BULK SURVEILLANCE IN THE DIGITAL AGE: RETHINKING THE HUMAN RIGHTS LAW APPROACH TO BULK MONITORING OF COMMUNICATIONS DATA

Authors: Pete Fussey & Daragh Murray (Pete Fussey is a Professor in the Department of Sociology at the University of Essex, Dr. Daragh Murray is a senior lecturer in the School of Law at the University of Essex. This work was supported by the Economic Social and Research Council, grant number ES/M010236/1. The authors would like to thank the anonymous peer reviewers for their helpful comments. The authors are available for contact at pfussey@essex.ac.uk and d.murray@essex.ac.uk respectively.)

ABSTRACT

The digital age has brought new possibilities and potency to state surveillance activities. Significant has been the advent of bulk communications data monitoring, which involves the large-scale collection, retention, and subsequent analysis of communications data. The scale and invasiveness of these techniques generate key questions regarding their 'necessity' from a human rights law perspective and they are the subject of ongoing human rights-based litigation. This article examines bulk communications data surveillance through a human rights law lens, undertaking critical examination of both the potential utility of bulk communications surveillance and – drawing on social science analysis – the potential human rights-related harm. It argues that utility and harm calculations can conceal the complex nature of contemporary digital surveillance practices, rendering current approaches to the 'necessity' test problematic. This paper argues: that the distinction between content and communications data be removed, that analysis of surveillance-related harm must extend beyond privacy implications and incorporate society-wide effects, and that a more nuanced approach to bulk communications data be developed. Suggestions are provided as to how the 'necessity' of bulk surveillance measures may be evaluated, with an emphasis on understanding the type of activity that may qualify as 'serious crime'.

Keywords: communications data, bulk surveillance, human rights, Snowden, chilling effect

1. INTRODUCTION

The digital age has sparked a fundamental transformation in state surveillance, both in terms of how surveillance is conducted and the type of insights it is intended to facilitate. This transformation is exemplified by the use of bulk communications data techniques,[1] which involve the large-scale collection, retention, and subsequent analysis of communications data.[2] These techniques have now become an integral feature of state surveillance. For instance, UK Intelligence and Security Services report that the use of bulk communications data is 'essential',[3] and a key tool in fulfilling their obligation to protect human rights. Others, however, have highlighted the potential for serious human rights concerns,[4] particularly with respect to rights such as the right to privacy, the right to freedom of expression, the right to freedom of assembly and association, and the prohibition of discrimination. While improved intelligence capabilities can unquestionably facilitate the fulfilment of state obligations with respect to the protection of life and public order, interference with the aforementioned rights has the potential to undermine both individual rights and the effective functioning of participatory democracy.[5]

This article examines bulk communications data surveillance through the lens of human rights law, drawing on social science perspectives to further analyse potential harms and impacts. In doing so, the article recognises limitations in comprehensively addressing all of the component parts of this issue. By nature, and as discussed below, exhaustive analysis of this highly dynamic area is problematic. Indeed, it is precisely these limitations that challenge the applicability of current human rights law tests. In response, this article highlights several core issues to draw out the inherent complexities, and to discuss how bulk communications data surveillance can be

[1] Also referred to as 'metadata', for further discussion see Section 2 below.
[2] See, for example, parts 4, 6 and 7 of the Investigatory Powers Act 2016 (UK).
[3] Government of the Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 1.7 (Operational Case).
[4] In the digital age, individuals produce a significant quantity of communications data. This can be used to make revealing inferences about specific individuals, providing insights into, *inter alia*, their health, sexual orientation or political affiliation. See further below Sections 2 and 5.1.
[5] See in this regard, ECtHR, *Szabo and Vissy v. Hungary*, App no 37138/14, 12 January 2016, para. 57; ouncil of Europe Commissioner for Human Rights, 'Democratic and effective oversight of national security services' (2015) 57.

understood, approached, and addressed going forward. This paper argues that the human rights law approach to bulk communications surveillance should be refined and proposes key considerations that should be taken into account. The focus is on bulk surveillance practices as they relate to domestic populations. Exclusively externally-focused surveillance raises relevant issues, but poses distinct questions, particularly in relation to the impact of any 'chilling effect'. This type of activity is not discussed herein.[6]

Although this is an issue of global interest, the UK Investigatory Powers Act 2016 and the case law of the European Court of Human Rights and the Court of Justice of the European Union are used herein for illustrative purposes.[7] The Investigatory Powers Act establishes a legal basis for advanced modern surveillance techniques, and so provides an appropriate framework to address the issues under discussion.[8] Equally, the process surrounding the adoption of this Act resulted in the production of a number of reports analysing bulk techniques, as well as comments by intelligence and security agencies. These provide significant insights. Mass surveillance techniques have also been actively litigated before European courts in recent years, and a number of high-profile cases are currently pending. As such, these courts have dealt with the issue at a greater frequency, and in greater detail, than other human rights bodies. To-date, the issue of bulk surveillance has not been comprehensively addressed from a human rights law perspective, and no specific guidance exists at the international level. This article intends to contribute to emerging understandings as to how to approach this issue.

[6] See, in this regard, Asaf Lubin, '"We Only Spy on Foreigners": The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance' (2018) 18 Chicago Journal of International Law 2, 502; Ashley Deeks, 'An International Legal Framework for Surveillance' (2015) 55 Virginia Journal of International Law 2, 291.

[7] This article does not intend to analyse the Investigatory Powers Act, or its compliance with human rights law requirements. Rather, it is presented as an example of modern domestic legislation regulating advanced surveillance practices. For further information on the Act itself, see Simon McKay, *Blackstone's Guide to the Investigatory Powers Act 2016* (OUP 2017).

[8] Other European surveillance regimes are discussed in European Union Fundamental Rights Agency, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU', Volume I: Member States' legal frameworks (2017).

Human rights law typically applies a three-part test to assess the legitimacy of surveillance measures.[9] First, does a legal basis exist under domestic law, and is this legal basis of sufficient quality to protect against arbitrary interference with individuals' rights? Second, does surveillance pursue a legitimate aim? Third, is the surveillance necessary in a democratic society, i.e. does it answer a pressing social need and is it proportionate to the legitimate aim pursued?[10] Evaluating the legal basis, and the quality of this legal basis, is dependent on the specific legal framework applicable in a given jurisdiction, while intelligence and security services uses of surveillance measures typically satisfy the legitimate aim test on the basis of protecting national security or public order.[11] As such, and to examine the specific human rights issues raised by the bulk collection of communications data at a more universal level, this article will focus on the third part of the human rights law test: evaluating the necessity in a democratic society of bulk communications surveillance. This requires an examination of both the potential utility,[12] and the potential human rights-related harm, of this practice. To facilitate an understanding of the core issues, this paper is organised over four areas of discussion. Section 2 begins by discussing the nature of communications data, and briefly highlighting some relevant human rights law issues. Sections 3 and 4 then engage in an initial discussion of how bulk communications data techniques may be seen through existing formulations of utility and harm.

Section 3 advances the argument that effective assessment of utility is increasingly challenged in its ability to capture the complexity of contemporary digital surveillance practices. In particular, this is because access to specific information demonstrating utility is circumscribed – often legitimately – by national security concerns, while there

[9] See, ECtHR, *S. and Marper v. the United Kingdom*, App nos 30562/04, 30566/04, 4 December 2008, para. 101.
[10] This is broadly similar to the test established in relation to the ICCPR and the American Convention on Human Rights. In these treaties reference is made to necessity and proportionality, but not always to the test of necessity 'in a democratic society'. See, for instance, the discussion of necessity in Human Rights Committee, General Comment No. 34, 'Article 19: Freedoms of opinion and expression', 12 September 2011, UN Doc. CCPR/C/GC/34.
[11] See, for example, ECtHR, *Weber and Saravia v. Germany*, App no 54934/00, 29 June 2006, paras. 103-104.
[12] i.e. how 'useful' bulk surveillance techniques are, in light of the legitimate aims pursued.

is also a more general sense of opacity concerning the instrumentality and impact of digitally generated data. This means that an accurate utility assessment is difficult to achieve. Nonetheless, the benefits associated with bulk practices should not be summarily dismissed. Section 4 examines the other side of the equation, drawing on social science analysis of surveillance to indicate the direct and indirect harms linked to bulk monitoring. However, as with utility, this section argues that although factors indicating harm do exist, the precise identification of, for example, a chilling effect, is difficult to achieve. Ultimately, the challenges associated with examinations of utility and harm raise pressing questions regarding the appropriateness of the human rights law test, as currently applied, and highlight the need for further transparency in relation to claimed utility, and further consideration of – and research into – the broader human rights harms, including at the societal level.

In an effort to resolve this issue, Section 5 argues that any analysis regarding the 'necessity' of bulk communications data surveillance should take into account: (a) the extent of information revealed by communications data, (b) the extent to which harms associated with retained communications data affect a broad range of rights, (c) the ease at which communications data can be subject to analysis, and (d) the utility of bulk communications data to law enforcement and intelligence agencies. On the basis of these factors it is proposed first that communications data be regarded as equivalent to content data, and second that human rights law should adopt a more nuanced approach to the issue of 'mass surveillance'. In order to take advantage of the utility associated with bulk communications data surveillance techniques, while mitigating the full range of associated harms, a clearer and stricter understanding of the types of activities to which bulk techniques may be applied is required. This section provides guidance as to how the 'necessity' test can be applied in the context of bulk surveillance, addressing how current broadly conceived notions of 'serious crime' can be revised.

