Automated Investigations: The Role of the Request Filter in Communications Data Analysis

Introduction

In the field of communications data[1] generated by mobile telephony and internet communications, and governed by the Investigatory Powers Act 2016, the 'request filter' provides for automated processing of data for use by public authorities. Promoted as a safeguard to prevent the disclosure of irrelevant communications data, the filter proposes to limit collateral intrusions by applying automated processing to the large datasets of communications data retained by communications service providers (CSPs).[2] By allowing for the processing of this data to establish connections between people and events, the 'request filter' offers a useful tool for law enforcement in the detection and investigation of crime. However, despite the proposed benefits of the filter, it remains controversial. The implementation and functionality of the filter does not occur through traditional law enforcement or other State run mechanisms. Rather, it is built and operated by the private sector and works as an intermediary device between traditional public authorities and the private companies whose data they must access. Removing public actors from the processing of data by virtue of automated filtering, poses a risk to transparency and accountability requirements underpinning the legitimacy of this mechanism, as private actors are not bound to comply with human rights instruments.[3] The collection and processing are carried out by private actors and it is questionable what liability could be assigned for any interferences. It is therefore necessary to first establish that in filtering the data, these private actors should be held liable for the potential interferences which result.

Following that, several elements of the 'request filter' are assessed to demonstrate the risk to human rights which must be taken into account when assessing the effectiveness of the instrument as a safeguard. The removal of the human element from the process does not guarantee the exclusion of biases from the system, nor from within the data sets themselves. Nor does the inclusion of an ever-expanding data pool in itself improve the abilities of law enforcement to draw meaning from the data; further analysis and interpretation is needed to effectively utilise the information disclosed by filtering. A critical analysis of the automated technologies employed for the retention and processing of communications data is therefore necessary in order to determine whether the 'request filter', as set forth in the Investigatory Powers Act, can be an effective safeguard for personal data and privacy.

This article will proceed by first assessing the development of the 'request filter' and its functionality and establishing that it is a Big Data instrument in the processing of personal

[1] Communications data is data held by a telecommunications operator or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its intended destination, describes how a person has been using a service or is about the architecture of the telecommunication system itself; Explanatory Notes to the Investigatory Powers Act 2016 ss 261.
[2] CSPs are defined as providers of a public telecommunication system, where that system exists for facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy pursuant to the Investigatory Powers Act s 261(13). These providers provide telecommunications services which include facilitating the creation, management, or storage of communications transmitted (s 261(12)).
[3] Human Rights Act 1998 s 6(5).

information.[4] Consideration is then given to the resultant issues of using this mechanism, with reference to the relevant literature. Finally, the claims of the safeguarding potential for individual data promoted by this tool are evaluated and prescriptions for improvement are offered.

The Request Filter

The 'request filter' seeks to improve the capability of law enforcement to establish connections between different people and events by analysing substantial amounts of communications data, and then filtering that information to only provide the relevant data to investigators. The communications data can then be assessed to determine links between suspects, provide exculpatory evidence, prove or disprove alibis, and so on. For example, if there were multiple murders, this tool could be used to determine what devices were near the crime scenes at the relevant times, thereby narrowing down substantially the suspect pool for investigators. Without the 'request filter' investigators would have to approach each service provider individually, with a separate authorization, and request the relevant data.[5] Each authorization must be duly approved to meet the requirements of necessity and proportionality and assure its relevance to the investigation. This traditional data request would disclose, not only the relevant data, but all other data that met the criteria of the application. The investigator would subsequently have to analyse all of the data provided to find the information needed. Such a procedure would be complex and the data would be subject to human interpretations and potential biases. This process would be time and resource intensive, which may put additional strains on the investigatory powers of the public authorities. The 'request filter' therefore offers a way to simplify complex search practices, and arguably limits the collateral intrusions into the data to those which are necessary for the limited purposes of the investigation.

1. Draft Communications Bill 2012

It is apparent that a tool such as this is of use to law enforcement and therefore easy to see why provisions for a 'request filter' have been a recurrent theme in discussions concerning communications data up to and including the passage of the Investigatory Powers Act 2016. For example, in 2008, a central government database of retained data was envisaged which would compile all the information into one easily searchable location. The communications data would be provided by CSPs but it would be stored on a Government owned and operated database.[6] This proposal was met with widespread criticism and was never implemented,[7] but the idea remained. In 2012, when considering the Draft Communications Bill, the 'request filter' was once again brought into the debate. The filter would similarly allow for the complex search of the retained data following a single request, but it would not be stored in a central database. 'So the same data is being stored about the same people and it is being stored in databases which are accessible to public authorities given powers under the Bill. The difference is that instead of one database there are many and they are privately owned'.[8] However, even though the databases would have been privately owned, the information held therein, including its format, data types, and retention length, would have been dictated by the

[4] Here Big Data is used broadly to encompass the large scale data sets which are compiled by the CSPs under the retention and collection requirements under Part 4 of the Investigatory Powers Act and then subjected to aggregation and analysis through the filtering process.
[5] Anderson D, *A Question of Trust: Report of the Investigatory Powers Review* (Stationary Office 2015) 180.
[6] Joint Committee, *Draft Communications Data Bill* (2012-13, HL 79, HC 479) 5.
[7] Travis A & Norton-Taylor R, 'Private firm may track all email and calls' *The Guardian* (London 31 Dec 2008) https://www.theguardian.com/uk/2008/dec/31/privacy-civil-liberties accessed 2 Feb 2017.
[8] See note 5 at 118 above.

