International Review of Law, Computers & Technology

ISSN: 1360-0869 (Print) 1364-6885 (Online) Journal homepage: https://www.tandfonline.com/loi/cirl20

Algorithmic surveillance: the collection conundrum

Maria Helen Murphy

To cite this article: Maria Helen Murphy (2017) Algorithmic surveillance: the collection conundrum, International Review of Law, Computers & Technology, 31:2, 225-242, DOI: 10.1080/13600869.2017.1298497

To link to this article: https://doi.org/10.1080/13600869.2017.1298497

Published online: 12 Mar 2017.

INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY, 2017
VOL. 31, NO. 2, 225–242
http://dx.doi.org/10.1080/13600869.2017.1298497

Routledge
Taylor & Francis Group

Algorithmic surveillance: the collection conundrum

Maria Helen Murphy

Department of Law, Maynooth University, Maynooth, Ireland

ABSTRACT

Supporters of increased surveillance see tremendous potential in the ever increasing creation, collection, and retention of personal data. Most acknowledge that the massive collection of information also creates challenges where the collection outpaces the ability to meaningfully process the data. Increased processing power and more finely tuned algorithms are often portrayed as the solution to this haystack conundrum. While a human may struggle to find the needle in an overflowing haystack of disordered information, powerful computers can take a logical and structured approach that will make the haystack eminently more searchable. This article evaluates this premise from a human rights perspective and considers whether algorithmic surveillance systems can be designed to be compatible with the right to privacy. In addition to assessing the incongruity between traditional safeguards (such as foreseeability and accountability) with algorithmic surveillance, this article also confronts the problem of initial collection and addresses the contention that well-defined algorithmic search can effectively limit the intrusiveness of surveillance. Evolution in the case law of the European Court of Human Rights and the Court of Justice of the European Union will be factored into this analysis.

ARTICLE HISTORY
Received 29 October 2016
Accepted 4 January 2017

KEYWORDS
Algorithms; surveillance; privacy

Introduction

As humans are inherently self-documenting, the increased use and sophistication of communications technologies, has led to previously unfathomable amounts of personal data being generated by the average individual (Crampton 2015; Miller 2013). A notable aspect of this is the proliferation of GPS enabled smart phones as aggregated location data can lead to the inference of much sensitive information about an individual's movements, connections, and relationships with others (Gellman and Soltani 2013b; Richards and King 2013). The increased generation of information has been a boon to intelligence agencies seeking to collect ever increasing amounts of personal information. Combining these developments with reduced data storage costs, significant government investment in intelligence collection, and government support for bulk retention, intelligence agencies have never had greater access to information regarding the general population. While individual data points may be revealing, the aggregation of data from a multitude of sources has the potential to be profoundly more intrusive and the expansion of the

CONTACT Maria Helen Murphy maria.murphy@nuim.ie

surveillance assemblage has been striking (Felten 2013, 716). Huge amounts of data can also be a burden if information is being collected to such an extent so as to overwhelm those tasked with the duty of interpreting and acting on that data. Algorithms, with their capacity to organise and process large quantities of data efficiently, appear to offer a solution to this problem (MacCormick 2012).

This article assesses the use of algorithmic surveillance from a privacy perspective and considers how the European Convention on Human Rights (ECHR) may be used to respond to such techniques. Once the background jurisprudence has been discussed, this article reflects on current developments in European case law that might influence the future modus operandi of intelligence agencies. An interesting aspect of the developments in Europe has been the cross-fertilisation between the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). In this article, the recent decisions of the ECtHR in *Roman Zakharov v Russia* and *Szabó and Vissy v Hungary* and the decision of the CJEU in *Digital Rights Ireland* receive particular attention.[1] Before delving into the case law, however, it is important to first consider the concept of algorithmic surveillance in more depth.

