the choices of the individual driver. For example, the route taken, does the driver wish to avoid motorways, visit points of interest suggested by the navigation system, avoid tolls and so on are often maintained as data generated by the vehicle. In 2011, Gasson and others conducted a study[70] of tracking four individuals from three EU Member States via their GPS enabled mobile phones. Their location data were stored in a central database for automated and manual processing (akin to data retention) in order to form profiles. Gasson noted that based on location data, a job profile could likely be drawn for certain participants.[71] Further, the researchers were able to infer the relationship (a business) between two of the participants based on travel

[59] A.S.Y. Cheung, 'Location Privacy: The Challenges of Mobile Service Devices' (2014) 30 *Computer Law and Security Review* 41, 43 'In this article, the terms "location data" and "location information" are used *interchangeably*.'
[60] ibid.
[61] ibid.
[62] Intelligence and Security Committee, para 143(V).
[63] T. Scassa, 'Information Privacy in Public Space: Location Data, Data Protection and the Reasonable Expectation of Privacy' (2009) 9(2) *Canadian Journal of Law and Technology* 193.
[64] A. Uteck, 'Ubiquitous Computing and Spatial Privacy' in I. Kerr *et. al.*, eds., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford: Oxford University Press, 2009), 85.
[65] Cheung, (n 59), 43; see also Y-A. de Montjoye, C.A. Hidalgo, M. Verleysen and V.D. Blondel, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 1376 *Scientific Reports*, 1.
[66] For a discussion of the applicability of the GDPR to CAVs, see Salami, E. 'Autonomous Transport Vehicles Versus the Principles of Data Protection Law: Is Compatibility Really an Impossibility? (2020) 10(4) *International Data Privacy Law* 330.
[67] R. van der Hilst, 'Characteristics and Uses of Selected Detection Technologies, Including their Potential Human Rights' (30 November 2011) <http://www.detecter.bham.ac.uk/pdfs/17_3_tracking_technologies.doc>, 2, 33, 38.
[68] ibid, 38.
[69] D. Ashbrook and T. Starner, 'Using GPS to Learn Significant Locations and Predict Movement Across Multiple Users' (2003) *Personal and Ubiquitous Computing* 7:5 275; M.C. Gonzalez, C.A. Hidalgo and A-L. Baraba´si, 'Understanding Individual Human Mobility Patterns' (2008) *Nature* 453 779; L. Backstrom, E. Sun and C. Marlow, 'Find Me If You Can: Improving Geographical Prediction with Social and Spatial Proximity' (2008) <http://cameronmarlow.com/media/backstrom-geographical-prediction_0.pdf>.
[70] M. N. Gasson, E. Kosta, D. Royer, M. Meints, and K. Warwick, 'Normality Mining: Privacy Implications of Behavioral Profiles Drawn from GPS Enabled Mobile Phones' (2011) *IEEE Transactions on Systems, Man and Cybernetics* 41:2 251, 252.
[71] ibid, 255.

patterns[72] and that one participant was in some way involved with children, based on trips to the park and kindergarten.[73] These points were expanded upon by Rushit et al (2019), from a US perspective, where ultimately

> a person's chronicled area and goal data would uncover 'unquestionably private' trips, for example, to a specialist, plastic specialist, fetus removal facility, AIDS treatment focus, strip club, criminal resistance lawyer, by-the-hour motel, association meeting, place of love, and gay bar. Beside the disclosure of private data, data about one's present area or travel examples may make a danger of physical mischief or stalking if that data fell into the wrong hands.[74]

On the issue of sensitive personal data, Gasson noted that although determining a participant's religion was inconclusive, it may be possible to classify a person's specific religion with some degree of certainty due to the fact that most mainstream religions have a defined routine, held in identifiable locations.[75] A point that Gasson notes is that based on just the data examined there was 'real potential for incorrect conclusions being reached based on the data.'[76] This relates to Solove's privacy problem of distortion which could have significant impact on individuals.[77] van der Hilst added that there 'is a possibility that the use of location tracking devices causes effects that are harmful to an individual or to society at large.'[78] In doing nothing, we may 'end up being a society that distrusts, that we break down the social fabric that we call networked groups and allow ourselves to be taken control over by the techno-political elite.'[79] The societal value of privacy is highlighted and the potential for its devaluation to change society forever. This is all the more serious as location data is difficult to anonymise.[80]