Government. This led some critics to argue that the provisions in the 2012 Bill were therefore a distinction without a difference from the earlier tabled proposals in 2008; the filter could still be equated to a federated database.[9]

In order to access the 'request filter' as proposed by the Draft Communications Bill, a specified process needed to be followed. Namely, the investigator would submit a request for the filter to examine the data from multiple CSPs' databases and automatically analyse the returns, providing investigators with only the relevant data. The Secretary of State would control the filter but it would be for the CSPs to design and implement their own systems to accommodate the requests. Once this was completed, only the details of the devices active in both locations would be sent back to the investigating officer. All other data would then be destroyed in a manner that would preclude further access to the information.[10] The general maintenance and design of this system was left to the individual CSPs as the databases required specialist skills to build, update, and maintain. This system arguably ensured that the criticism present in the 2008 proposal, namely of placing the information in a central, government run database, was mitigated.

However, the proposed request system, like much of the failed Draft Communications Bill, was heavily criticised. In spite of its value as a mechanism to diminish the amount of data transferred to public authorities and thereby reduce levels of intrusion and protect privacy,[11] the proposals were rejected. Critics questioned the ability of the filter to truly provide an independent and impartial check on the processing of data when the system itself remained a function, delegated or otherwise, of the Secretary of State who was also responsible for issuing warrants and notices concerning the data.[12] Impartial governance of the system was necessary to ensure independence and this provision could not be met with the level of control exerted by the Secretary of State. Demands were made for independent audits of the use of the filter by the Interception of Communications Commissioner (IOCCO). These audits would add a level of accountability to the authorisation and access procedures governing the filter. The accountability would also be enhanced by effectively applying the requirements of necessity and proportionality before the filter could be used.[13] Yet under the Draft Communications Bill, little guidance was offered on how these specific requirements would be met in a request to filter communications data.

Accountability, it was argued, would further be enhanced by acknowledging, 'the necessity and proportionality tests need to be applied not just to the individual data streams as supplied by CSPs but to the likely effect when they are assembled together'.[14] The ability of the data to create inferences about individuals was amplified by the comprehensive nature of the data collected and retained. This could not be neutralised by the fact that the data solely related to context rather than content of communications. Professor Robin Mansell, in her evidence to the Joint Committee examining the Draft Communication Bill, noted that 'Even if conventional content is separated from other forms of information which have meaning, the expansion of opportunities for authorities to draw inferences about citizens' intention or behaviour from patterns emerging from electronic tracing of their activities is growing exponentially'.[15] These problems were further compounded by the lack of clarity concerning

[9] *Ibid*
[10] Explanatory Notes, Draft Communications Bill 2012 para 81. It is worth noting here that this provision only applied to data sent to the filter. The data would remain stored by the relevant CSPs.
[11] Home Office, *Draft Communications Data Bill Written Evidence* (2012-13) 242
[12] Sommer P, *Draft Communications Data Bill Written Evidence* (2012-13) 526.
[13] See note 5 at 126 above.
[14] See Sommer at note 12 533 above.
[15] Mansell R, *Draft Communications Data Bill Written Evidence* (2012-13) 399.

the design and maintenance of the system. The proposed processes used for filtering the data were not subject to public input nor discussion leaving the filter open to criticism. An element of transparency and scrutiny of the technical means would be required to ensure that the mechanism was being implemented appropriately. 'In the absence of clarity about this issue, authorities requesting and processing data will be continuously open to charges of bias'.[16] The problems highlighted in the development of the 'request filter' in the Draft Communications Bill largely remain under the provisions in the Investigatory Powers Act 2016 (IPA) to which discussion now turns.

2. Investigatory Powers Act 2016

Despite the failure of the 2012 Bill, the need for a system to search, analyse, and connect relevant communications data to facilitate investigations remained a priority for law enforcement. Concurrently, criticisms of the data retention regime by the Courts mandated that greater safeguards were required to ensure these information regimes limited the interferences with privacy and personal data. These two factors informed the development of the 'request filter' in the IPA. The provisions relating to the 'request filter' can be found in sections 67 to 69 which set out the method, authorizations, and limitations of the 'request filter'. Principally, access is granted under the same conditions as those set out in the 2012 Draft Bill. Section 67 provides for the powers to establish arrangements for the lawful, efficient, and effective obtaining and processing of communications data under the filter. The filter can be accessed by any listed public authority, when the test for granting access to that data has been met.[17] The filter has a limited function and can only process specified communications data as a result of a targeted communications data authorisation. A request is sent to the filter which acquires the data from the relevant CSPs and then discloses the data to those authorised to see it. The Home Office evidence for this provision attempted to distinguish it from its predecessors, noting that it would not enable those 'fishing expeditions' which were of concern in previous iterations. 'The 'request filter' is not a data mining tool or a search engine, as it can only operate on limited sets of authorised data using specified and authorised processing steps'.[18]

Whilst the requirement of a 'targeted authorisation' appears to address concerns about the potential abuse of the filter and its relative level of intrusiveness, it is questionable to what extent these concerns are effectively mitigated. The description of the requirements of the 'target' are broad; any data which is retained pursuant to the provisions of Part 4 of the IPA and any data which can be derived from this data may be 'targeted' for processing by the 'request filter'.[19] The Explanatory Notes to the Act give an example of when this power might be used in the case of IP address resolution. In such a scenario. The investigator may have details of a number of IP addresses which they believe relate to an individual. IP addresses are routinely shared between numerous individuals so it is not always possible identify a single user at a given time. The 'request filter' in this scenario would look through the data relating to each IP address to find individuals in common and relate only that information. However, in order to find such information, even more personal data must be processed, as it is not only the data relating to a specific individual which is being processed, but data which satisfies all relevant criteria. Such processing can still result in an interference for those individuals who are not under investigation, absent necessary safeguards.