2. UNDERSTANDING COMMUNICATIONS DATA?

The term 'communications data' (or 'metadata') refers to all of the information associated with a communication, apart from the actual substance of the communication.[13] A frequently used example suggests that communications data consists of the information on the outside of an envelope, while content data relates to the information contained within the actual letter. However, this analogy does not reflect the true nature or extent of communications data in the current era, or the fact that it can be just as invasive as content data. The widespread integration of technology into everyday life, coupled with increasing digitisation, means that individuals produce significant amounts of communications data in the course of a normal day.[14] This information can reveal extensive insights, such as a near comprehensive record of an individual's movements, who they communicate with, how frequently, and for how long. Communications data is not restricted to conventional communications – such as phone calls, emails, or messaging – but also includes communication between computers and Internet browsing histories.[15]

Communications data is deemed particularly useful to the intelligence and security services when combined and aggregated to produce a near-comprehensive record of an individual's communications and Internet-based activity.[16] Such data is used to find patterns in, or characteristics of, communications that may indicate involvement in a threat to national security or the commission of a crime,[17] or to construct a more generalised 'intelligence picture' of a particular subject. In particular, communications data can be used to uncover the composition of a network, potential hierarchies within

[13] The UK High Court classified communications data into three broad categories: subscriber data, service data, and traffic data. See, *David Davis and others v. Secretary of State for the Home Department* [2015] EWHC 2092, 17 July 2015, para. 13.
[14] For instance, normal use of a smart phone will indicate the user's location history, the identity of everyone they communicate with (over email, phone, or messaging), the time and duration of this communication, and their Internet search history.
[15] See, for example, Section 61, Investigatory Powers Act 2016 (UK); 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue', 17 April 2013, UN Doc. A/HRC/23/40, para. 15.
[16] The utility of bulk communications surveillance is discussed in greater detail in Section 3 below.
[17] David Anderson, Independent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, p. 129.

that network, and a series of related yet non-obvious relationships. This information can also be used to develop revealing individual profiles.[18]

Advances in the collection, storage, collation and analysis of communications data have transformed the extent of detail that can be exposed. As noted by the European Advocate General, the use of such data makes it possible to 'create both a 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 personal identity.'[19] The Special Rapporteur on Freedom of Opinion and Expression similarly noted that:

> When accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of an individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone. By combining information about relationships, location, identity and activity, States are able to track the movement of individuals and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with.[20]

For intelligence agencies, the benefit of communications data over content-based information may be demonstrated by the following (simplified) example. If a state agent wishes to identify all those individuals who attended a particular protest march, or all those who oppose government policy in relation to a specific issue, they may attempt to do so using content-based information, but this would require considerable

[18] For example, computational science research has consistently demonstrated how a only a few partial scraps of data can be merged to reveal a comprehensive picture of someone's identity. This includes the sufficiency of only four spatio-temporal points to identify 95% of both an individual's identity *and* their unique travel patterns (see de Montjoye *et al*., 'Unique in the Crowd: The privacy bounds of human mobility', 3 *Nature Scientific Reports*, (2013) 1).

[19] Opinion of Advocate General Saugmandsgaard Oe, Case Nos. C-213/15 & C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, (CJEU, 19 July 2016) para. 253.

[20] 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue', 17 April 2013, UN Doc. A/HRC/23/40, para. 42.

resources.[21] However, a cursory search of retained communications data will immediately reveal all those who were at the location of the protest march during the identified timeframe, and all those who contacted a particular opposition group (by phone, message, email, or by visiting a website), and will also instantly provide further information, such as how frequently this contact occurred. Those individuals who fall into all of the specified categories may then be quickly, indeed almost instantaneously, identified.[22] In addition to revealing information about an individual's political opinion or participation, communications data can also be combined, analysed and used to infer other highly sensitive personal information, such as an individual's health status, position in a social network, political affiliation, financial situation or sexual orientation.[23]

Bulk communications data surveillance refers to the large-scale collection and retention of communications data – as opposed to the targeted collection of such data[24] – and is today employed by both intelligence and law enforcement agencies.[25] For instance, the UK Investigatory Powers Act allows the Secretary of State to require domestic telecommunications operations to retain communications data for a period of up to 12 months.[26] The retention of communications data may be requested in relation to a broad range of objectives including: 'the interests of national security', 'for the purpose of preventing or detecting crime or of preventing disorder', or 'for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department'.[27] As

[21] This is partially due to the complexity associated with understanding and accurately analysing speech, and the difficulty in effectively automating this practice.

[22] See Opinion of Advocate General Saugmandsgaard Oe, Case Nos. C-213/15 & C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, (CJEU, 19 July 2016) paras 257-259.

[23] V. Mayer-Schoenberger and K. Cukier, *Big Data. A Revolution that will transform how we live, work, and think* (John Murray 2013).

[24] i.e. the collection of communications data relating to a specific individual, initiated on the basis of a reasonable suspicion that that individual is engaged in criminal activity.

[25] See *inter alia* David Lyon *Surveillance after Snowden* (Polity Press 2015).

[26] Section 87, Investigatory Powers Act 2016 (UK). If this retained data is accessed by the intelligence and security services, and therefore becomes 'operationally relevant', it is possible that it may be retained by these agencies for significant periods of time and, also, potentially reassembled into new forms in the future thus ensuring a more enduring legacy. This may be a loophole in existing legislation, such as the UK Investigatory Powers Act, that has the effect of facilitating the retention of communications data for significantly longer than envisaged in the legislation.

[27] Sections 61(7)(a), (b), (f) Investigatory Powers Act 2016 (UK) (respectively).

telecommunications operators are the principal providers of Internet access, the Act allows for collection of information relating to virtually all individuals within the jurisdiction.

The retention of bulk communications data, in and of itself, constitutes an interference with the right to private life,[28] and the right to freedom of expression.[29] In order to determine whether this interference is legitimate or results in a violation of human rights law the three-part test developed by the European Court of Human Rights must be applied.[30]

3. BULK COMMUNICATIONS DATA SURVEILLANCE AND CLAIMED UTILITIY

Evaluating the utility of bulk communications data surveillance is a complex task, and two key difficulties must be highlighted. First, information relating to state surveillance activity remains necessarily restricted, and this factor is heightened in the national security context, despite increased transparency and scrutiny in recent years.[31] Second, it is somewhat difficult to identify the specific contribution of bulk communications data surveillance to particular operations. In this regard, and in one of the few authoritative public sources available on these activities, the UK Independent Reviewer of Terrorism Legislation noted:

[28] See, ECtHR, *Barbulescu v. Romania*, Judgment, App no 61496/08, 12 January 2016, para. 36.

[29] The European Court of Human Rights examined the right to private life and freedom of expression together in ECtHR, *Telegraaf Media Nederland Landelijke Media BV and Others v Netherlands,* App no 39315/06, 22 November 2012, para. 88. The European Court of Justice similarly discussed both privacy and expression in Cases C-203/15, C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deprtment v. Watson and others*, (CJEU, 21 December 2016) paras. 92, 93. For further discussion on the content of the right to freedom of expression, see Human Rights Committee, General Comment No. 34, 'Article 19: Freedoms of opinion and expression', 12 September 2011, UN Doc. CCPR/C/GC/34.

[30] A similar test is applied when evaluating compliance with the International Covenant on Civil and Political Rights. See, Human Rights Committee, General Comment No. 34, 'Article 19: Freedoms of opinion and expression', 12 September 2011, UN Doc. CCPR/C/GC/34, para. 22.

[31] See, for example, Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016; David Anderson, Independent Reviewer of Terrorism Legislation, 'Report of the Bulk Powers Review', August 2016; David Anderson, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015; Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court', 23 January 2014.

> Cause and effect in this area are not always straightforward: indeed it will only rarely be possible to attribute a successful outcome solely to the exercise of a particular power. In almost every scenario to which I have been introduced, both in the course of this Review and in several years of reviewing counter-terrorism operations … [a] mosaic of different information sources is classically involved in identifying a target or threat.[32]

While acknowledging these complexities, the current human rights law approach nonetheless necessitates that efforts be made to identify the particular benefit of this surveillance practice: this examination of utility is essential to determining whether the techniques are 'necessary'. To analyse these issues effectively, we acknowledge a key distinction between the related themes of 'use' and 'utility'. 'Utility' in this sense constitutes a more value-laden assessment of the worth of these distinct and potential 'uses'. As such, the following four areas of discussion first explore attributions of use as expressed by those operating and overseeing these techniques. Here, reports by the UK Intelligence and Security Services,[33] the UK Independent Reviewer of Terrorism Legislation,[34] and others, indicate that the use and utility of bulk data communications surveillance relates to, *inter alia*: mapping of activity and network composition, pattern identification, resource efficiencies, and the ability to 'look into the past'. While implicit in these discussions, the fifth area of discussion engages in more detailed analysis of utility and the claims made for the operational value of these measures.

[32] David Anderson, Independent Reviewer of Terrorism Legislation, 'Report of the Bulk Powers Review', August 2016, para. 4.12.
[33] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 1.7.
[34] David Anderson, Independent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, para. 9.28.

3.1. Mapping of activity and network composition

The collection and retention of bulk communications data allows intelligence and security services to create a map of all – or nearly all – communications activity. This map may be used to determine the composition of a particular organisation or network, identify previously unknown persons of interest, develop partial intelligence leads, link anonymous profiles to real world identities, or note changes in communications activity that may be suspicious.