As noted above, there is a movement by CAV OEMs and their service providers to refrain from collecting personal data and selling it on to third-parties or to use it in a way which would compromise the privacy of the data subject (privacy by design). Such a safety feature might also be considered to have been incorporated in the drafting of the IPA 2016. During written evidence to the Joint Committee on the draft Investigatory Powers Bill the Home Office noted that there were no proposals being brought forward for the retention of third-party data.[81] Although there may have been no such proposals (when in fact there were),[82] third-party data retention is still possible. Third-party data is described as 'information that's collected by an

[72] ibid, 257.
[73] ibid.
[74] D. Rushit, E. R. Sowells Boone, and K. Roy, 'Efficient Data Privacy and Security in Autonomous Cars' *Journal of Computer Sciences and Applications* 7(1) (2019): 31-36. doi: 10.12691/jcsa-7-1-5, 32.
[75] Gasson et al., (n 70).
[76] ibid, 260.
[77] ibid.
[78] R. van der Hilst, (n 67), 35.
[79] K. Michael and M.G. Michael, 'The Social and Behavioural Implications of Location-Based Services' (2011) 5(3-4) *Journal of Location Based Services* 121, 132.
[80] Open Rights Group, 'Cashing in on Your Mobile? How Phone Companies are Exploiting their Customers' Data' (4 March 2016) <https://regmedia.co.uk/2016/04/04/cashinginonyourmobile.pdf>.
[81] Joint Committee on the Draft Investigatory Powers Bill, written evidence, (n 182), Home Office, para 2, p. 491.
[82] Written evidence submitted by GreenNet (IPB0063), para 7.

entity that doesn't have a direct relationship with consumers'[83] or anyone.[84] Or more specifically, where 'one telecommunications operator is able to see the communications data in relation to applications or services running over their network, but where they do not use or retain that data for any purpose.'[85] As noted above, s. 87(4)(d) of the IPA 2016 allows third-party data to be retained if it is used or retained for a lawful purpose. Moreover, this can be imposed on telecommunications operators via s. 87(9)(b)(i) by requiring them to process data for the purposes of retention. iiNet (in an Australian context) argued that data retention would force commercial businesses to become agents of the state in storing and safeguarding large databases they have no business need to do so[86] (as noted above). This is certainly true for UK businesses when one considers that data generated can be obliged. Section 46(2) of the IPA 2016 allows any business (s. 46(4)(a)) to conduct interception if it constitutes a legitimate practice reasonably required for the purpose, in connection with the carrying on of any relevant activities for the purpose of record keeping. Subsection 2(b) indicates that this includes communications relating to business activities. Due to being vaguely defined, this essentially allows interception for 'business purposes' which would fit with the Home Office's narrative in 2009 when, in respect to Deep Packet Inspection, it identified that '… many communications service providers currently identify and obtain communications data from their networks for their business purposes.'[87] If Regulations are made for business purpose interception, s. 87(4)(d) would not apply because this would constitute a lawful purpose for retention. Consequently, this could allow interception of data and its retention[88] unsuspectedly, highlighting again the severity of interference and that third-party data actually can be retained.

A further concern is of generated communications data. An ICR would need to be generated in order to be retained, this however, does not limit the possibilities for other data to be retained. As techUK noted, 'a CSP may be required to generate data about the location of its users and then store that data purely for the purposes of law enforcement.'[89] Moreover, s. 87(9)(b) can place requirements for *obtaining* (including by generation) data for the purpose of retention. Smith asked the question as whether this could mean that a telecommunications operator could obligate a customer or third-party to generate data so it could be obtained and retained.[90] Telecommunications operators could be obligated to conduct traffic and social network analysis and data mining[91] either to be obtained or generated for retention purposes, increasing the severity of interference.[92] This may be particularly concerning given that even in 2014, 'Jim Farley, the Global Vice-President of Marketing and Sales at Ford [Motors], told

[83] J. Marshall, 'WTF is Third-Party Data?' (5 February 2014) <https://digiday.com/media/what-is-third-party-data/>.
[84] J.F. Houpert, 'What You Need to Know About 1st, 2nd and 3rd Party Data' (20 June 2017) <https://www.datacratic.com/blog/first-second-third-party-data>.
[85] Explanatory notes for the IPA 2016, para 262.
[86] iiNet, 'Limited Submission to the Committee' <http://www.aph.gov.au/DocumentStore.ashx?id=cd64d063-5791-4336-8606-0ee36926b8f9&subId=206461>.
[87] Home Office, 'Protecting the Public in a Changing Communications Environment, Summary of Responses to the 2009 Consultation Paper' <http://webarchive.nationalarchives.gov.uk/+/http:/www.homeoffice.gov.uk/documents/cons-2009-communication-data/cons-2009-comms-data-responses2835.pdf?view=Binary>, p. 15.
[88] Joint Committee on the Draft Investigatory Powers Bill, written evidence, Open Rights Group, para 125, p. 1104.
[89] ibid, techUK, para 25, p. 1268.
[90] G. Smith, (n 47), para 28; G. Smith, 'Illuminating the Investigatory Powers Act' (22 February 2018) <https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html>.
[91] L. Feiler, 'The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection' (2010) 1(3) *EJLT* <http://ejlt.org/article/view/29/75>.
[92] ibid.