[16] *Ibid* at 400.
[17] S 67 Investigatory Powers Act (IPA) 2016; relevant public authorities include not only law enforcement but additional authorities as well from groups as wide ranging as the HMRC to the Food Standards Agency.
[18] Home Office, *Joint Committee on the Draft Investigatory Powers Bill Written Evidence* (2016 IPB0146) 518.
[19] IPA 2016 s 67(2)

Some safeguards can be found in the authorisation process which consists of an application being made and approved by a designated senior officer of at least the rank of inspector.[20] It is important to note that approval by an officer here is a relatively low requirement for approval, and does not meet the requirements of independent approval typically required in the processing of personal data. Further, there is no statutory requirement that this officer be independent of the investigation for which he is reviewing the application. This potentially impacts on the impartiality of the approval process and may give rise to claims that the authorisation process is more akin to a 'rubberstamp' procedure than an effective safeguard. This officer will consider the necessity and proportionality of the application and determine whether to grant access to the filter. In assessing this, the officer must confirm that the authorisation is necessary to obtain the data for a public protection purpose or for the purpose of a specific operation, and that the conduct is proportionate to the aims of the investigations.[21] However, like its predecessor under the Draft Communications Bill 2012, little concrete guidance is offered in the relevant statutory instruments for when an application will meet the threshold for necessity and proportionality. Additional safeguards are guaranteed in the Act to ensure that no communications data can be obtained or processed for any additional purposes outside of those for which the authorisation is given. Once the information has been provided to the relevant investigator, all additional data relating to the request will be deleted from the 'request filter'; the CSPs will continue to retain the data for their normal retention period.

The Act further puts provisions in place to allow for oversight of the process, along the lines of those requested in the 2012 Bill. Data must be made available to the Investigatory Powers Commissioner (IPC) for their functions of audit and oversight.[22] Any errors in the release of information processed by the filter must be reported to the IPC as well. Security of the system is required and provisions regarding the maintenance, testing, and development of the mechanism have also been included, however, there is very little explicit detail as to the format and structure the filter will take.[23] These specifications are aimed at ensuring that the filter is subject to rigorous control.

However, many of the flaws inherent in the proposals for the 'request filter' in the 2012 Bill have been maintained in the IPA. The Secretary of State remains responsible for the establishment and maintenance of the system.[24] Therefore there remains a lack of truly impartial overall governance of the system. Similarly, there remain risks of high levels of interference due to the expansive nature of the data and relatively large pool of authorities who have access to the filter. 'Public authorities will have a permanent ability to access the 'request filter', which will make it an enticing and powerful tool that could be used for a broad range of statutory purposes. The ability to conduct the complex queries that the 'request filter' will allow for could increase the temptation…to sift data in search of relationships and infer that consequences are meaningful'.[25] Further, the farming out of the retention systems, thereby removing it from a centralised Government control, does not necessarily mitigate the potential risks from the filter. This concern is exacerbated by the fact that there remains a lack of transparency both in the development of the filter, including who is responsible for its creation and maintenance. Finally, issues with oversight remain, as despite the inclusion of the audit and error powers for the IPC, there is no requirement of

[20] IPA 2016 s 67
[21] *Ibid* at ss 68(4) & 68(5).
[22] *Ibid* at s 69.
[23] *Ibid* at s 69(6).
[24] See note 12 at 520 above.
[25] Cherry J HC Deb 14 April 2016, vol 607, col 240.

judicial approval in the authorisation process. In order to thoroughly assess the efficacy of the 'request filter' as a safeguard, these factors are now considered.

Filtering and Big Data: A Critique

The 'request filter' is only able to meet its aims by sifting and analysing large quantities of communications data and interpreting that data to determine whether it satisfies the criteria of the requests. It can be broadly classified as a 'Big Data' tool, wherein Big Data refers to the use of large data sets for predictive analysis.[26] These data sets are frequently defined as '…high-volume, high-velocity, and high-variety information assets that demand cost effective, innovative forms of information processing for enhanced insight and decision making'.[27] In the context of the 'request filter', Big Data itself is a product of technological and analytical elements. The technological aspect accounts for the development of systems and algorithms to gather, link, and compare data.[28] In the case of the 'request filter', the mechanism itself is the technological element. It is a collaborative technology which utilises filtering techniques to process information put forward by CSPs who store and retain the data. The analytical components then use the data compiled to establish the necessary connections between data points, e.g. identifying common subscriber information for multiple locations. This is where law enforcement sees the value of the mechanism; establishing linkages and patterns between disparate data points held across multiple service providers.