For example, if certain members of a criminal organisation are known, examining a map of communications activity will indicate all those users that the suspect individuals communicated with, and the relationship between them. This can be used to identify the membership of a particular network or group.[35] Importantly, this process may flag individuals previously unknown to the security services. Further analysis of these individuals' communications can then be used to infer whether they themselves are suspect. For example,

> The security and intelligence agencies' analysis of bulk data uncovered a previously unknown individual in 2014, in contact with a Daesh-affiliated [ISIS] extremist in Syria, who was suspected of involvement in attack planning against the West. As this individual was based overseas, it is very unlikely that any other intelligence capabilities would have discovered him.[36]

This form of analysis may also be initiated on the basis of sparse information, as the ability to place even limited information within a near comprehensive communications data set may well indicate other avenues for investigation. In this regard, intelligence leads

> […] might indicate that a British extremist who travelled to join Daesh in Syria in late 2014, whose full name is not yet known, is trying to make

[35] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 5.6.
[36] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, p. 28.

> contact with a group of known extremists back in a particular region in the UK. The intelligence might indicate that the group potentially has access to firearms, and may be planning an attack.[37]

In such cases, the analysis of data obtained in bulk is frequently the only means of identifying those involved.[38] Further analysis may also indicate key individuals within a network. For instance, communications patterns may identify a hierarchy amongst the members, or interlocutors through which a high percentage of communications pass through. The ability to examine individual users in the context of all communications activity also facilitates the identification of 'anonymous' users.[39] Individuals may use specific software or practices to hide their identity. However, by placing the communications activity of an anonymous user within the entire pool of communications activity, patterns or overlaps may be identified.

3.2. Pattern identification

Bulk communications data can be analysed to identify suspicious patterns of behaviour. Unlike mapping-related activity, which depends on previously identified information,[40] this form of analysis is more proactive, and is used to generate new intelligence and to reveal (or 'surface') individuals, devices, etc. worthy of further investigation. For instance, it can be used to flag specific users engaged in 'suspicious' patterns of communications activity, such as visiting specific websites, communicating with certain persons, using particular forms of communication, searching for particular terms online, following accounts, or 'liking' posts on social media sites. These individuals may then be prioritised for further investigation. For example, in relation to social media the UK security and intelligence services state they:

[37] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 5.3.
[38] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, paras. 5.2, 5.3.
[39] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016. 3.13.
[40] For instance, a specific individual, or a suspect's device.

> […] use bulk communications data and bulk personal datasets to gain vital insights into the plans of those plotting against the UK, and to understand the connections between individuals. These capabilities frequently provide one of the only sources of information at the early stages of an investigation.[41]

This pattern analysis may also be used to search for suspect means of communication and applied for cybercrime as well as counter-terrorism operations. In this regard, it is reported that:

> In 2010, an intelligence operation identified a plot which came right from the top of al-Qaida: to send out waves of operatives to Europe to act as sleeper cells and prepare waves of attacks. The intelligence specified unique and distinctive communications methods that would be used by these operatives. GCHQ, in partnership with many other countries, was able to identify operatives by querying bulk data collection for these distinctive patterns. This international effort led, over a period of months, to the arrest of operatives in several European countries at various stages of attack preparation – including one group literally *en route* to conducting a murderous attack.[42]

3.3. Resource efficiencies

Analysis of retained communications data may facilitate more efficient resource utilisation by reducing the number of personnel required to conduct physical surveillance,[43] or by discounting potential avenues of investigation. For instance, if UK security services identify a suspected member of the Islamic State, but that individual does not communicate with anyone within the UK, they may accordingly be

[41] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 3.17.
[42] David Anderson, Independent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, p. 337.
[43] See, for instance, *Carpenter v. United States*, 585 US _ (2018), p. 12.

discounted as a threat to the UK (and perhaps passed on to other intelligence services) thereby freeing up resources to focus on UK-specific threats.[44] This ability to discount potential avenues of investigation can also accelerate investigative processes: 'enabl[ing] the security and intelligence agencies to narrow down likely targets much more quickly, so that they can focus limited investigative resources where it is really needed.'[45] The intelligence and security services state that access to retained communications data facilitates this process, as it removes the need to make individual requests, or a series of such requests: '[b]y using bulk communications data, links can be established that would be impossible or significantly slower (potentially taking many days) to discover through a series of individual requests to communications service providers. This can sometimes be the difference between identifying and disrupting a plot, and an attack taking place.'[46]

3.4. Retained communications data: The ability to 'look into the past'

All these methods of interrogating retained communications data benefit from the ability to look into the past,[47] and several specific benefits may be highlighted. First, in the event of a crime, retained data allows the security services to 'rewind' events, facilitating the identification of suspects and a better understanding of what happened. For instance, if a body is found in waste ground and murder is suspected, analysis of retained data may indicate individuals present at the location where the body was found, and enable investigation of their prior activity.[48] Second, retained data allows analysts to 'look back' and immediately identify a suspect's pre-existing network. It is argued that this ability is particularly important in the context of foreign

[44] In the US context, see Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT ACT and on the Operations of the Foreign Intelligence Surveillance Court', 23 January 2014, p. 146.
[45] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 9.6.
[46] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 9.5.
[47] National Research Council of the National Academies, 'Bulk Collection of Signals Intelligence: Technical Options', 2015, p. 57.
[48] i.e. through smartphone location data.

intelligence activities.[49] Third, pattern identification is heavily dependent on accessing retained data.[50] Fourth, access to retained data facilitates speedier investigations, as the data is immediately available in full, and access is not dependent upon targeted requests. For example, the UK Intelligence and Security Services report that:

> Following a failed terrorist attack in London in 2007, the security and intelligence agencies were able to confirm that the perpetrators were the same as a group who had carried out another attack shortly afterwards. This was achieved in a matter of hours through the analysis of bulk communications data, and was vital in understanding the scale of the threat posed in a fast-moving post-incident investigation, because of the ability to identify connections at speed; it would not have been possible to do this at speed by relying on requests for targeted communications data.[51]

Additionally, it is important to note that a wide range of other agencies claim utility in the retention and analysis of bulk communications data. Indeed, in the UK, the same legislation legitimating intelligence and security services' use of this data – the 2016 Investigatory Powers Act - has enabled other non-security-focused agencies to access, and retain access to, such information.[52]

[49] National Research Council of the National Academies, 'Bulk Collection of Signal Intelligence: Technical Options', 2015, p. 52.
[50] This is particularly useful in the cyber defence context.
[51] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, p. 41.
[52] For example, the UK police and Crown Prosecution Service are reported as highlighting three benefits of retained data:
(a) Conspirators become more guarded in their use of communications as the moment of a crime approaches. Older data may therefore be the best evidence against them.
(b) It may be relatively easy to arrest the minor players in a drugs importation or smuggling ring. But by going through their historic communications data, it may become possible to trace the bigger players who have taken care to remain in the background.
(c) A time lapse between the incident and the identification of a suspect will mean that old data is needed, David Anderson, Independent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, para. 9.45.

3.5. Examining the utility of bulk communications data surveillance

In terms of the utility of bulk communications data surveillance in practice, recent UK Intelligence and Security Service releases of information and statistics report that bulk communications data has:[53]

- 'played a significant part in every major counter terrorism investigation of the last decade, including in each of the seven terrorist attack plots disrupted since November 2014';[54]
- 'been essential to identifying 95% of the cyber-attacks on people and businesses in the UK discover by the security and intelligence agencies over the last six months' [to 2016];[55]
- 'been used to identify serious criminals seeking to evade detection online, and who cannot be pursued by conventional means, supporting the disruption of over 50 paedophiles in the UK in the last three years';[56]
- been used 'in 95 per cent of serious and organised crime prosecution cases handled by the Crown Prosecution Service Organised Crime Division and has been used in every major Security Service counter-terrorism investigation over the last decade';[57]
- played a significant role in terrorism prosecution: 'The CPS reviewed a snapshot of recent prosecutions for terrorist offences and concluded that in 26 recent cases, of which 17 have concluded with a conviction, 23 could not have been pursued without communications data and in 11 cases the conviction depended on that data.'[58]

[53] For further examples highlighting the utility of retained data provided by the French Government, see Opinion of Advocate General Saugmandsgaard Oe, Case Nos. C-213/15 & C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, (CJEU, 19 July 2016) para. 183.
[54] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 4.5.
[55] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 1.8.
[56] Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, para. 1.8.
[57] Government of the United Kingdom, 'Operational case for the use of communications data by public authorities', n.d., p. 5.
[58] David Anderson, Independent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, para. 9.22.

Despite these broad claims of utility it is difficult to examine the *specific role* and *degree of influence* played by bulk communications data surveillance, given the limited publicly available information. From a human rights law perspective, the issue is not whether bulk communications data surveillance is useful, but rather whether it is 'strictly necessary in a democratic society', including whether it is 'strictly necessary […] for the obtaining of vital intelligence in an individual operation.'[59] Although this test was applied to content and not communications data, it suggests that should the European Court of Human Rights specifically address bulk communications data surveillance it may examine whether these techniques constitute a 'vital' part of an operation.

The case studies released by the UK Intelligence and Security Services raise a number of questions regarding the useful/vital nature of bulk techniques. For example, the *Operational Case for Bulk Powers* presents a case study relating to a terrorist attack being planned in Northern Ireland, where it was suspected that the terrorists 'had already obtained explosives for the attack and were escalating their activity.'[60] In this instance, it was reported that:

> Bulk communications data provided the breakthrough. Through interrogation of the data, the security and intelligence agencies found previously unknown members of the network and were able to increase their coverage of the expanded group. As a result they became aware of a sudden further increase in activity from analysis of the group's communications activity. This led to police action and the recovery of an improvised explosive device.[61]

This example gives rise to questions regarding the 'vital' role played by retained communications data. If a number of the suspected terrorists were known, this

[59] ECtHR, *Szabo and Vissy v. Hungary*, App no 37138/14, 12 January 2016, para. 73.
[60] 'Case Study: Protecting Northern Ireland' in Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, p. 39.
[61] 'Case Study: Protecting Northern Ireland' in Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, p. 39.

indicates that targeted surveillance could have been initiated. This would facilitate the mapping of the network (by monitoring who the known individuals communicate with), and the monitoring of the groups' communication patterns (facilitating, for instance, identification of hierarchies), without resort to retained bulk communications data. Similarly, the 'preventing a kidnap' case study relates to a plot by known terrorists to stage a kidnapping.[62] As the terrorists were known, surveillance could feasibly have been initiated with respect to their devices.