participants of the Consumer Electronics Show: "We know everybody who oversteps the law, we know when you're doing it. We have GPS in your auto, so we realize what you're doing."'[93] Furthermore, section 87(9)(b) can also impose requirements for the processing of data for retention.

The title for Part 4, which contains the retention powers, refers not to the retention of relevant communications data, but to *certain data*. This implies that retention is not limited to relevant communications data. Given that s. 87(9)(b) does not refer to relevant communications data but just 'data,' it may be possible that telecommunications operators could be obliged to obtain/generate and retain data as defined in s. 263(1). The only example given is that of ICRs, but it is clear that s. 87(9)(b) would not be limited to them. For example, it could force zero-logging[94] Virtual Private Networks (VPNs)[95] to now log data by way of generation for the purposes of retention. This would effectively defeat the purpose of their existence (to prevent internet histories from being stored and the masking of locations). This means that communications data can still be more intrusive than what is considered 'content.'

The consequence is that given the broad definitions in the IPA 2016, and despite privacy by design being a feature of EU law which should form part of OEMs production of connected vehicles, CAVs continue to produce rich data in volumes which are subject to retention and access by state authorities for a range of purposes, not all of which can be justified. It is in the generation and access of these data, created by CAVs and facilitated by the IPA 2016, where concerns regarding a new form of surveillance society, one of the mobile panopticon, emerge.

COMMUNICATIONS DATA MORE INTRUSIVE THAN CONTENT?

Communications data have often been distinguished from the content of communications. Content is usually described as what is *within* a message such as the body of an email or conversation over a telephone.[96] Section 261(6) of the IPA 2016 defines content as any element of the communication or data logically associated with which reveals anything of what might reasonably be considered the meaning of the communication. Section 261(6)(a) and (b), however, consider inferences[97] that can be drawn from communications do not equate to content, neither does systems data[98] as set out in s. 263(4).[99] Systems data is described as data which may be used: to identify, or assist in identifying, any person, apparatus, system or service; to identify any event; or to identify the location of any person, event or thing.[100]

[93] R. Dave, E.R. Sowells Boone, and K. Roy, 'Efficient Data Privacy and Security in Autonomous Cars' (2019) 7(1) *Journal of Computer Sciences and Applications* 31, 32.
[94] No web information collected to provide to law enforcement.
[95] Cryptmode, 'Best No Logs VPN' (25 March 2017) <https://cryptmode.com/best-no-logs-vpn/>.
[96] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092 (Admin), [13].
[97] Explanatory notes to IPA 2016, para 728.
[98] Which means any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following—(a) a postal service; (b) a telecommunication system (including any apparatus forming part of the system); (c) any telecommunications service provided by means of a telecommunication system; (d) a relevant system (including any apparatus forming part of the system); (e) any service provided by means of a relevant system.
[99] The explanatory notes to IPA 2016 incorrectly refers to s. 264 for the definition of systems data, para 729.
[100] Explanatory notes to IPA 2016, para 735.

National courts have demonstrated a tendency to acknowledge that interception of content is more intrusive than access to communications data.[101] This is also, and not surprisingly, the position of various law enforcement agencies e.g. the National Crime Agency, police forces,[102] and Government Communication Head Quarters.[103] The ISC acknowledged that communications data makes it possible to build a richer picture of an individual, but they were of the opinion that it was significantly less intrusive than content.[104] The then Home Secretary likened the newly defined ICRs as the modern equivalent of an itemised phone bill.[105] In *Schrems*, the Court of Justice of the European Union (CJEU) maintained that the legislation permitting public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of Article 7 of the Charter of Fundamental Rights (Article 8 of the ECHR's corresponding right).[106] In contrast, the CJEU in *Digital Rights Ireland* held that data retention does not adversely affect the essence of Articles 7 and 8 (data protection) because it does not permit the acquisition of knowledge of the content of the electronic communications as such.[107] The essence of the right (which may be similar to the 'very substance of the right')[108] is adopted from the jurisprudence of the European Court of Human Rights (ECtHR).[109] The ECtHR has used the essence of the right for various Convention Rights[110] and therefore, there is no reason why this could not be adopted for the interpretation of Article 8. Though not defined, Hoyano indicates that it may mean that there is an absolute indispensable core to the right which cannot be impaired regardless of the circumstances of any particular instance.[111] The ECtHR in *Uzun v Germany*[112] considered that surveillance via GPS interfered less with Article 8 than interception of phone calls. This was used as justification by the Investigatory Powers Tribunal in *Liberty v GCHQ* to maintain that interference with communications data was not as serious as interception.[113]