As danah boyd and Kate Crawford note 'Big Data is less about data that is big than it is about a capacity to search, aggregate, and cross-reference large data sets'.[29] Big Data is facilitated by the exponential increase in both data creation and technological capabilities.[30] It is not just technological capacities that are increasing, but the ability to generate meaningful data with essentially every communication and transaction in the digital age. As a result, the data gathered about people is more extensive, easier to aggregate, and able to be analysed in increasingly sophisticated and complex ways. These powers, according to Helen Nissenbaum, 'make it possible for large troves of information to be reliably, efficiently, and meaningfully organized and accessed; to be effectively moved into massive aggregations and disaggregated into usable chunks; and to be transmitted to sites when needed'.[31] These powers are clearly reflected in the creation and use of the 'request filter'

At a fundamental level, the 'request filter' allows for the analysis of a large scale data set of all relevant communications data retained under the provisions of the IPA by CSPs under notice. It does so by 'filtering' the data. Cryptanalyst and former NSA Officer William Binney describes the basic concept behind filtering: 'Filtering can occur at the point of collection, or during subsequent processing, and also occurs when analysts access bulk storage systems. Filters can be, and are, applied to exclude material or to select (include)

---

[26] Crawford K & Schultz J, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms' (2014) Boston C L R 93, 96.
[27] Information Commissioners Office, 'Big Data, artificial intelligence, machine learning, and data protection' (Report 2017) < https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 25 July 2017.
[28] Crawford K, 'Critiquing Big Data: Politics, Ethics, Epistemology' (2014) 8 Intl J of Comm 1663.
[29] boyd d & Crawford K, 'Critical Questions for Big Data' (2012) 15 Information, Communication, and Society 663.
[30] Moore's law which states that the amount of integrated circuits doubles every two years is reflective of this and ensures that massive amounts of information can now be easily stored, analysed, and interlinked.
[31] Nissenbaum H, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford U Press 2009) 37.

material'.[32] The 'request filter' is described as a mechanism to exclude material irrelevant to the investigation from being sent to the officer. In order to do so, all information which is collected under the broad retention policies of the IPA must be processed, even if that information is of no practical relevance.[33] The filter performs these processes through complex profiling queries and automated analysis of information. 'With the increased automation of data collection and analysis – as well as algorithms that can extract and illustrate large scale patterns in human behaviour – it is necessary to ask which systems are driving these practices and which are regulating them'.[34] The following examines the issues inherent in filtering a Big Data set to assess whether the 'request filter' under the IPA can truly act as a safeguard.

1. Role of Private Actors

In order to determine whether the 'request filter' can be challenged on the basis of its interference with human rights, it is first necessary to establish that the private actors who process the personal information through the filter are performing a public function when doing so and are therefore required to comply with the rule of law in this regard.

When the idea of a 'request filter' was first proposed, the aim was to retain and centrally store the relevant data on a central Government run database. This was widely criticised as it was seen to place far too much information in the hands of the Government.[35] These plans did not come to fruition and instead private actors in the form of CSPs are used to retain the data on multiple separate databases. However, there are issues with using intermediaries to run what is effectively a law enforcement mechanism. In retaining and later processing the data, CSPs are essentially fulfilling a public interest objective but are not subject to the same limitations a public authority would be in fulfilling this role. This is in part a direct result from the nature of the retention systems. The information retained in these systems largely loses its value to the CSPs due to changing business models, wherein the longer retention periods imposed upon them by the IPA diminish the value of the data they are required to hold; CSPs are also subject to limitations on use of the data, and mandatory system requirements. 'If companies no longer need to retain the data, it would seem to follow that the company is discharging a public, as distinct from a private, function in retaining it'.[36] The idea that intermediaries are acting in the public interest in this process is further demonstrated by the provisions concerning the maintenance and development of the 'request filter'. These provisions are enforced on private actors though statutory mandate, and their function and implementation is done under the direction of the Secretary of State.[37] These factors lend

[32] Binney W *Joint Committee on the Draft Investigatory Powers Bill Written Evidence* (2016 IPB0161) 182.
[33] It is worth noting here that even the processing of personal data has been held to interfere with rights and must be strictly circumscribed see Joined Cases C-293/12 & 594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] ECR I-238 paras 51-58; the courts have similarly ruled that processing of personal information does trigger concerns with regards to fundamental rights (although it is note that these are heard in the cases of private processing under the Data Protection Directive, and therefore do not necessarily apply to the processing of information for law enforcement purposes). See: C-465/00 *Österreichischer Rundfunk & Ors* [2003] ECR I-294; C-28/08 *Commission v Bavarian Lager* [2010] ECHR I-378; C-275-06 *Promusicae v Telefonica de Espana SAU* [2008] ECR I-54.
[34] See note 29 at 664 above.
[35] Notably, former DPP Ken MacDonald stated that 'This database would be an unimaginable hell-house of personal private information…No government of any colour is to be trusted with such a roadmap to our souls' in Travis A & Norton-Taylor R, 'Private firm may track all email and calls' *The Guardian* (London 31 Dec 2008) https://www.theguardian.com/uk/2008/dec/31/privacy-civil-liberties accessed 2 Feb 2017.
[36] Holmes A, 'Private Actor or public authority? How the status of communications service providers affects human rights' (2017) 22 Comm L 21, 26.
[37] IPA 2016s 69

themselves to the argument that intermediaries, in discharging these functions, can be considered 'functional public authorities' and thereby be required to comply with the human rights instruments.[38]