A similar analysis may be applied to the drug smuggling ring example provided by the UK Police and Crown Prosecution Service.[63] While it may be faster to identify 'the bigger players who have taken care to remain in the background'[64] using retained communications data, the same result could be achieved by the initiation of surveillance targeting identified 'minor players'. The 'vital' role played by retained communications data in these operations is difficult to demonstrate.

Ultimately, the case studies presented by the UK Intelligence and Security Services demonstrate the important role played by retained bulk communications data. They do not, however, unequivocally demonstrate that these measures were strictly necessary, or vital to all of the operations in question.[65] Two points may be made. First, in certain of the case studies, it is not clear that the same outcome could not have been achieved by initiating targeted surveillance of specific individuals, devices, etc. Second, in other cases the benefit appears to be speed and efficiency.

Accordingly, it is possible that a Court may not regard bulk communications data techniques as vital and therefore find them to be incompatible with international human rights law. Such a conclusion, however, risks simplifying a more complex reality. It is difficult to draw a bright line distinction between those intelligence techniques that are merely useful and those that are vital. An approach that fails to

[62] 'Case Study: Preventing a kidnap' in Government of the United Kingdom, 'Operational Case for Bulk Powers', 2016, p. 40.
[63] David Anderson, Independent Reviewer of Terrorism Legislation, 'A Question of Trust: Report of the Investigatory Powers Review', June 2015, para. 9.45.
[64] David Anderson, Independent Reviewer of Terrorism Legislation, 'Report of the Bulk Powers Review', August 2016, para. 9.30.
[65] Of course, evidence of a vital role may be present but restricted on national security grounds.

take these difficulties into account risks ignoring factors such as the benefit of developing an overall intelligence picture. As highlighted by the UK Independent Reviewer of Counter-Terrorism Legislation:

> '[c]ause and effect in this area are not always straightforward: […] A mosaic of different information sources is classically involved in identifying a target or threat, developing an understanding of the situation or taking the decision to launch disruptive action.'[66]

In particular, the embeddedness of these practices within intelligence work renders it difficult to conduct a post-operation review to identify which specific components of the operation contributed to a successful outcome. An operation will necessarily draw on myriad available techniques, and it is exceptionally difficult to know which will be effective in advance. In this context, serious consideration must be given to the intelligence and security services' experience, and their claims that bulk communications data techniques are 'essential'.

4. EXAMINING THE POTENTIAL HARM CAUSED BY BULK COMMUNICATIONS DATA SURVEILLANCE

This section draws on social science research and empirical evidence to examine the potential harms associated with bulk collection of communications data and seeks to progress beyond the well-worn frame of privacy costs. Any survey of surveillance harms is necessarily selective. The purpose here is not to supply a comprehensive inventory of potential impacts of surveillance.[67] Instead, it seeks to focus the discussion on a number of potential impacts resulting from the rapid spread of bulk communications data collection. Claims and counter claims are common in this contested field of debate. In order to establish clarity, social science research and

[66] David Anderson, Independent Reviewer of Terrorism Legislation, 'Report of the Bulk Powers Review', August 2016, para. 4.12.
[67] For wide ranging reviews of such impacts see Pete Fussey, 'Beyond Liberty, Beyond Security: The Politics of Public Surveillance' (2008) 3 *British Politics* 120-135; David Lyon *Surveillance Society: Monitoring everyday life* (Open University Press 2001); John Gilliom and Torin Monahan *SuperVision: An Introduction to the Surveillance Society* (University of Chicago Press 2013).

empirical evidence is drawn upon to stake a number of core areas in which potential harms of surveillance have been identified. Principal among these are: chilling effects and shifting modes of suspicion with the latter subdivided into issues of labelling and mental health. In doing so, a series of arguments are developed which gravitate towards two prominent polarities used to assess the permissibility and impact of surveillance practices.

Similar to the debates regarding the utility of surveillance, surveillance harms are highly complex and contested issues. Analysis of these debates further challenges the adequacy of utility-harm oppositions to understand the benefits and impacts of surveillance practices in the digital age.

4.1. Chilling Effects

In the context of surveillance, a chilling effect is said to arise when individuals refrain from engaging in certain forms of activity because of the perceived consequences if that activity is observed.[68] As such, any chilling effect immediately brings into play rights such as freedom of expression, freedom of association, and freedom of assembly, as it will impact upon individuals' ability to freely access information, to develop their understanding of specific issues, to engage in communication – or meet – with particular individuals or organisations, and so on. When these rights considerations are addressed at a societal level, it is apparent that a chilling effect can impact upon the effective functioning of a participatory democracy. In short, democracy is dependent upon an informed citizenry, capable of engaging with a diverse range of ideas, and of challenging the status quo. This is the essence of the 'free marketplace of ideas'.[69] It is the possibility that individuals refrain from engaging in activity perceived to be contentious that risks undermining democracy.

[68] This may include, for instance, accessing particularly information, communicating with particular individuals or organisations, attending certain events, etc.

[69] See, *Aduayom et al. v. Togo* ,Communication Nos. 422/1990, 423/1990, 424/1990, U.N. Docs. CCPR/C/51/D/422/1990, 423/1990, 424/1990 (Jun. 30, 1994), §7.4; Justice Oliver Wendell Holmes Dissenting Opinion, Abrams v. United States, 250 U.S. 616 (1919).

Potential chilling effects brought about by surveillance have long been an area of debate and scholarly interest. The origins of such inquiries are unclear but extend at least to the Watergate-era and Gregory White and Phillip Zimbardo's analysis of what they describe as the psychological breaching of the first amendment.[70] In a small study, participants were asked about their views on the legal status of marijuana consumption. These views became attenuated in significant ways depending on their likely exposure to law enforcement agencies for 'training purposes'. For those authors, 'surveillance engenders both anxiety and inhibition'[71], stimulating inhibitions and encouraging those threatened with state surveillance to 'act in ways to deindividuate themselves by increasing their anonymity and guarding their behaviour so that they don't seem "out of line"'[72]. Whilst this study is fairly small, simplistic and 'pre-digital' – and thus restricted in its application vis-à-vis understanding more complex unseen and opaque contemporary forms of surveillance – potential chilling effects have remained a prominent area of debate, and are a key focus of human rights law analysis.[73] These ideas have gained importance since Snowden's 2013 revelations. Indeed, given how the right to freedom of expression applies to more than what is merely said, but also covers a range of communications and interactions, a number of recent studies have been quick to link bulk surveillance activities to wide-ranging chilling effects on freedom of expression and association across society.[74]

However, despite such potential impacts of a surveillance-induced chilling effect on

[70] Gregory L White and Phillip G, Zimbardo 'The Chilling Effects of Surveillance: Deindividuation and Reactance' (1975) *Stanford University Technical Report prepared for the Office of Naval Research* (The Chilling Effects of Surveillance). Available at http://www.dtic.mil/get-tr-doc/pdf?AD=ADA013230 (last visited 12 October 2017).

[71] The Chilling Effects of Surveillance (n 70) 14.

[72] The Chilling Effects of Surveillance (n 70) 6.

[73] See, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin', 28 December 2009, UN Doc. A/HRCD/13/37, para. 33; Cases C-293/12 & C-594/12, *Digital Rights Ireland*, (CJEU, 8 April 2014), para. 28; Cases C-203/15 & C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deprtment v. Watson and others*, (CJEU, 21 December 2016) para. 92. Also, although a chilling effect is not directly discussed see, ECtHR, *Szabo and Vissy v. Hungary*, App no 37138/14, 12 January 2016, para. 68.

[74] Glenn Greenwald, *No place to hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Hamish Hamilton 2014); Ian Brown (2014) 'Social Media Surveillance', in R. Mansell et al. (eds), *The International Encyclopedia of Digital Communication and Society* (Wiley 2015) 1.

individual rights and the functioning of democracy, robust empirically grounded studies of this phenomenon are rare. An exception to these is a survey by the Pew Research Center.[75] In a survey of 475 adults the research identified how 34% of those aware of NSA surveillance programs had taken one or more measures to conceal their online information, while 25% stated that they had modified how they used technological platforms. Elsewhere, a survey of 520 US authors by PEN America found that many writers were worried about state surveillance and, as a result, engaged in significant levels of self-censorship.[76] According to this survey, large numbers of writers 'reported avoiding writing or speaking about particular subjects that they thought could make them a target of surveillance',[77] with 28% of participants having reduced or avoided social media and 24% consciously avoiding discussing particular topics via telephone or email. Significantly, 16% of participants stated that they have avoided writing or talking about specific topics for which they would feel scrutinised.

Despite the prominence of this theme, and the apparent – albeit limited – empirical support for its existence, identifying chilling effects is far from straightforward and existing studies are afflicted with a range of shortcomings. First is the issue of generalizability. The aforementioned studies have relied on very small sample sizes and (largely) highly specific contexts. These studies cannot claim a more general societal impact and, indeed, the generalizability of studies on chilling effects are influenced by issues of 'ecological validity', where findings from low stakes scenarios in social psychologists' laboratories face difficulties of replication in the more high-stakes and messy social world.