The ECtHR's decision in *Uzun* that surveillance through a vehicle's GPS tracker is an infringement of Article 8, but not a breach because other forms of surveillance 'disclose more information on a person's conduct, opinions or feelings'[114] is surprising. Similar issues have been discussed in a US context (and admittedly after the *Uzun* ruling) by jurists including Justice Sonia Sotomayor. Sotomayor, in *United States v Jones,*[115] explained how 'Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is

[101] *Davis*, (n 96), [81]; *Liberty and Others v Government Communication Head Quarters and Others* [2014] UKIPTrib 13_77-H, 5 December 2014, [34], [111], [114].
[102] D. Anderson, 'A Question of Trust, Report of the Investigatory Powers Review' (June 2015, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>, para 9.30.
[103] ibid, para 10.40(c).
[104] Intelligence and Security Committee, para 143(V).
[105] T. May, 'Home Secretary: Publication of Draft Investigatory Powers Bill' (4 November 2015) <https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill>.
[106] Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECR-I 650, [94].
[107] *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238, [39-40]. The High Court took the same approach in *Liberty v Secretary of State for the Home Department and Others* [2018] EWHC 975, [3].
[108] *Geotech Kancev GMBH v Germany* App no. 23646/09 (ECHR, 2 June 2016), [51].
[109] L. Hoyano, 'What is Balanced on the Scales of Justice? In Search of the Essence of the Right to a Fair Trial' (2014) 1 *Criminal Law Re*view 4, 11.
[110] ibid.
[111] ibid, 15.
[112] *Uzun v Germany* App no. 35623/05 (ECHR, 2 September 2010), [66].
[113] *Liberty and Others*, (n 101) [34], [111], [114].
[114] at [52].
[115] *United States v Jones* - 565 U.S. 400, 132 S. Ct. 945 (2012). Available at https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

susceptible to abuse.'[116] Specifically in relation to something as simple as GPS, which has been significantly superseded through the data tracking capabilities of CAVs, she continued that 'making available… such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track… [might] alter the relationship between citizen and government in a way that is inimical to democratic society.'[117] With CAVs, a certain amount of data production, collection, collation and retention will be known by the driver. This includes the most basic of data from features such as the satellite navigation system, contacts list associated with their connected mobile phone and so on. This element of overt surveillance, of knowing that they are being watched and monitored, has the power to curtail freedom of movement and even to 'assure that individual behavior conforms to societal norms.'[118] This might extend to the recording of individuals within their vehicle, thereby affecting their actions such as smoking, drinking, using a handheld mobile phone and so on.[119]

However, of more serious concern is perhaps the covert surveillance possible with CAVs and the recording and use of personal information. This is performed away from the driver, undertaken remotely and secretly so the driver does not appreciate what data is being taken, for what purpose and how it might be used. Tesla vehicles create and send to various bodies vast and detailed personal and environmental data (content and communications data). As noted above, this is in some instances with the driver's consent but in many others, without. There is also the incentive for drivers to allow data to be sent remotely to ensure the safety and functionality of the CAV. Regardless of which method is used, they facilitate surveillance of individuals (targeted surveillance) and of groups (mass surveillance). Targeted surveillance enables the identification of a person and, with use of a CAV and their smartphone, monitoring of communication and movements. To achieve this, the user is often sold on the premise of the convenience of the devices being connected which provides assistance (including troubleshooting) features that might be appreciated. For example, the navigation system in a user's car offering to locate a nearby service station when the fuel tank/battery warning is triggered. Such vehicle tracking systems, when the data are communicated beyond the vehicle, has been held as unconstitutional in the US (*United States v Jones*)[120] without the issuing first of a warrant. Of course, our discussion differs from the US context as we consider the law of England and Wales with the IPA 2016, yet similar information accessed by the state in *Jones*, in its unencrypted state, is accessible in the UK and available for state agencies to access. The data could then be tracked, subject to longitudinal analysis, and held by third-parties, before being available on request to be handed over to state agencies for examination.