However, in the absence of such interpretation, using intermediaries for retention and processing which intrude into privacy and data protection, can limit the rights of individuals. Private actors are generally beyond the scope of the requisite protections of the Human Rights Act 1998 and therefore individuals have little right to redress against companies acting in a manner which goes against their interest. These companies are not statutorily bound by the obligations to comply with Convention rights and such protections are only provided through secondary instruments which lack legal force.[39] These mechanisms cannot be substituted for directly enforceable rights.[40] Therefore, using intermediaries removes a crucial element of oversight and redress for individuals whose data is captured and retained on these private databases, and then filtered for use by public authorities.

2. Interpretation of the Data

The power of Big Data mechanisms is that their increasingly sophisticated techniques allow for the development of exact descriptive and predictive meanings from seemingly unrelated points of information.[41] This analysis allows for an objective and purely informational device. Within the 'request filter' this element is promoted as a safeguard; it keeps individual investigators from abusing the powers of the filter and making inferences about the data that are informed by their own biases. If the information can be filtered without the need for human inputs and interpretation proponents argue that all that will be released will be impartial and factual results which the authorities can then use in their investigations.

However, it would be incorrect to imply that the human element can ever be fully removed from this type of data processing. All decisions, from the development of the system, to the request for access, incorporate a human element, whether it be in the design of the filter or the interpretation of the results. As such, 'data sets are not, and can never be, neutral and theory free repositories of information waiting to give up their secrets'.[42] This interpretation is critical to rebutting the presumption that automatic processing of data reduces the intrusions into personal lives. As Lawrence Busch found: 'even the most apparently obvious results require (1) a degree of interpretation (in the formation of cases, in data collection, and analysis), and (2) the weaving of a master narrative around the data'.[43] When the data is interpreted, there is an implicit decision which favours a certain type of facts or elements over others.

Within the 'request filter', the interpretation of the data is informed by human input in the selection of categories to data collected under notice, the criteria applied to the data during filtering, and the subsequent interpretation of the results. It is the Secretary of State who determines what companies to provide with a notice which will mandate the collection and retention of data.[44] This notice will also state the types of data to be retained.[45] Such

[38] See note 36 above for a fuller discussion on how these private actors can be considered functional public authorities in the collection and retention of communications data.
[39] Home Office, *Communications Data Draft Code of Practice* (2016) p 16.3.
[40] Joint Committee on Human Rights, *The Meaning of a Public Authority under the Human Rights Act (*2003-04, JL 39 HC 382)
[41] See Nissenbaum at note 31 pg 42 above.
[42] See note 28 at 1668 above.
[43] Busch L, 'Dozen Ways to Get Lost in Translation: Inherent Challenges in Large-Scale Data Sets' (2014) 8 Intl J of Comm 1727, 1738.
[44] IPA 2016 s 87.

decisions potentially bias the data set as they limit the data pool and the individuals within it. For example, retention notices under the IPA are not served on every provider of a telecommunications service operating within the jurisdiction. As such, it is not possible to determine which users of mobile telephony and internet services will be liable to be identification by the filter. Further, the interpretive bias is manifest in the forms and process themselves; applicants can specify that they want to search for one type of information over another (e.g. mobile over internet) or examine data for certain locations but not others. To an extent this interpretation is necessary in order to ensure that the filter can function in an efficient manner. The data must be circumscribed at some stage, and the human input into which data to search make this possible. However, it does mean that the promise that the data is objective and based on 'pure facts' cannot stand; if interpretation is incorporated into the decisions on what to search, certain facts will be weighted more heavily than others.

3. *Automation of the Process*

An aspect of Big Data filtering which is interrelated with the preceding concept of interpretation, is that of automation; the idea that the system can function without any unnecessary interactions with individuals who can influence the data. As opposed to the interpretation of the data discussed above which principally concerns authorizations, this element relates to the creation and process of the technological systems used to filter the data. Automation, advocates argue, enables the processing of data at speed; allows for the processing of higher volumes of data; and reduces the potential for errors being made when connecting data points. The use of automated systems thereby mitigates the need for human interaction and consequently their influences. Yet this interpretation fails to account for the technical realities of the system; technology cannot be fully removed from human input. This is readily apparent when the mechanisms used to perform the filtering functions are considered. The 'request filter' is primarily used to filter out data which is not relevant to a request made by an authorised individual (e.g. filter out location data of all cell phones that were not in both specified locations at the specified times). The request is sent to the filter, who then requests information from CSPs based on the criteria set forth in the authorisation. Once the information is provided by the CSPs, it is processed through the filter to identify relevant data points to be conveyed to the authorised party. On its face, this would appear to build a neutral element into the filter; however, this interpretation ignores the human role in shaping and developing the filter and selecting the relevant variables to be utilised by the filter in processing. Instead of removing the human element, automated systems merely transfer that element into the decision-making process itself in a manner that is more opaque.[46]

This lack of opacity is particularly significant as the filtering allows for ex post interpretations to be made and meaningful patterns to be found within the data. Indeed, the promise of these technologies is that they can produce predictions of social behaviour, thereby enabling the detection of potential criminals and national security threats. However, basing these predictions on set categories of data is insufficient to be determinative. The criteria themselves which are defined and matched, and the level of similarity necessary to determine a match has been made, is a technical engineering choice, made by designers.[47]

---

[45] *Ibid.*

[46] See note 43 above wherein Busch discusses this issue in the context of investment bank traders replaced by an algorithm which did the same work but with relatively less transparency.