Second, problems exist in capturing how intentions are mobilised. For example, successfully identifying a chilling effect rests on measuring a non-event (e.g. a failure to engage in some form of activity). Also important are problems over accurately

[75] Pew Research Center, 'Americans' Privacy Strategies Post-Snowden' (2015) available at http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/ (last visited 13 October 2013).
[76] PEN America' 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor' (2013) available at https://pen.org/sites/default/files/2014-08-01_Full%20Report_Chilling%20Effects%20w%20Color%20cover-UPDATED.pdf (last visited 13 October 2013).
[77] PEN America *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (2013) 6.

measuring distinctions between one's intention to express something and the actual likelihood of articulating such thoughts.

Third, surveillance practices operate in a complex social and cultural milieu which make it difficult to isolate surveillance as the sole driver for mediating specific intentions and behaviours. Such circumstances make it challenging to identify the precise driver of any chilling effect, whether it be, for example, fear of hostile reception from a disagreeing audience, fear of a punitive sanction from more remote and invisible state agencies, or something else. Relatedly, chilling effects may be mediated by a range of subjective, social, psychological and ideological beliefs – such as belief in the legitimacy of state surveillance, levels of fear, perceived likelihood of terrorist attack, demographic location, and so on – which makes additionally complex more generalised conclusions that a censored opinion is solely related to state surveillance.

While encountering similar limitations of sample size and potential for generalization one recent study does provide a more nuanced and detailed analyses of this latter issue of socio-cultural location.[78] While small – 225 self-selecting participants (and therefore not controlled for non-response bias) – key findings reveal the highly focused impacts of chilling effects and their mediation via a range of subjective and social perceptions. Amongst the results are suggestions that it is an individual's perceived dissonance with majority opinion, rather than exposure to information about online surveillance, that most heavily influences the likelihood of someone expressing an opinion online. It is possible to thus extend this analysis to identify two major yet related implications for the consideration of surveillance chill. First, as numerous other empirical studies have pointed out, chilling effects are not generalizable, precisely because they are not felt evenly across social groups.[79] Second, and as a corollary, it is important to

[78] Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of silence Effects in the Wake of NSA Internet Monitoring' (2016) 93 *Journalism and Mass Communication Quarterly* 296-311.

[79] *Inter alia* Sidhu, D. (2007) 'The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans', *University of Maryland Law Journal of Race, Religion, Gender and Class* vol. 7(2) 375-393; Starr, A., Fernandez, L., Randall, A., Wood, L., and Caro, M. (2008) 'The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis', *Qualitative Sociology*, vol. 31(3): 251-270; Bloss, W. (2007) 'Escalating US Police Surveillance after 9/11: An Examination of Causes and Effects', Surveillance and Society, Vol. 4(3): 208-228.

recognise that it is the groups holding the fewest resources and social capital required to challenge authority that are most heavily impacted by chilling effects. This has particular relevance for any human rights law analysis as it directly relates to the ability to challenge the status quo and thus to the effective functioning of participatory democracy. It directly brings into play rights such as the right to freedom of expression, and the right to freedom of assembly.

Overall, such insights provide a corrective to crude statements that a linear path exists between state surveillance and a generalized chilling of expression. Available evidence challenges the notion that chilling effects hold a uniform and very general coarse-grained impact across the societal range. Instead, a range of variables assert themselves onto the process, attenuating their intensity, form, and prevalence.

Concerns over the ambiguity and reach of chilling effects have found expression in the courts and served to weight arguments against acknowledging surveillance harms. Perhaps most well-known among these occurred just a few months before Snowden's revelations, during the 2013 US Supreme Court defence by then NSA chief James Clapper against Amnesty International USA's challenge to FISA-authorised surveillance. Here, and citing the 1972 *Laird v Tatum* case, the Court declared that, '[a]llegations of a subjective "chill" are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm', and repeatedly stated that claims for chilling effects were 'speculative'.[80]

Nevertheless, one of the most robust analyses of chilling effects focuses on Internet usage and, co-incidentally, covers the period in which the US Supreme Court ruled on the speculative nature of surveillance chill claims. Focused on access to 48 Wikipedia articles – selected due to alignment with the keywords used by the US Department of

[80] *Clapper v Amnesty International USA*, 568 US 398 (2013). This case focused on Section 702 of the US Foreign Intelligence Surveillance Act of 1978 (FISA). A 2008 amendment allowed the Attorney General and the Director of National Intelligence (Clapper, in this instance) to collect intelligence on individuals reasonably believed to be outside of the US. Several US-located civil society groups argued that because they may be in contact with individuals subject to these surveillance measures, they might themselves become objects of scrutiny with their communications and other interactions monitored. Among other arguments, the plaintiffs argued that such surveillance activities exerted a chilling effect on their First Amendment Rights.

Homeland Security to track and monitor social media – this study sought to examine variations in related web traffic for the months immediately preceding and following the June 2013 Snowden revelations.[81] Quantifying such activity through advanced statistical modelling techniques the authors were able to demonstrate a 'large, sudden, and statistically significant drop in the total view counts' for these articles, an 'immediate drop-off of over 30% of overall views',[82] translating into a reduction of 995,085 views and suggestive of a substantial chilling effect on online searches.

Taken together, available evidence suggests chilling effects can be neither assumed in their totality, nor summarily rejected out of hand as unproblematic. Yet empirical evidence suggests that chilling effects hold complex and variegated forms and assert diverse impacts most acutely felt outside the 'mainstream'; i.e. an underlying element in why an individual modifies (or 'chills') their behaviour is to bring their activity in-line with perceived majority sentiment.. This last point is pertinent for the current discussion, given the implications with respect to individual development and democratic participation.

4.2. Reconfigured suspicion and surveillance collateral

Often expressed through a familiar trinity of justifications - that no harm is inflicted, individuals are unaware of being observed, and only the smallest fragments of meta-data are recorded – digital data collection and analysis are regularly assigned benign labels.[83] Yet it is also possible to argue that the warehousing of data associated with millions of people, almost all of whom are law-abiding and engaged in normal daily life, exerts a profound impact on how suspicion is rendered and administered. Bulk monitoring elevates millions into the realm of the potentially suspicious in a narrowed

[81] Jon Penney, 'Chilling effects: Online surveillance and Wikipedia use' (2016) 31 *Berkeley Technology Law Journal* 117-182. This study offers empirical evidence of chilling effects on online searches relating to Wikipedia articles following Edward Snowden's revelations of June 2013 and the publicity that followed. The study identifies a reduction drop in 995 085 (over 30%) of visits to Wikipedia sites that could be deemed subjected to government surveillance (such as those discussing terrorism, suicide attack, and Al-Qaeda among others).
[82] Jon Penney, 'Chilling effects: Online surveillance and Wikipedia use', 147.
[83] *Inter alia Clapper v Amnesty International USA*, 568 US 398 (2013) above.

field of enquiry. In such circumstances, suspicion does not precede data collection; i.e. surveillance is not initiated on the basis of 'reasonable suspicion'. Rather, it is generated by analysis of the data itself. As discussed below, such practices raise important questions over the role of probable cause and reasonable suspicion alongside issues of due process and the presumption of innocence.

These questions are not exclusive to the bulk monitoring of digital communications and exist in parallel to debates accompanying other technological forms of security such as the use of Automatic Licence Place Recognition,[84] thermal imaging,[85] digital facial recognition surveillance,[86] and surveillance drones.[87] Yet the scope and scale of bulk collection extends far beyond the reach of these other practices, signifying a transformation in the way suspicion is characterised.

Of key concern here is the range of activities that may be described as bulk monitoring. Whilst Snowden's exposure of GCHQ's TEMPORA programme[88] offers a picture of indiscriminate and comprehensive data warehousing, this should not be regarded as an exemplar for all forms of bulk monitoring. Common to surveillance more generally, there are gradations of intensity, with highest concentrations centred on particular populations, typically those at the margins of society. For example, NSA chain analysis is performed by analysing associations across degrees of separation, or "hops" in the intelligence vernacular. Whilst the net is wide, a filtering and triaging process is at play that necessarily focuses bulk collection activities in highly specific ways. Attention congregates most intensively at particular nodes, communities and networks, elevating specific populations into the realm of the potentially suspicious. Inevitable among these are cohabitees of identity, culture, ethnicity and territory as

[84] Samuel Nunn, 'Seeking tools for the war on terror: a critical assessment of emerging technologies in law enforcement' (2003) 26 *Policing: An International Journal of Police Strategies and Management* 454-272.
[85] Samuel Nunn, 'Seeking tools for the war on terror: a critical assessment of emerging technologies in law enforcement' (2003).
[86] Pete Fussey, 'Protecting Britain's Crowded Spaces from Terrorist Attacks: Key criminological reflections', in A. Silke (ed.) *Psychology, Terrorism and Counterterrorism* (Routledge 2010) 164.
[87] Tyler Wall and Torin Monahan, 'Surveillance and violence from afar: The politics of drones and liminal security-scapes' (2011) 15 *Theoretical Criminology* 239-254.
[88] TEMPORA was a secret GCHQ initiative that infiltrated over 200 fibre optic cables carrying internet traffic. This allowed detailed access to both the content and meta-data of enormous quantities global internet information.

well as any activist and advocacy groups that support these populations: a process we may define as 'surveillance collateral'. Overall, any boundary between bulk collection and targeted surveillance become blurred in significant ways. This will bring into play a number of human rights considerations relating, for example, to dignity, non-discrimination, and equality.