On a more intrusive scale is the possibility of mass surveillance. Users of CAVs could find that collated communication data may be collected to establish models of behaviour and to create profiles of users, establish more effectively how drivers and/or their vehicles behave in various conditions and to determine whether CAVs in autonomous modes replicate these accurately. On a mass surveillance scale, it is not simply the vehicle itself and its data that may be used, it is the data created from the external communications between the vehicle and sources on the highway and with other CAVs. Usually mass surveillance is covert so as not to affect the

[116] ibid, 3.
[117] ibid, 3-4.
[118] Glancy, (n 20), 1208.
[119] Such actions have also been attributed to negatively affecting individuals' psychological health as it will reveal journeys of a distinctly private nature, see *People v. Weaver*, 12 N.Y.3d 433, 441–42 (2009) as quoted by Sotomayor in *United States v Jones*, op. cit., (n 115), 3.
[120] *United States v Jones* (n 115).

patterns of human behaviour being recorded. But it can be overt, as Bentham explained in the Panopticon Prison. For instance, speed cameras may be established which record vehicle license plates, the speed of the travelling vehicle and even pictures of the driver. These devices are used to deter unlawful behaviour but operate to control all drivers who enter their scope. As Glancy puts it, autonomous vehicles now operate as a 'mobile panopticon,' moving along roads and literally taking in all details about what is going on in the areas through which the vehicle travels.[121]

One argument presented against the possible intrusiveness of the data collected and shared from CAVs has been the establishing of VPNs. Indeed, the CAV OEMs are adopting VPNs to protect the public connections CAVs will make between other vehicles and infrastructure. Not all VPNs respect privacy, and furthermore,[122] under Part 4 of the IPA 2016, as noted earlier, it is possible that those organisations operating VPNs could be compelled to generate data, thus destroying anonymity. It is accepted that anonymity must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.[123] However, the general nature of retention powers, as *Breyer* notes, interferes with anonymity[124] (by even impeding or eliminating it)[125] on a scale that cannot be compared to *KU v Finland*[126] which concerned the anonymity of an individual. Notably, the ECtHR held that on occasion Articles 8 and 10 must yield to other legitimate imperatives[127] and this was seized upon by the Home Office to justify blanket indiscriminate data retention as envisaged in the draft Communications Data Bill.[128] At the ECtHR, it was noted in *Breyer* (in a reference to *Rotaru*)[129] that anonymity has been traditionally linked to the protection of personal data.[130] Worryingly, the Chamber of the ECtHR ruled that an obligation on companies to identify all phone users was compatible with Article 8.[131] In effectively eradicating anonymity, the Chamber's ruling is in contrast with the Grand Chamber (GC) in *Delfi* where it was noted that 'Anonymity has long been a means of avoiding reprisals or unwanted attention.'[132] Judge Ranzoni's dissent brings strong arguments for a referral to the GC and a CJEU ruling that follows that of the Advocate General may help them revisit many of the arguments that succeeded before the Chamber.[133] It also needs to be recognised that deanonymisation of data is possible through algorithms that take microdata and can re-identify, and to a high probability, the human traces therein.[134] This is also possible through the

[121] Glancy, (n 20) 1215.
[122] https://www.techradar.com/uk/vpn/best-no-logs-vpns-to-stay-private-and-anonymous.
[123] See *Delfi AS v Estonia* App no. 64569/09 (ECHR, 16 June 2015), [149].
[124] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016], [24].
[125] L. Mitrou, 'Communications Data Retention: A Pandora's Box for Rights and Liberties?' in A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati (ed) *Digital Privacy: Theory, Technologies, and Practices* (Auerbach Publications 2007), 426.
[126] *KU v Finland* App no. 2872/02 (ECHR, 2 December 2008).
[127] ibid, [49].
[128] Home Office, Draft Communications Data Bill (Cm 8359, 2012), 97.
[129] *Rotaru v Romania* App no. 28341/95 (ECHR, 4 May 2000).
[130] *Breyer v Germany* App no. 50001/12 (ECHR, 30 January 2020), [5].
[131] ibid.
[132] *Delfi AS*, (n 123) [147].
[133] D. Naranjo, 'ECtHR: Obligation on companies to identify all phone users is legal' (3 February 2020) < https://edri.org/ecthr-obligation-on-companies-to-identify-all-phone-users-is-legal/>.
[134] S. Gambs, M. O. Killijian, and M. N. del Prado Cortez, 'De-anonymization Attack on Geolocated Data' (2014) 80(8) *Computer and System Sciences* 1597.