[47] The Royal Society, *Machine learning: the power and promise of computers that learn by example* (Creative Commons 2017) < https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf> 92.

This is exacerbated by the idea that the more any indicator is used, the greater its apparent impact will be, both on users and data subjects, and therefore its importance may become self-reinforcing.[48] The more the communications data is searched and linked, the more influence it will have on investigations. This can lead to situations where instead of being an investigative tool used solely when necessary and proportionate, the filter will be used as a preliminary investigative tool, resulting in further intrusions into the personal information the filter is designed to limit.

Similarly, the existence of data in a system, or of matches therein, does not necessarily mean that those elements are linked. 'Too often, Big Data enables the practice of apophenia: seeing patterns where none actually exist, simply because enormous quantities of data can offer connections that radiate in all directions'.[49] Even where the patterns detected are relevant, they may not necessarily be replicated in a manner that enables efficient investigations, as linked or multiple crimes which the 'request filter' is designed to investigate(e.g. crimes occurring in multiple related locations), are relative outliers.[50] There is an additional risk that the algorithm may detect patterns which display a bias which would be unacceptable in traditional policing methods. This can occur when the 'algorithm correctly finds that a particular attribute of individuals is valuable in predicting outcomes, in contexts where society may deem use of such an attribute inappropriate'.[51] The impact of these factors can be succinctly summarized in the words of scholar Evgeny Morozov: 'Given enough data and the right algorithms, all of us are bound to look suspicious'.[52]

Further, the lack of transparency in the formation and implementation of the automated filtering technologies means that the results are not subject to independent and impartial checks. Often the processes used for the information sorting are proprietary and as a result, if the mechanism is flawed, these flaws may not be widely known. In the context of the 'request filter' the argument is that to make this information known would be to diminish the effectiveness of the filter as a tool for law enforcement; revealing the patterns that trigger identification would tip off criminals to the ways to avoid detection.[53] However, an element of oversight and transparency in the processes is necessary, particularly due to the potential for the information to impact significantly on people's lives. Without oversight, the accuracy of data which potentially makes assumptions regarding people's criminal liability, cannot be established; nor can individuals know when their information will potentially be processed and used for the purposes of the investigation and detection of crime. If these provisions are not satisfied, the process enabled by the 'request filter' cannot be said to be a sufficient check on the potential abuse of these powers in line with that required by the relevant human rights instruments to prevent undue interferences with personal data and privacy.

4. Context of the data

The lack of transparency, both for the processes which inform the design of the automated processing systems, and for the later interpretation of the filtered data, is compounded when the context of the data is altered to conform to system requirements. Context is important in

[48] Campbell's Law as set out in Campbell D, 'Assessing the impact of Planned social change' (1979) 2 Eval & Prog Planning 67.
[49]See boyd note 29 at 668 above.
[50] Solove D, *Understanding Privacy* (Harvard U Press 2008) 186.
[51] See note 47 at 92 wherein the Royal Society states that protected categories of sensitive data such as age, race, and gender, even when explicitly excluded from the algorithm may be inferred from other criteria used as predictors.
[52] Morozov E, *To Save Everything Click Here* (Penguin 2013) 189.
[53] Solove D, *Nothing to Hide: The False Trade-off Between Privacy and Security* (Yale U Press 2013) 194.

analysing data; meanings will change depending on the situation. Communications data can be used to draw meaningful inferences about people's connections to one another, about their movements, even about the strength of their relationships, but these interpretations need to be understood in a particular context to be persuasive. It is only within the known contexts that the analytic elements of the filter would be effective. Roger Clarke, posing his theory of dataveillance, described the importance of context for data. 'When the data aren't used in their original context, the probability of misinterpreting them increases greatly. This is the reason why information privacy principles place such importance on relating data to the purpose for which they are collected or used'.[54] When the data is removed from the context in which it was generated, processed, and collected, it means that the patterns and meanings derived are incomplete or lost.[55]

Yet, in the processing of data sets, this change of context is often necessary for the system to be able to function. In order for the 'request filter' to operate effectively, the data needs to be in a standardised format. This standardisation applies to the collection, analysis, and interpretation procedures. However, different business procedures and the lack of a statutorily mandated format in the legislation mean that it is possible that each CSP will retain the data in a manner designed to optimise their own aims. This will necessarily result in the data being altered so that it can be processed in the format required by the 'request filter'. Absent regulatory requirements, companies will collect and retain data in a way that remains commercially viable, even if the core purpose of the retention is to enable law enforcement. This will lead to them optimizing the quality of some categories of data over others.

Take the case of location data for example. Location data is data processed indicating geographical position of the user's equipment and potentially includes latitude and longitude, direction of travel, or the time the location information was recorded.[56] A notice served by the Secretary of State on a CSP may require that this type of data be retained and can therefore be subsequently utilised in the 'request filter'.[57] It is then up to the private actors to collect and retain the mandated information. There are several ways in which a company can do so, with varying degrees of accuracy which depend on why the information is required.