Algorithmic surveillance

When dealing with large collections of data, algorithm-based data mining can be used to process and filter bulk datasets (Gillespie 2016; Cheney-Lippold 2011). The data sets are filtered using selectors, such as selectors relating to language, key words, communication paths and other technical data (Venice Commission 2015, 11). For example, previously identified suspect telephone numbers may be used as selectors in order to identify new potential suspects. An individual who is in contact with a number of individuals under suspicion can be highlighted as a potential target for further scrutiny (Venice Commission 2015, 11–12). While the term 'algorithm' can be very simply defined as a 'sequence of computational steps that transform the input into the output', machine learning algorithms 'modify their processing operations autonomously on the basis of newly acquired information' (Johns 2015; Cormen et al. 2009; Witten, Frank, and Hall 2011).

Profiles play a crucial role in algorithmic surveillance. The development of suspect profiles involves the collection and processing of information in order to make assumptions about a data subject and his or her 'future behaviour' (Korff 2012; Korff 2015, 23). Profiles are constructed based on correlations between certain actions – often fundamentally non-incriminating – and certain behaviours or associations. To provide a basic example, an individual who purchases an airline ticket with cash, travels under a name not associated with the registered phone number, has a nervous disposition, and does not check-in any baggage may be identified as a 'probable drug trafficker'.[2] Such an identification could then trigger a more in depth investigation of that individual.[3] While that is a simple illustration, a powerful machine learning algorithm can analyse 'exponentially more data points' and can identify more complex relationships than is possible when applying a traditional police profile (Rich 2015–2016, 905; Flach 2012, 9; Heumann and Cassak 2001, 919–921). In addition, precise weightings can be applied to different factors in the profile (Flach 2012, 25–32). Andrejevic states that '[t]he promise of predictive analytics is to incorporate the future as a set of anticipated data points into the decision-making process' (2013, 24). In effect, the shift from investigation to prediction means that

investigative authorities are pursuing a 'potential terrorist, a subject who is not yet fully in view, who may be unnamed and as yet unrecognizable' (Amoore 2014, 108–112).

As the aim of strategic surveillance is to be proactive by identifying threats rather than investigating known threats, in practical terms, this requires the identification of 'high risk' individuals based on algorithmic selectors and profiles (Venice Commission 2015, 12; Korff 2015, 41). Strategic surveillance is prevalent in surveillance operations where the prevention of terrorist attacks is the primary goal and where the prosecution of terrorists for committing terrorist acts serves as a less prioritised secondary objective (Venice Commission 2015, 3). Such an approach is appealing from a security perspective but poses clear risks for human rights (Venice Commission 2015, 35). In addition to constituting a threat to privacy – as is focused on in this article – where the network of targeted individuals is likely to include subversives, members of minority religious groups, and journalists there are also clear implications for the protection of free speech and the prevention of discrimination. At a point in time where mass surveillance is under ever increasing scrutiny from human rights authorities, it is important to recall that mass data collection and algorithmic processing are inherently interlinked. Not only does algorithmic processing enable the filtering and sorting of huge data sets into manageable outputs, but effective algorithmic analysis depends on large and accurate data sets.[4] Having set out the manner in which algorithmic methods are used to process large collections of data, it is now necessary to consider the privacy implications of such techniques.

The right to privacy and algorithmic surveillance

From a European Convention on Human Rights perspective, the Article 8 right to respect for private life is most pertinent to the issue of generalised surveillance and the subsequent algorithmic processing of data collected through surveillance.[5] Even though the ECtHR has interpreted the scope of 'private life' broadly, it accepts that it is not an absolute right and that it can be limited where the intrusion is 'in accordance with the law' and 'necessary in a democratic society' in the pursuit of a 'legitimate aim'.[6] Each of these requirements is mandatory and cumulative. The concept of a legitimate aim is broadly drawn, with legitimate aims including the prevention of disorder or crime, the protection of public safety, economic well-being, and the rights and freedoms of others. It will often not be too difficult to determine whether a particular surveillance measure is conducted in the pursuit of a legitimate aim as surveillance measures are generally directed at the prevention of crime and the protection of public safety. In fact, it can be argued that the inclusion of the word 'prevention' in the second paragraph of Article 8 provides some support for the practice of strategic surveillance. While it may be a straightforward matter to identify a legitimate aim to support the generalised collection and filtering of personal information by government authorities, this is not the end of the inquiry when determining compliance with criteria under Article 8.