processing of background knowledge and the cross-correlation with other databases to re-identify individual data records.[135]

As Schneier asserts, communications data gives us context,[136] and context matters because it gives us meaning.[137] It has been noted that the effect of communications data 'is that a very comprehensive dossier on an individual's private life can be produced (including contacts, where he or she has been, is, or will be going, and his or her interests and habits).'[138] This opinion has also been endorsed by the German Constitutional Court'[139] and AG Saugmandsgaard Øe in *Tele2 and Watson* where it was maintained that risks associated with the access to communications data may be greater than access to the content of communications.[140] This is because communications data is structured, making it more suitable for aggregation and analysis. Furthermore, content can be disguised more easily through encryption[141] or using coded language.[142]

ALTERNATIVES TO SURVEILLANCE AND THE INVESTIGATORY POWERS ACT 2016

Data retention creates harm which, when assessed in respect of its proportionality to the severity of interference, is detrimental. For instance, and as has already been raised, it is the 'the fear of being watched or eavesdropped upon [that] makes people change their behaviour, even behaviour that is not illegal or immoral.'[143] Feiler questioned whether social minorities (based on political views, income class, religion, or other factor) feel pressured to assimilate to the mainstream, so as to not raise any suspicions regarding their behaviour.[144] van der Hilst[145] and York[146] have both noted how wide-scale communications data retention can have a severe chilling effect on freedom of association 'which is a loss for the democratic functioning of society.'[147] The chilling effect on rights exercised under Articles 8-11 and Article 2 Protocol 4 can lead to what Schep coins as 'social cooling' because 'the long-term negative side effects of living in a reputation economy' results in everything being remembered.[148]

Solove noted that the value of protecting against chilling effects is not measured simply by its effects on individuals exercising their rights, but its harms to society because among other

[135] A. Narayanan, and V. Shmatikov, 'Robust Deanonymisation of Large Sparse Datasets' (2008) *In Security and Privacy* 111. IEEE Symposium.
[136] B. Schneier, 'Security vs. Privacy' (29 January 2008), <https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html>, 17, 26.
[137] P. Tompkins, and J. Lawley, 'Context Matters' (5 April 2003). <http://www.cleanlanguage.co.uk/articles/articles/205/1/Context-Matters/Page1.html>.
[138] N. Taylor, 'Policing, Privacy and Proportionality' (2003) *European Human Rights Law Review* 86, 97.
[139] *BVerfG*, judgment of the First Senate of 02 March 2010 - 1 BvR 256/08 - Rn. (1-345), [227].
[140] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Watson* [2016] ECR I-572, Opinion of Saugmandsgaard Øe, [259].
[141] P. Bernal, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1(2) *Journal of Cyber Policy* 243, 248.
[142] Joint Committee on the Draft Investigatory Powers Bill, written evidence, P. Bernal, para 3.9, p. 132.
[143] R. van der Hilst, 'Human Rights Risks of Selected Detection Technologies: Sample Uses by Governments of Selected Detection Technologies' (2009) Available at <http://www.detecter.bham.ac.uk/D17.1HumanRightsDetectionTechnologies.doc> p. 20.
[144] Feiler, (n 91).
[145] van der Hilst, (n 143).
[146] J. York, 'The Harms of Surveillance to Privacy, Expression and Association' (2014) Available at <https://giswatch.org/en/communications-surveillance/harms-surveillance-privacy-expression-and-association>.
[147] van der Hilst, (n 143).
[148] T. Schep, 'Data Leads to Social Cooling' Available at <https://www.socialcooling.com/>.

things 'they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.'[149] In addition to the severity of the interference with an individual's rights to privacy and data protection, it can also be argued that the changes in society, potentially resulting from a constant surveillance, are contrary to the public purpose.[150] For instance the ECtHR found violations of Articles 10 and 11 in *Segerstedt-Wiberg and Others*[151] despite actual harm not being demonstrated.