4.2.1. Labelling

Surveillance collateral may intersect with forms of chilling to assert further potential for harm. For more than half a century sociologists of deviance developed a series of influential theories identifying the complex individual responses to being labelled as an object of suspicion. Like chilling effects, the feeling that one falls into a suspect group is also sufficient to exert an influence. The processes by which this occurs are complex and debated yet include individuals internalising the label of suspicion and increasingly acting outside of the law,[89] and the ways ascriptions of suspicion act as a 'master status',[90] defining individuals as suspects above all other potential attributes. Other more focused surveillance-related research argues that a series of deeper transactions occur once someone feels they are subject to suspicion. Given the asymmetry of power relations among surveyor-surveyed interactions, this includes the communication of clear messages regarding eligibility for social inclusion and citizenship.[91] This will bring into play a number of human rights considerations relating, for example, to dignity, non-discrimination, and equality.

4.2.2. Mental health

[89] Robert K. Merton 'Social Structure and Anomie' (1938) 3 *American Sociological Review* 672-682; Edwin M. Lemert, *Social Pathology* (McGraw-Hill 1951).
[90] Howard S. Becker *Outsiders: Studies in the Sociology of Deviance* (Free Press 1963).
[91] Clive Norris and Gary Armstrong, *The Maximum Surveillance Society* (Berg 1999).

Such transactions of suspicion hold further material effects on the observed. For example, recent studies have evidenced deleterious mental health impacts among those living in communities subjected to increased police scrutiny. Moreover, these impacts are not evenly distributed among all inhabitants of targeted neighbourhoods. In one study in New York City that drew on microlevel health data of over 8000 cases, researchers found that within areas of high police surveillance activity, it is minorities living in areas of high ethno-racial diversity that are likely to experience the most significant impacts on their mental health.[92] Other related research identifies the gendered impact of such activities, with men likely to experience markedly higher degrees of psychological distress.[93] Whilst these findings largely focus on visible policing strategies in urban areas, and the implications of the extended reach of formal corrections and criminal justice into the civil domain,[94] they hold wider resonance. For example, in the national security context, research into the UK's anti-radicalisation 'PREVENT' agenda has consistently identified how those subjected to scrutiny regularly view state agencies similarly in terms of coercive potential.[95] By extension, further corollary effects of heighted suspicion and surveillance may impact on the ability of non-coercive public agencies such as social work and community-based organisations to operate effectively in these same communities. These effects raise clear concerns regarding perceived ability to engage in democratic processes.

4.3. Summary

Overall, this discussion has focused on the potential for multiple indirect and less visible harms brought by bulk collection and analysis of communications data. In

[92] A.A. Sewell and K.A. Jefferson, 'Collateral Damage: The Health Effects of Invasive Police Encounters in New York City' (2016) 93 *Journal of Urban Health: Bulletin of the New York Academy of Medicine,* 42.

[93] Abigail A. Sewell, Kevin A. Jefferson and Hedwig Lee, 'Living under surveillance: Gender, psychological distress, and stop-question-and-frisk policing in New York City'(2015) 156 *Social Science & Medicine* 1.

[94] See *inter alia* Loic Wacquant, 'The New "Peculiar Institution": On the Prison as Surrogate Ghetto' (2000) 4 *Theoretical Criminology* 377-389 for authoritative critique on the eroding boundaries between the corrections estate and heavily policed urban spaces.

[95] B. Spalek, Community Policing, trust and Muslim Communities in relation to "new Terrorism", Politics and Policy, vol. 38(4): 789-815 (2010)

addition to prominent arguments over potential chilling effects is the potential for transformations of established constructions and applications of suspicion in itself. Most obvious, perhaps, are questions over thresholds for reasonableness or probable cause along with the potential circumvention of the presumption of innocence. In such circumstances, questions are raised over whether simply engaging in certain forms of activity or communication, or a tenuous indirect association with someone worthy of suspicion, becomes sufficient to become an object of suspicion. Importantly, as discussed above, such consequences are focused heavily on marginalized communities, affecting opposition to the status quo. Labels of suspicion may assert further corollary effects that may condition the availability of life chances and the sustainability of mental health. These factors demonstrate that significant further research into the impact of a chilling effect is required and that consideration of harm must be broadened beyond an exclusive, or near exclusive, privacy focus. Quite simply, an exclusive reliance on privacy is incapable of addressing the totality of the rights implications.

5. RE-EXAMINING THE HUMAN RIGHTS LAW APPROACH TO BULK COMMUNICATIONS DATA SURVEILLANCE

The above discussion demonstrates the complexities involved in assessing potential utilities and harms associated with bulk communications data techniques. Given the significant human rights concerns involved – relating not only to the protection of individuals' rights, but also to the effective functioning of democracy itself – this is of serious concern. In particular, this uncertainty and ambiguity make effective assessment of the necessity of bulk communications data surveillance difficult to achieve.[96] In light of the risks posed by ineffective regulation, and mindful of the need

[96] See, ECtHR, *Szabo and Vissy v. Hungary*, App no 37138/14, 12 January 2016, para. 73.

to ensure the full spectrum of human rights protections,[97] a new more nuanced approach is clearly required.

In determining how human rights law could more effectively respond to bulk communications monitoring, four factors should be taken into account: (a) the extent of information that can be revealed by communications data, (b) the extent to which harms associated with the retention of communications data affects other rights, (c) the ease of analysing communications data, and (d) the operational utility of bulk collection. Each of this are addressed in turn as they provide the basis for the subsequent recommendations.

5.1. The extent of information revealed by communications data

As noted above, communications data is not benign. It can be used to reveal highly sensitive personal information including sensitive health conditions,[98] psychological wellbeing,[99] sexual orientation, relationship status, political affiliation and activist histories.[100] As the former general counsel at the NSA stated, communications data can, 'absolutely tell you everything about somebody's life.'[101]

5.2. The broad impact of bulk communications data retention on human rights

To-date, courts and human rights bodies have primarily focused on the impact of surveillance in light of the right to privacy. However, a number of other rights may be affected, and the effect on these rights may be particularly severe in the context of bulk communications data surveillance. Relevant rights include, for example, the rights to

[97] i.e. ensuring both the protection of the right to life, and the right to freedom of expression or the right to privacy.
[98] Jonathan Mayer, Patrick Mutchler and John C. Mitchell, 'Evaluating the privacy properties of telephone metadata', PNAS Early Edition, p. 5.
[99] Opinion of Advocate General Saugmandsgaard Oe, Case Nos. C-213/15 & C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, (CJEU, 19 July 2016) para. 257.
[100] Opinion of Advocate General Saugmandsgaard Oe, Case Nos. C-213/15 & C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, (CJEU, 19 July 2016) para. 258.
[101] Ian Sample, 'Even basic phone logs can reveal deeply personal information, researchers find', The Guardian, London, 16 May 2016.

freedom of expression, association, and assembly, and respect for human dignity. Importantly, although it has not addressed the issue in detail, the European Court of Justice has acknowledged that retention of communications data may affect individuals' willingness to engage the right to freedom of expression.[102]

Notwithstanding the difficulties associated with demonstrating the chilling effect, particular attention must be paid to identifying and understanding its impacts given the potentially serious consequences for both individuals and society. For example, if individuals are discouraged from engaging in their right to freedom of expression, this risks impairing the fundamental objectives underpinning the right. The right to freedom of expression is regarded as essential to, *inter alia*, individuals' development, and the effective functioning of a pluralist democracy. If individuals cannot engage in expression, or if this expression is restricted, then they cannot fully develop their identity or fully participate in the democratic process. If individuals are concerned that a state may react to certain expression, it is more likely that this concern will arise in relation to non-mainstream opinions, such as political expression, i.e. expression that may be regarded as opposing the state, the Government, or elements of Government policy. If this political expression is restricted, then the ability to oppose Government policies will be undermined. Existing research indicated that those most vulnerable to a chilling effect are opposition movements, minority groups, and those with fewest resources to challenge the status quo.[103] The effect is such that it may reproduce marginalisation and impact upon, or undermine, the basis of a pluralistic democracy; that is, the ability to debate and oppose Government policies. This risks a further, corollary, erosion of the right to freedom of expression. This line of reasoning may be straightforwardly extended to the rights to freedom of association and assembly.

---

[102] Cases C-203/15 & C-698/15,*Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deprtment v. Watson and others*, (CJEU, 21 December 2016) para. 101. See also, Cases C-293/12 & C-594/12, *Digital Rights Ireland*, (CJEU, 8 April 2014), para. 28.

[103] Sidhu, D. (2007) 'The Chilling Effect of Government Surveillance Programs on the Use of the Internet by Muslim-Americans', *University of Maryland Law Journal of Race, Religion, Gender and Class* vol. 7(2) 375-393

5.3. The ability to analyse communications data

Rights interferences caused by the bulk retention of communications data are significantly compounded by the ease with which this data can be analysed. State agents' ability to analyse communications data both removes barriers for conducting comprehensive surveillance,[104] and significantly increases the risk – real or perceived – to specific individuals. In a traditional physical surveillance context the resources required of the state to subject all those potentially of interest are simply too great. As noted in *Carpenter v. United States*:

> Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." […] For that reason, "society's expectation has been that law enforcement agents and others would not - and indeed, in the main, simply could not - secretly monitor and catalogue every single movement of an individual's car for a very long period."[105]

Bulk communications data surveillance extends the possibilities for monitoring beyond the movements of a car, to the movements of an individual, and indeed, an identification of their entire pattern of life. The possibility that individuals or groups may be subject to surveillance is therefore dramatically increased if the state can routinely monitor not just one instance of engagement with this political group, but *all* engagement, and if this information – and any other relevant data – can be accessed instantaneously with little or no resource implications.[106]

It is this ability to monitor and to analyse that makes communications data so useful to intelligence agencies. Indeed, the UK Intelligence and Security Committee noted that 'the primary value to GHCQ of bulk interception was not in reading the actual

[104] This is particularly true in relation to the significantly reduced resource implications associated with digital surveillance, compared to other techniques.
[105] *Carpenter v. United States*, 585 US _ (2018), p. 12.
[106] See, *Carpenter v. United States*, 585 US _ (2018), p. 13.

content of communications, but in the information associated with those communications.'[107] This transforms the nature of surveillance. It is no longer the case that the state can subject certain individuals to surveillance and gain relatively limited insights into their activity. Communications data surveillance makes it possible to monitor virtually all activities of all individuals, to discover and evaluate their relationship with others, and to gain profound insights into their lives.