Once a legitimate aim has been identified, the ECtHR will consider whether the measure is 'in accordance with the law'. The ECtHR has clarified that in addition to requiring a legal basis for intrusive action, domestic laws should provide adequate accessibility and foreseeability for individuals.[7] These are related obligations and constitute essential rule of law values that protect against abuses of power. The accessibility requirement that individuals must have an adequate indication as to the legal rules applicable to a given case has

meant that historically secretive practices, such as covert surveillance, must now be supported by a publicly accessible legal basis.[8] The foreseeability requirement mandates that laws be formulated 'with sufficient precision to enable the citizen to regulate his conduct'.[9] While foreseeability in the surveillance context 'cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly',[10] the risk of arbitrary covert action necessitates the provision of 'clear, detailed rules'.[11] Crucially, the domestic law must indicate the scope and manner of exercise of any discretion conferred on the competent authorities in order to give the individual adequate protection against arbitrary interference.[12] In search of a practical means of preventing arbitrary interference in the opaque world of surveillance, the ECtHR has developed a number of safeguards that must be set out in law in order to prevent abuses of surveillance powers.[13] According to the ECtHR, seriously intrusive surveillance measures should be provided for in legislation that sets out:

> the nature of offences which may give rise to an interception order; the definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed.[14]

While these safeguards were originally developed to protect against abuse of individualised surveillance methods, in the case of *Weber and Saravia*, the ECtHR confirmed that safeguards are equally important in the context of strategic surveillance.[15] The ECtHR has addressed the issue of generalised as opposed to individualised surveillance in a number of decisions.[16] While merely a decision on admissibility, the reasoning in *Weber and Saravia* is widely regarded as very significant. The decision considers strategic monitoring and has been frequently cited with approval in subsequent rulings on surveillance.[17] In *Weber and Saravia*, the Court distinguished 'individual' from 'strategic' monitoring by pointing out that individual monitoring 'serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed'.[18] The key is individualised suspicion. In contrast, the measures examined in *Weber and Saravia* were

> aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences.[19]

Even though the strategic surveillance regime did not constitute blanket surveillance of the entire population, the collection was indiscriminate with respect to the existence or absence of any suspicion of criminal involvement.

The ECtHR reviewed the safeguards outlined in the German legislation and found them to meet the standards discussed above to the level necessary in order to give citizens 'an adequate indication as to the circumstances in which and the conditions on which the public authorities were empowered to resort to monitoring measures'.[20] The German regime provided extensive safeguards but the application of standards developed in the context of individualised surveillance raised some novel questions for the ECtHR. The challenge of applying standards developed to regulate targeted surveillance to strategic surveillance scenarios, illustrates how developments in surveillance practices can

result in the evolution of established principles. Even though different issues arise in the setting of standards for the duration, use, communication, retention of data, etc. in the context of strategic surveillance,[21] the issue of how to categorise potential surveillance targets is particularly relevant when considering the role of algorithms. As strategic surveillance is inherently generalised, the regime examined in *Weber and Saravia* raised some questions as to how the requirements for laws to detail 'the nature of offences' which may give rise to surveillance and 'categories of people' liable to surveillance could be met.