Further, and as noted with regards to OEMs establishing CAVs with 'privacy by design', we have noted how the definition of telecommunications operator and communications data allowed retention notices to be issued on essentially anything that can communicate, whether it be a CAV or an IoT object to retain essentially any type of data, including Big Data. The term 'surveillance by design' was first coined by Thani et al[152] and for the purposes of this paper, it will be used in a different context. As Wisman notes, it only takes a few tweaks to turn CAVs into an 'unprecedented surveillance-society.'[153] Wisman continued that if data retention is applied to these devices (which it does under the IPA 2016), the 'amount of data and the level of detail will increase dramatically and will leave less space for citizens to keep information about their lives to themselves.'[154] Although Wisman refers to this as purpose creep by design, it is argued that the concept of 'surveillance by design' is more appropriate in this context because CAV use *is* surveillance[155] and if the state can compel the retention of such data generated, it only marks a shift in *who* is conducting the surveillance. Thus, this highlights that CAVs will feed 'into the surveillance apparatus of the state.'[156]

Data retention found within Part 4 (mainly s. 87) of the IPA 2016 does not satisfy any of the requirements of legality, necessity and proportionality found within the Convention Rights (Articles 8-11 and Article 2 Protocol 4). Article 6(2) and 6(3)(c) of the ECHR is potentially violated, and each of the above Convention rights are violated in conjunction with Article 14. This has been evidenced when considering data retention judgments in other EU member states,[157] the severity of interference with fundamental rights, who is obligated to retain, and therefore *what* data is retainable, to supplement ECHR arguments. Most damning of all, perhaps, is the commentary by Cobbe who argued that the IPA 2016 does not satisfy the requirements of *Tele2 and Watson* because, amongst others, retention notices can be issued in pursuit of a range of purposes other than those permitted; retention is indiscriminate; the length of the retention period is not objectively determined and limited to what is strictly necessary;

[149] D. J. Solove, ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review*, 745, 746.
[150] Feiler, (n 91).
[151] *Segerstedt-Wiberg and Others v Sweden* App no. 62332/00 (ECHR, 6 June 2006), [105], [107].
[152] S. Khalizah, S. OthmanThani, N. H. M. Hashim and W. H. W. Ismail, 'Surveillance by Design: Assessment Using Principles of Crime Prevention through Environmental Design (CPTED) in Urban Parks' (2016) Elsevier Procedia - Social and Behavioral Sciences 234, 506.
[153] T. Wisman, 'Purpose and Function Creep by Design: Transforming the Face of Surveillance through the Internet of Things' (2013) 4(2) *European Journal of Law and Technology* Available at <http://ejlt.org/article/view/192/379>.
[154] ibid.
[155] J.M. Porup, 'The Internet of Things is a Surveillance Nightmare' (20 March 2016) Available at <http://kernelmag.dailydot.com/issue-sections/staff-editorials/16196/internet-of-things-surveillance-nightmare/>.
[156] Wisman, (n 153).
[157] M. White, 'Protection by Judicial Oversight, or an Oversight in Protection?' (2017) 2(1) *Journal of Information Rights, Policy and Practice* 1, 2.

and the IPA 2016 does not provide clear and precise rules governing the scope and application of retention.[158]

Ultimately, what the IPA 2016 does is to infringe individuals' human rights in a manner which is disproportionate to achieving its aims. The requirement of adopting a 'least restrictive measure' approach as noted by Brems and Lavrysen[159] and by the ECtHR in *Nada v Switzerland* necessitates that for a measure to be proportionate and necessary, the possibility of recourse to a less damaging measure to fundamental rights which fulfils the same aim *must* be ruled out.[160] It was in *Glor v Swtizerland*[161] where the principle, as a general rule, was established, regardless of the Convention provision invoked and regardless of the context of the case.[162] Further, ECtHR case law is more certain on the principle's efficacy when considered in a surveillance context. Thus in *Klass*, the ECtHR accepted that German law confined secret surveillance to where there were factual indications of suspicion of serious crimes, where other measures were without the prospect of success or considerably more difficult, thus preventing *general surveillance.*[163]

A measure in the alternative to data retention is 'data preservation.'[164] Data preservation, also referred to as *quick freeze* and *freeze plus* refers to communications data which are temporarily secured relating only to specific suspects of criminal activity which may subsequently be made available to law enforcement authorities following judicial authorisation.[165] It is a position preferred by the Council of Europe and is articulated in Article 16 of the Budapest Convention,[166] which despite criticisms,[167] the UK ratified in 2011. It has been argued that data preservation is likely to only affect 1% of the population,[168] and therefore is less intrusive to privacy[169] and other fundamental rights in terms of the scale and number of people it affects. It is also considered to be equally as effective.[170] Yet such an approach is not without its critics,