The first is utilising the GPS on the device. This generates the latitude and longitude coordinates of the user which can then be processed to generate location results.[58] This method tends to be highly accurate but is limited as it relies on satellite data to generate locations which can degrade in obstructed locations and areas with high density populations. Many core network services use GPS data to provide services to their customers and therefore location data collected by these actors will be fairly accurate. Another method companies may use to collect location data is by tracking the Wi-Fi networks a device connects to. This method tracks location to between 10-100 metres when WIFI signals are

[54] Clarke R, 'Information Technology and Dataveillance' (1988) 31(5) Comm of the ACM 498, 506.
[55] See Busch note 34 who refers to this concept as 'lossiness' 'that is, data collection and/or analysis may involve aggregation, case construction, or standardization in such a way that certain aspects of the phenomena are lost' 1732
[56] Information Commissioners Office, 'Location Data' < https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/> accessed 15 Mar 2017.
[57] IPA 2016 s 87.
[58] Hamel S, 'Case Study: Accuracy & Precision of Google Analytics Geolocation' (*Digital Analytics,* 29 Mar 2016) < https://radical-analytics.com/case-study-accuracy-precision-of-google-analytics-geolocation-4264510612c0> accessed 10 April 2017.

present,[59] making it a reliable method for determining location and one that works in more densely populated areas. The final method a private actor may use in collecting location data is via IP address tracking. This collects the data about the IP addresses a user connects to, an address which often varies significantly from the location of the user, making it much less accurate than the two proceeding methods. This method of data collection is used in mobile applications and even in the framework of core operating systems such as Google Analytics.[60] If the location data being fed into the 'request filter' differs greatly in its accuracy, it calls into question the validity of the results. Errors in determining location made by private actors in their commercial endeavours may have the end result of someone being shown targeted advertising which does not relate to them; the consequences are far more serious when the error relates to a potential criminal investigation.

Utilising information outside of the context for which it was collected has potentially negative consequences on individuals, concerns which are not mitigated by the oversight provisions of the 'request filter'. As these retention databases are a secondary use for data collected by the CSPs, there will remain a question of what format of data to optimise, with preference being given to those formats that are of most use to the private actors. This can result in collecting information, such as location data, in a way that is more commercially viable, even if it is less accurate for law enforcement purposes. Further, CSPs have little impetus to devote additional resources to ensure that the oversight and maintenance of the retention system which facilitates the 'request filter' complies with the requirements in all instances.[61] Similarly, even though the Investigatory Powers Commissioner is given the powers to audit these systems, this process is likely to be slow and lack of resources on the part of the IPC for this oversight will decrease their abilities to ensure that the filtered data are not presenting false correlations due to changes in context.[62] It is therefore important to recognize the issues which arise by altering the context of the data. As Crawford notes, 'Data are not generic. There is value to analysing data abstractions, yet retaining context remains critical, particularly for certain lines of inquiry. Context is hard to interpret at scale and even harder to manage when data are reduced to fit into a model'.[63] By allowing the context of the data to change, there is the risk that the potential for interferences which unnecessarily intrude into individual rights will be amplified.

5. Human Rights Concerns

Even if the 'request filter' is able to overcome the aforementioned issues concerning interpretation, lack of transparency, changes in context, and administration by intermediaries, the core human rights concerns arising from the use of this data would remain. Communications data provides for a clear picture of personal lives; in an aggregated form, the power of this data is even greater. Whereas a single piece of communications data may provide that a person was at a specific location, the aggregated impact could show that they go to that location every Tuesday for two hours, and another person is similarly always at that same location at those same times. This allows for inferences to be made which, rather than decreasing the intrusion into a person's private life, exponentially increase it. Further, even where the data isn't immediately attributable to a known individual, the correlations across data sets, like those enabled by the filtering process, allow for individuals to be identified

[59] Mobile Marketing Association, 'Demystifying Location Data Accuracy' (*MMA Global*) < http://www.mmaglobal.com/files/documents/location-data-accuracy-v3.pdf> accessed 15 Mar 2017.
[60] See Hamel note 58 above.
[61] It is questionable how much funding is provided to CSPs to ensure that these systems comply in this regard.
[62] IPA 2016 ss 229-231, 238, & 239.
[63] See boyd note 29 at 671.

from this data. If adequately safeguarded and overseen, this can provide a valuable tool for law enforcement. However, it can also provide a potential mechanism to squash dissent and target people for other purposes, for example, identifying lead activists or protesters in a movement. 'Suspicious profiles might involve information about people's free speech, free association, or religious activity'.[64] This issue is further aggravated by the wide range of public authorities who can access and use the 'request filter'. Increased access capabilities result in greater risks for abuse, a fact that is similarly amplified by the lack of resources for independent oversight of the mechanism. Further action is needed to ensure that the 'request filter' complies with the relevant human rights obligations and can act as an effective safeguard against the spurious processing of communications data and potential for collateral intrusions into privacy.