While it is a straightforward task to delineate the relevant offences and persons liable to targeting when surveillance is being directed at individuals; generalised, strategic surveillance creates new challenges. In addition to being detrimental to free expression and sanctity of thought, a law that clearly states that every individual is the potential (or actual) subject of surveillance, renders any foreseeability benefit superficial and potentially chilling of speech and action. In *Weber and Saravia*, the ECtHR highlighted that the legislation indicated the categories of person liable to have their communications intercepted. According to the law, participants in international telephone conversations via satellite connections or radio relay links and participants in international telephone conversations via fixed telephone lines where the monitoring was conducted to avert an armed attack on Germany were potentially liable to surveillance.[22] In addition, if German nationals were to be subjected to surveillance, they were required to use certain catchwords in order to trigger an investigation.[23] While surveillance was carried out in *Weber and Saravia* without the existence of traditional individualised suspicion, the ECtHR emphasised the fact that the information was filtered through the use of 'catchwords' that were suitable for the 'investigation of the dangers described in the monitoring order'.[24] The fact that the ECtHR examined a surveillance system where government authorities filtered surveillance information through the application of predetermined selectors is, of course, highly pertinent to algorithmic surveillance. Crucially, the German law required that catchwords be listed in the monitoring order which meant that the catchwords were recorded and subject to supervision by an independent authority (the G10 Commission).[25] The use of catchwords in conjunction with the provision of an extensive system of safeguards would appear to be important as the ECtHR subsequently found a UK system of generalised surveillance that utilised filtering catchwords to be in violation of the ECHR due to the lack of accessible information regarding how the system and its safeguards operated.[26]

The decision in *Weber and Saravia* to recognise the use of filtering catchwords as a safeguard could be seen as an endorsement of the contention that algorithmic filtering of mass data sets can have a positive human rights effect. Proportionality is a requirement of Article 8 and the use of filtering catchwords can be viewed as a minimisation technique that reduces the scope of intrusive measures. The Venice Commission has suggested that the use of relevant and specific selectors can be used to limit unnecessary intrusion (Venice Commission 2015, 11–12). In other surveillance contexts, algorithms have been used to minimise data retention and to restrict access to data deemed irrelevant to the legitimate purpose of detecting suspicious behaviour (Neyland 2016).[27] This position has intuitive appeal. As evidenced by the mass adoption of many online products and the indifference of some to reports of automated scanning of emails and photographs stored in the cloud, it appears that many individuals feel less violated when a 'computer' carries out surveillance as opposed to a human (Gibbs 2014). While the strategic collection of data entails the absence of individualised suspicion, the filtering of the data through the

use of certain independently reviewed catchwords limits the additional intrusion. It could be argued that reasonable suspicion can be inferred from individual use of a relevant catchword, such as 'bomb', 'nuclear', or 'rocket' ('Secret services ramp up online surveillance' 2012). Setting aside for now the fact that such an approach appears to ignore the intrusive effect of the initial collection, even if this argument is accepted, it is challenging to imagine how the protection provided by the use of simple and understandable selectors translates to the use of modern complex algorithms. The difficulty of ensuring foreseeability and accountability is increased exponentially when algorithms are dynamic and where the eventual criteria for selection are impossible to predict.

Traditionally, the existence of individualised suspicion has been determined by human actors based on a non-technical assessment of probabilities. Factors such as who the target is, where they have been, what they have done, and when have they done it can all be considered when assessing the probability of a criminal act being committed. Modern data mining and machine learning capabilities would appear to threaten the traditional model and present the possibility that more accurate determinations of probability could be made based on complex analysis of detailed data sets (Rich 2015–2016, 877–888).[28] For example, machine learning techniques can be used to reveal 'otherwise unrecognizable patterns in complex processes underlying observable phenomena' (Rich 2015–2016, 874–875; Alpaydin 2014, 2).

Sophisticated investigatory programmes use machine learning processes in an effort to predict individual criminality based on algorithms (Eligon and Williams 2015; Harcourt 2007; Rich 2015–2016, 876). Where data are imperfect, systems can make 'probabilistic predictions' based on pattern recognition (Rich 2015–2016, 876; Alpaydin 2014, 2–3). Crucially, modern technologies allow for the automation of the process where a programme can search for correlations in the data set that may indicate criminal activity and to develop its approach and iteratively 'learn' over time (Rich 2015–2016, 876). As a dynamic algorithm continues to interrogate data, identify patterns, and develop, the processes of the algorithm can become opaque even to those who designed it (Gillespie, 172; De Zwart, Humphreys, and Van Dissel 2014, 718). As pointed out by Korff, the dynamic refining of selectors means that the algorithms 'lose the link with the originally simple (or at least relatively simple) "selectors"' (2015, 41). While the ECtHR has consistently recognised that the concept of foreseeability in the surveillance context does not mean that individuals should be able to predict when they may be subject to surveillance, the application of machine learning in the surveillance contexts presents a striking, perhaps unconquerable obstacle to the provision of foreseeability.