[158] See Cobbe, (n 18).
[159] E. Brems and L. Lavrysen "'Don't Use a Sledgehammer to Crack a Nut": Less Restrictive Means in the Case Law of the European Court of Human Rights' (2015) 15 *Human Rights Law Review* 139, 140.
[160] *Nada v Switzerland* App no. 10593/08 (ECHR, 12 September 2012), [183].
[161] *Glor v Switzerland* App no. 13444/04 (ECHR, 30 April 2009), [94].
[162] Brems and Lavrysen, (n 159) 155.
[163] *Klass and Others v Germany* App no. 5029/71 (ECHR, 6 September 1978), [51].
[164] C. Walker and Y. Akdeniz, 'Anti-Terrorism Laws and Data Retention: War is Over?' (2003) 52(2) *Northern Ireland Legal Quarterly* 159, 177; The Czech Republic Constitutional Court 2011/03/22 - Pl. ÚS 24/10, [55].
[165] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) (2011) Available at <http://www.statewatch.org/news/2011/may/edps-opinion-eu-mand-ret-opinion.pdf> [54].
[166] Council of Europe's Convention on Cybercrime ETS No. 185, 23.XI.2001; I. Brown, 'Communications Data Retention in an Evolving Internet' (2010) 19(2) *International Journal of Law and Information Technology* 95, 107; European Digital Rights 'Shadow Evaluation Report on the Data Retention Directive (2006/24/EC)' (17 April 2011) Available at <https://www.edri.org/files/shadow_drd_report_110417.pdf>, p. 6; All Party Parliamentary Internet Group, 'Communications Data: Report of an Inquiry by the All Party Internet Group' (January 2003) Available at <https://www.cl.cam.ac.uk/~rnc1/APIG-report-commsdata.pdf>, [108].
[167] Walker and Akdeniz, (n 164); J. Fisher, 'The Draft Convention on Cybercrime: Potential Constitutional Conflicts' (2001) 32 *University of West Los Angeles Law Review* 339; Article 29 Working Party, 'Opinion 4/2001 On the Council of Europe's Draft Convention on Cyber-crime' Available at <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp41_en.pdf>.
[168] Open Rights Group, 'Digital Surveillance' Available at <https://www.openrightsgroup.org/assets/files/pdfs/reports/digital-surveillance.pdf> accessed 20 November 2020, p. 47.
[169] European Data Protection Supervisor, (n 165), [56].
[170] *Mouvement Raëlien Suisse v Switzerland* App no. 16354/06 (ECHR, 13 July 2012).

having been referred to as futile,[171] and 'wholly impracticable.'[172] Yet it would be for the ECtHR to consider the reasonableness of the national authorities' choice between a slightly more effective measure that is more detrimental to individual interests and a rather less effective, but one which is also a less restrictive provision.[173] Whether the UK will reconsider the scope and powers provided for in the IPA 2016 remain to be seen, but alternatives do exist and are more respectful of fundamental human rights. CAVs are a source of significant data, personal to the driver/person in charge, but much more importantly, aggregated to communities and types of user which might be called upon by the state for examination. It would seem unlikely that given the complexity and richness of the data contained in these devices, their increasing use and development over time, their increasing presence in communities, and the ability to extract information from the exterior of the vehicles, thus covering a much more compelling area than presently available through CCTV, that the state would change the IPA 2016 and curtail access to these sources. Perhaps in a post-Brexit, post-Covid UK, the matter will be reconsidered nationally and by the ECtHR.

CONCLUSION

With the enactment of the IPA 2016, potential personal and mass privacy breaches are advancing, this is being aided through the sophistication and increasing prevalence of CAVs. As such vehicles become more commonplace, as the convenience they offer becomes more mainstream and relied upon, they may become like smartphones – ubiquitous items which people use on a daily basis yet so often forget about the potential it has for tracking movements. Still, they are arguably more dangerous than smartphones as, inter alia, they allow the surveillance of groups, and vulnerable groups in particular understand the potential for abuse through the tracking of their activities by state agencies. CAVs have the potential for monitoring individuals beyond the scope of those who use them, their cameras can establish a detailed view of the local environment, and the IPA 2016 can require communications operators to maintain the data produced by CAVs for later interception. It can require VPNs to maintain the data produced and each, on a micro and macro scale, can be used to track individuals (and groups) and interfere with their human rights.

The movement to CAVs, beginning with the UK government's aim to restrict new car sales to electric (and thus more likely to be CAV) vehicles by 2030, will exacerbate this infringement of individuals' privacy and human rights. Perhaps the old maxim 'if you've got nothing to hide then you've got nothing to fear' might be an apt strapline for CAV manufacturers in the future.

[171] Walker and Akdeniz, (n 164) 177.
[172] *Davis & Ors*, (n 96) [70].
[173] J. Gerards, 'How to Improve the Necessity Test of the European Court of Human Rights' (2013) *I•CON* 11:2 466, 479, 484.