5.4. The utility of bulk communications data collection

While the previous sub-sections have focused on the potential human rights harms associated with bulk communications data collection, in developing appropriate human rights responses it is important to highlight that the activities of the intelligence and security services do contribute to the fulfilment of states' human rights law obligations. In particular, states are subject to a positive obligation to protect rights, such as individuals' right to life and right to property, from threats posed by terrorists or other criminal organisations. Indeed, a state's failure to 'take measures within the scope of their powers which, judged reasonably, might have been expected to avoid'[108] an identified risk will result in a violation of their human rights obligation. This obligation may apply not only in relation to specific threats against identified individuals, 'but also in cases raising the obligation to afford general protection to society'.[109] In this regard, and as discussed briefly above in Section 3, bulk communications data collection can play a significant role in contributing to the fulfilment of state's human rights obligations. Although a lack of knowledge with respect to what techniques are used, and how, make this component difficult to

[107] Intelligence and Security Committee of Parliament (UK), 'Privacy and Security: A modern and transparent legal framework', 12 March 2015, para. 80.
[108] ECtHR, *Tagayeva and Others v. Russia,* Judgment, European Court of Human Rights, App nos 26562/07, 49380/08, 21294/11, 37096/11, 14755/08, 49339/08, 51313/08, 13 April 2017, para. 482.
[109] ECtHR, *Tagayeva and Others v. Russia,* Judgment, European Court of Human Rights, App nos 26562/07, 49380/08, 21294/11, 37096/11, 14755/08, 49339/08, 51313/08, 13 April 2017, para. 482.

engage with from outside, the utility of bulk communications data techniques should not be lightly dismissed.

That said, in order to ensure effective oversight and regulation, and to maintain public confidence in the state and its security apparatus, it is essential that transparency be prioritised. The professed utility of bulk measures should be more clearly demonstrated, and their necessity – or strict necessity – more clearly addressed. Public disclosure of certain activities may legitimately be restricted on the basis of national security considerations, but transparency should be the rule and secrecy the exception.

5.5. Rethinking human rights law considerations in the digital age

This paper identifies how bulk communications data surveillance can both contribute to the protection of human rights and result in human rights harm. Widespread interference with these rights may have implications both at the individual level – affecting individuals' ability to freely develop their identity and opinion – and at the societal level. The societal effect is such that these interferences may fundamentally alter the balance between the state and its citizens, potentially impairing the effective functioning of a pluralistic, participatory democracy. At the same time, the protection of individuals' rights, and in particular the right to life, is clearly and appropriately a key concern of the state. Efforts to effectively address this potential conflict are compounded by the fact that a precise analysis of utility and harm, and an identification of the specific role played by bulk communications data techniques in a given operation, is exceptionally difficult. In determining how best to move forward, two factors should be considered. First, the current distinction between content and communications data in terms of the level of rights protection should be removed. Second, a more nuanced approach to the regulation of bulk communications data surveillance should be developed.

5.5.1. Removing the (now artificial) distinction between content and communications data

To-date, courts have drawn a distinction between content and communications data, granting content a higher degree of protection. For instance, in *Maximillian Schrems v. Data Protection Commissioner* the European Court of Justice held that: 'legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life'.[110] This may be contrasted with the finding in *Digital Rights Ireland* where it was held that the retention of communications data 'is not such as to adversely affect the essence of these rights given that […] the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.'[111] This distinction was also made by the UK High Court: 'interception of content is more intrusive than access to communications data.'[112]

However, the distinction between the content of communications and communications data is no longer viable.[113] As discussed above, the insights revealed by communications data, and the ease at which this data may be subject to analysis, indicate that it is wholly appropriate that communications data and the content of communications be granted an equivalent level of protection. Not only are analyses of metadata as intrusive as the examination of content, the partition between metadata and content is in itself a spurious distinction. Much of the latter can be discerned from the former and their delineation can only be achieved through highly subjective means. Simply put, there is no meaningful distinction between the sensitivity of information revealed by content or communications data. There is increasing recognition as regards the validity of this conclusion. For instance, the European

[110] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (CJEU, 6 October 2015) para. 94.
[111] Cases C-293/12 & C-594/12, *Digital Rights Ireland*, (CJEU, 8 April 2014) para. 39.
[112] *David Davis and others v. Secretary of State for the Home Department* [2015] EWHC 2092, 17 July 2015, para. 81.
[113] See, Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harvard International Law Journal, 81, 141.

Advocate General stated that 'the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications'.[114] Similarly, and persuasively in this context, statements from various intelligence agencies indicate a prioritisation of communications data over content data.[115] At a national level, this may require modification of the existing legal framework in order, for example, to harmonise the rules applies to the acquisition, retention, and management of content data (i.e. through lawful intercept) and communications data.

Removing the distinction between communications data and content data in terms of the level of human rights protection is a first step towards a more realistic appraisal of surveillance practices. There are indications that the European human rights system is moving in this direction. For instance, in *Szabo and Vissy* the European Court of Human Rights stated that the protections established in the Court's case law – which currently focus on content interception – 'need to be enhanced'[116] in order to address bulk communications data techniques. More recently, in *Big Brother Watch and Others*, the Court stated that it was 'not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content.'[117] At the domestic level, US Supreme Court has also moved in this direction, holding in *Carpenter* that access to communications data – at least in the context of modern surveillance – required a warrant, thereby treating it as equivalent to content interception.[118]

This re-classification of communications data may raise certain challenges to bulk communications data surveillance regimes, and may require a departure from existing case law. In *Maximilian Schrems v. Data Protection Commissioner* the Court of Justice of the European Union held that 'legislation permitting the public authorities

[114] Opinion of Advocate General Saugmandsgaard Oe, Case Nos. C-213/15 & C-698/15, *Tele2 Sverige AB v. Post-och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and others*, (CJEU, 19 July 2016) para. 259.

[115]

[116] ECtHR, *Szabo and Vissy v. Hungary*, App no 37138/14, 12 January 2016, para. 70.

[117] ECtHR, *Big Brother Watch and Others v. the United Kingdom*, App nos 58170/13, 62322/14, 24960/15, 13 September 2018, para. 356.

[118] *Carpenter v. United States*, 585 US _ (2018).

to have access on a generalised basis to the content of communications must be regarded as interfering with the essence of the fundamental right to respect for private life'[119] and as such unequivocally impermissible. In *Digital Rights Ireland*, a communications data-related case, the Court reached a different conclusion:

> …even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights given that […] the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.[120]

This finding is in keeping with the existing, but inappropriate, distinction between content and communications data. Going forward, this position should be reconsidered. Any legislation permitting access on 'a generalised basis' to communications data must also be regarded as interfering with the essence of the right to privacy, and thus as unequivocally impermissible, in line with *Maximilian Schrems*. This is entirely appropriate if content and communications data are to be granted the same level of protection vis-à-vis the right to privacy. The question arises, therefore, as to what this means for bulk communications data surveillance regimes. Key in this regard is the Court's prohibition of access on a 'generalised basis', that is:

> without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail.[121]

[119] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, (CJEU, 6 October 2015) para. 94.
[120] Para 39
[121] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, (CJEU, 6 October 2015), para. 93.

This does not indicate that all bulk communications surveillance is unlawful. Rather, the legality of any bulk communications data surveillance regime will depend not only on satisfying the necessity test, but also on ensuring appropriate limitations vis-à-vis collection, access, use, sharing, detention, and so on. In *Big Brother Watch and Others* the European Court made significant steps forward in relation to safeguards,[122] although these were applied exclusively in the content of externally-focused surveillance activities. These appear to constitute an appropriate starting point, and so attention will now turn to how 'necessity' is evaluated.

5.5.2. *Developing a more nuanced approach to bulk communications data techniques: understanding what constitutes 'serious crime'*

As noted, the opacity associated with effectively measuring both the utility and harm of bulk powers renders a straightforward application of the current human rights law test problematic. To overcome these difficulties, it is suggested that a more nuanced approach is required, so that the poverty of this dichotomy, and the complexity and dynamism of the operating environment can be fully taken into account. As it currently stands, there is insufficient information in the public domain to take a position as to whether particular bulk powers satisfy the relevant human rights law test and can therefore be lawfully deployed. However, these are live issues – both in terms of legislative developments and judicial proceedings – and so it is essential that the human rights law test be clearly set out.

In developing any approach, recourse must be had to existing case law. The required standard has been set forth most clearly by the European Court of Human Rights in *Szabo and Vissy*:

[122] See, ECtHR, *Big Brother Watch and Others v. the United Kingdom*, App nos 58170/13, 62322/14, 24960/15, 13 September 2018, paras 328-347.