These actions should incorporate several considerations. First, there needs to be greater transparency in the development of the technology and automated systems used in the processing of the data. This does not require that this information be provided publicly; rather, it should be subject to independent inspection by technical experts who can assess the impartiality of the mechanism.[65] 'Oversight is much better conducted by well-staffed and knowledgeable outside evaluators'.[66] Second, further information concerning the resolution of potential errors in processing and authorisation need to be set out. The automated elements of the system need to be subject to regular checks to ensure that they are not resulting in misinterpretation of personal information. Similarly, individuals whose personal information and privacy has been intruded upon erroneously need to be informed of this and be given a right to remedy. Finally, there needs to be an element of judicial oversight in the system as a whole.

The aforementioned actions are necessary to ensure that the system complies with the relevant case law, including the joined cases of *Tele2 & Watson* which found that general and indiscriminate retention of emails and electronic communications was disproportionate and that prior authorisation by a court or independent body was necessary for access to be authorised.[67] Following the decision in this case, and in preparation for the Court of Appeal judgment on the CJEU *Watson* decision, the Government undertook a consultation on the Investigatory Powers Act in November 2017. Amongst the proposals set forth in the consultation were provisions for a new communications data code of practice and regulations amending the IPA. Regarding the 'request filter', relevant provisions in the proposed Regulations seek to substitute 'a person' for a 'designated senior officer' in those provisions concerning who is authorised to access the filter.[68] This lowers the requirements for access to the filter and enables a larger pool of individuals in relevant public bodies to access this tool. Far from ensuring that such access is limited and adequately safeguarded, the expansion of persons entitled to use the filter increases the risk for unnecessary and disproportionate processing of data by the filter. The Draft Code of Practice does address the issue of errors in the data processed by the filter, however, the protections for individuals whose data erroneously used remain weak. The Code states that 'the omission of or incorrect matches in filtered results, or the release of results that exceed specified thresholds' are reportable errors.[69] As reportable errors, these are communicated to the Investigatory Powers

[64] See Solove note 53 at 189 above.
[65] See: Wachter, Mittlestadt, & Russell, 'Counterfactual explanations without opening the Black Box: Automated Decisions and the GDPR' (2017 forthcoming) Harvard J of L & Tech.
[66] See Schneier B, *Data and Goliath* (WW Norton & Co 2015) Loc 2548.
[67] Joined Cases C- 203/15 and C-698/15 *Tele2 Sverige AB and Watson & Ors* [2016] ECR II-970.
[68] Draft Statutory Instruments 2018 No x, 'The Data Retention and Acquisition Regulations 2018'.
[69] Home Office, Draft Communications Data Code of Practice Nov 2017, 11.30.

Commissioner. However, there is no requirement that the error be disclosed to the individual concerned unless the error is found to be 'serious',[70] and the determination of an error as serious does not mean that it will be found to be in violation of a person's Convention rights. This is particularly concerning as these errors can have significant effects on individuals, principally if they result in them being suspected or wrongly accused of a crime. Further, the Draft Regulations and Code of Practice contain no requirements for any independent judicial authorisation or review by an independent administrative body either in using the filter *ex ante* or *ex post*, in direct contrast with the ruling of *Tele2 & Watson*.

Conclusion

Law enforcement are facing constant challenges to keep pace with technological developments and find ways to utilise these advances for their benefit. The exponential increase in personal data, resulting from essentially every interaction, communication, and transaction, means that there is a growing data set of information that could be of value to law enforcement. In recognition of the investigative value of this information, the Investigatory Powers Act provides for the creation of a 'request filter' to sift through the data and make meaningful connections about the data. The filter processes the relevant data, and only discloses that which is necessary for the purposes of the investigation, thereby limiting collateral intrusions. This mechanism therefore purports to act as a safeguard, whilst still permitting the necessary processing and interpretation of the data.

Yet the overall impact of the large data sets collected, retained, and processed by this filter raises concerns due to its interference with fundamental rights concerning privacy and personal data. The mere processing of communications data has consistently been held by the Courts to amount to an interference.[71] Interpretations of this mechanism as a safeguard fail to consider the risk the mechanism represents through the existence of interpretive biases; lack of transparency; delegated responsibilities to intermediaries; and lack of judicial authorisation and effective oversight. In its current iteration, the proposed 'request filter' does not satisfy the necessary requirements to justify its interference with the privacy rights of the individuals affected. There must be further steps taken to provide higher thresholds for access to the filter, independent judicial or administrative authorisation, and rights for individuals to seek remedies. In the absence of such provisions, the 'request filter', designed with the aim of minimising intrusions into personal information and privacy, will become an instrument of those intrusions itself.

[70] The ECtHR has underlined that the absence of notification directly undermines the effectiveness of any remedies against such measures. See: *Roman Zakharov v Russia* App no 47143/06 [ECHR 4 Dec 2015]. It must also be noted that this is not a problem solely with the 'request filter' but also applies to other errors in communications data acquisition and disclosure in the Investigatory Powers Act.

[71] See: *Valenzuela Contreras v Spain* App no 58/1997/842/1048 (ECHR 30 July 1998); *Copland v United Kingdom* App no 62617/00 (ECHR 3 April 2007); *Liberty v United Kingdom* App No 58243/00 (ECHR 11 Jul 2008); Joined Cases C-293/12 & 594/12 *Digital Rights Ireland* [2014] ECLI-238; and Joined Cases C- 203/15 and C-698/15 *Tele2 Sverige AB and Watson & Ors* [2016] ECR II-970.