> A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the [sic] safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation.[123]

Two core requirements emerge from this ruling. First, the use of bulk techniques must be restricted to circumstances strictly necessary to safeguard the democratic institutions. This indicates that powers may only be used in relation to certain categories of serious crime,[124] although this requirement should perhaps be more appropriately read as safeguarding the components essential to democratic society. Second, if such powers are appropriate as a general consideration, then the strict necessity test further requirements that, at an operational level, powers must be 'vital' to an individual operation. These requirements will be discussed in turn.

In relation to the first component, it is appropriate that the use of bulk powers be restricted to only the most significant threats. As discussed above, although the harm associated with bulk surveillance is difficult to quantify, it is of a nature to undermine the effective functioning of democratic society. It stands to reason, therefore, that only threats that themselves threaten democratic society could justify such measures. However, uncertainty exists as to what crimes may be defined as 'serious' for these purposes. For instance, the European Court of Justice has referred to threats to national security and activities that will affect the monetary stability of the state,[125] while the UK Investigatory Powers Act defines serious crime as that which will result in a three year or longer custodial sentence.[126] This is a significant difference and clarity is required.[127]

---

[123] ECtHR, *Szabo and Vissy v. Hungary*, App no 37138/14, 12 January 2016, para. 73.
[124] Cases C-203/15 & C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deprtment v. Watson and others*, (CJEU, 21 December 2016) para. 102.
[125] See, Cases C-465/00, C-138/01 & C-139/01, *Rechnungshof v. Osterreichischer Rundfunk and Others,* (CJEU, 20 May 2003) para. 71.
[126] Investigatory Powers Act 2016 (UK), section 263.
[127] It is noted that the Court of Justice of the European Union effectively invalidated elements of the UK Investigatory Powers Act where access to retained communications data was for purposes deemed to fall short of 'serious crime'. The UK

Clearly, defining the specific crimes to which bulk communications data techniques may be applied is an important step. It should be based upon determining those crimes that constitute a genuine threat to democratic institutions, for which extensive powers are warranted. It should not be based on a general understanding as to what constitutes 'serious' crime. Although it is difficult to define serious crime in the abstract, the human rights law test, and the invasiveness of the measures in question, point to a high threshold. At issue, therefore, is crime that is defined as actively threatening the functioning of democratic society – for instance through attacks on or interference with democratic institutions and processes – and crime that affects the functioning of society itself, for instance through large-scale interference with the ability to live a normal life. In this regard, serious threats to national infrastructure (such as dams, power plants, or the national grid), serious threats posed by organised terrorism (such as that previously posed by the Provisional IRA), or foreign espionage, may satisfy the threshold. Other activities threatening national security should also be addressed. However, caution is required in this regard, as national security is a broad concept, and one that has been abused in the past. Rather than being regarded as a catch-all category justifying bulk powers, only those specific national security threats rising to the threshold elaborated above should be considered. This will require answering difficult questions. For instance, should the threat posed by lone-wolf attackers be distinguished from the threat posed by more organised terrorist groups?

Equally, the human rights law threshold means that other crimes, although 'serious' in terms of their gravity and impact on affected individuals, will not satisfy the required threshold. For instance, murder is unquestionably a serious crime that will result in a significant custodial sentence. However, it is not of a nature to threaten the functioning of democratic society. To reiterate, this does not suggest that those crimes that fall below the initial strict necessity threshold are not grave, or do not warrant full

Government must now present changes, and put amendments to the legislation before parliament. See, Cases C-203/15 & C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Deprtment v. Watson and others*, (CJEU, 21 December 2016) para. 125; Consultation Outcome: Investigatory Powers Act 2016. Available at: https://www.gov.uk/government/consultations/investigatory-powers-act-2016.

and effective investigation; indeed, in a large number of instances international human rights law requires that effective investigations be undertaken, and requires that the state be held to account should it fail to do so. Rather, it is a clear acknowledgement that bulk powers are particularly invasive and pose harms that may undermine or impair the functioning of democratic society. Only threats to democratic society itself can justify such measures.

The second component requires that measures be 'vital' to a specific operation. In the context of bulk powers, this is a potentially difficult test to apply as a 'mosaic' of different approaches are used in the development of intelligence or investigative profiles. Care should therefore be taken to develop an appropriately nuanced approach. It may be impossible to make a bright line distinction as to whether bulk techniques are useful or vital in specific operations. However, utility exists across a spectrum, and the nature of the role bulk powers play may be evaluated in light of the existence of alternative techniques. Essentially, this requires determining whether other (non-bulk) techniques exist, and distinguishing between those situations in which bulk powers are useful and those situations where they are 'vital'; i.e. the operation cannot proceed without bulk powers. For example, traditional or targeted techniques are arguably sufficient to murder investigations, or efforts to uncover hierarchies within domestic terrorist, drug or organised crime organisations. In these cases, although bulk techniques may be useful, proven alternative techniques exist and may be deployed. Of course, important questions do arise in relation to efficiencies generated by bulk surveillance, particularly in relation to time and costs. However, the relevance of these factors must be considered in light of the invasiveness of the techniques and it does not seem appropriate that they should be decisive for those crimes falling below the 'serious crime' threshold.

Bulk techniques may play a much more significant role in other operations. For instance, bulk techniques may be essential in relation to certain cyber security threats,

or threats from foreign-based terrorist organisations. This has been acknowledged by the European Court of Human Rights. In *Centruum for Rattvisa v. Sweden*, the European Court accepted that the operation of a bulk interception regime 'in order to identify hitherto unknown threats to national security is one which continues to fall within State's margin of appreciation',[128] while *Big Brother Watch and Others* addressed externally-focused threats and accepted, in principle, the appropriateness of bulk measures in this context.[129] In such circumstances it is for the state to demonstrate the necessity of such powers, and to detail why traditional alternatives are inadequate. In doing so, state agencies could develop a methodology for ascertaining the degree of indispensability of bulk powers in any given application. The existence, operation and credibility of this methodology could be a key focal point for oversight agencies.

Given the potential harm, resource or efficiency savings cannot provide justification, in and of themselves. It should be recalled that in situations where bulk powers cannot be justified, targeted surveillance measures may be initiated. As such, the benefits of, for example, communications data analysis are not necessarily denied to security agencies. The requirement is that such surveillance be initiated on the basis of reasonable suspicion.

6. CONCLUSION

This paper has argued for the importance of defining the specific offences to which bulk communications data techniques may be applied. Such determinations should focus on activities that constitute a genuine threat to democratic institutions, for which extensive surveillance powers are warranted. This approach recognises the utility of bulk communications data techniques, but avoids the pitfalls associated with attempting to determine the role played by such techniques in specific operations. While deliberations over acceptable thresholds for risk, and of resourcing for policing

[128] ECtHR, *Case of Centruum for Rattvisa v. Sweden,* App no 35252/08, 19 June 2018, para. 112.
[129] ECtHR, *Big Brother Watch and Others v. the United Kingdom*, App nos 58170/13, 62322/14, 24960/15, 13 September 2018, para 314.

and security agencies, will no doubt continue, clarity in this regard will also provide guidance to the intelligence and security services, and help to protect against overreach. Importantly, this approach does not create an artificial distinction between intelligence and policing activities, but instead focuses on the actual crimes or activities being combatted. Other benefits include greater operational clarity than that existing through the current understanding of the strict necessity test, which focuses on utility in specific operations. A clear onus must be placed on the intelligence and security agencies to demonstrate the strict necessity requiring the use of such exceptional and far-reaching measures.

However, human rights concerns do not end with a clearer understanding of what 'serious crime' means in this context. Access to bulk communications data and oversight must be addressed. Both of these components are essential, not only with respect to preventing abuse, but also to ensuring public confidence. In particular, if access to bulk communications data is tightly circumscribed, and accompanied by effective oversight, then the harm associated with surveillance and the chilling effect may be reduced: active surveillance will be – and will be known to be – the exception and not the rule. Human rights case law establishes a number of relevant requirements in relation to both access and oversight.[130] These will not be discussed in detail here. Instead a few foundational elements may be highlighted.

The authority to conduct bulk communications data surveillance must be limited to those situations where it is 'strictly necessary in a democratic society', and should therefore only be permissible in relation to serious crime, as defined in the above discussion. It is equally essential that access to the product of any bulk communications data programme be correspondingly restricted. In most – if not all – situations, the request to initiate bulk surveillance must be linked to a defined operation, and access restricted to that same operation. This will ensure that

[130] See, for example, ECtHR, *Szabo and Vissy v. Hungary*, Judgment, App no 37138/14, 12 January 2016, para. 77; ECtHR, *Zakharov v. Russia*, App no 47173/06, 4 December 2015, para. 233.

information collected is ring-fenced, and is not re-purposed. This would not only mitigate a range of potential surveillance harms, but may also bring ancillary benefits with regard to conformity with good practice within data protection and data management regimes. Failure to restrict access appropriately undermines or negates the requirements imposed on the initial collection, potentially resulting in an extension of exceptional powers to non-exceptional incidents.

Oversight measures provide a key means of both preventing abuse, and ensuring public confidence in the use of bulk powers. Accountability, and the role of the courts, are clearly important issues. However, it is equally essential that independent oversight bodies examine the day-to-day practice of those agencies involved in the use of bulk techniques,[131] and issue public facing reports.[132] They should ensure that procedures are followed, but also should examine how information is stored, who has access to it, how data is processed, deleted, and so on. Future research into effective access and oversight regimes could build on these insights and thus add additional weight to the 'downstream' elements of bulk data handling that exist beyond the point of collection, yet exert additional potential for harm.

[131] This was discussed in *Big Brother Watch and Others*, see conclusions reached at para. 387.

[132] The role of the Investigatory Powers Commission in this regard is interesting, and although it is too early to reach a conclusion, this body may provide insight into how effective oversight in a national security context may be conducted.