The challenges of providing foreseeability and accountability in the context of algorithmic surveillance may be impossible to overcome,[29] but even if a sufficiently protective regime could be developed, the requirement that the system be necessary in a democratic society would remain. Most surveillance programmes are designed to respond to a perceived social need, but the Convention requires the response to be proportionate to that legitimate aim.[30] Accordingly, in order to be compatible with the Convention, a surveillance system should be suitable and should strike a reasonable balance between the various competing interests (Gerards 2012, 200; Christoffersen 2009, 69; Arai-Takahashi 2002, 11).[31]

Unfortunately, many algorithmically driven surveillance systems would appear to fall at the first hurdle by not even being suitable to achieve the legitimate aim.[32] An inherent

problem with such surveillance is the base rate fallacy and the high likelihood of 'false positives' (Korff 2010, 22; Schneier 2006). False positives are particularly likely – and particularly harmful – when algorithmic techniques are used to identify potential terrorists. Due to the rarity of terrorist attacks, pattern searching is liable to mistakes. While the inherently probabilistic nature of such determinations is not a serious problem when the consequence is an online advertisement targeting an uninterested consumer, an incorrect categorisation as a terrorist can have significant human rights implications for the incorrectly targeted individual (Schneier 2015, 137). Not only that, but in such a system, false categorisations of actual terrorists as probable non-terrorists are also likely to occur (Grothoff and Porup 2016). As a result, the use of such techniques not only harms falsely targeted individuals, but can also squander resources that could be more effectively used on more traditional or more targeted investigative techniques (Thomson 2016). As intelligence agencies use machine learning in order to process huge amounts of data, another problem occurs (Moody 2016; Danezis 2016). In order to ensure the effectiveness and accuracy of an algorithm in identifying potential terrorists, it must be both trained and tested using different data sets. This is an impossible task where little information about 'known terrorists' is available to 'train and test the model' (Grothoff and Porup 2016).

When the ECtHR has considered the issue of necessity in the surveillance context it has stated that surveillance measures must be 'strictly necessary for safeguarding democratic institutions'. The ECtHR focuses on the existence of safeguards when examining this question and considers whether the system provides 'adequate and effective safeguards against abuse'.[33] Whether or not a regime provides adequate and effective guarantees against abuse:

> depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law.[34]

To best ensure compliance with Convention principles, surveillance measures should be subject to independent supervision at each stage of data collection and analysis. If algorithms are used to filter surveillance data they must be reviewed in order to ensure that surveillance powers are not exercised arbitrarily. To ensure the effectiveness of supervision, procedural protections are not only required at the design of the algorithms or rule-making stage but should also apply to decisions made based on algorithmic predictions (Citron and Pasquale 2014, 19; Bosco et al. 2015). In the general context of algorithmic determinations, Crawford and Schulz argue that the auditing of 'the data that was used to make a determination' would provide a beneficial safeguard (Crawford and Schultz 2014, 117; De Zwart, Humphreys, and Van Dissel 2014, 721). Even where secrecy is an operational necessity, accountability should still be provided through oversight mechanisms. While the Committee on Civil Liberties, Justice and Home Affairs acknowledges the necessity of 'a certain level of secrecy' in order to protect ongoing surveillance operations, the Committee maintains that 'such secrecy cannot override or exclude rules on democratic and judicial scrutiny' or other rule of law values such as transparency (Moraes 2014, 19). Similarly, Anderson has reported that while some secrecy may be necessary in the surveillance context, adequate safeguards and 'direct public engagement' are also required (Anderson 2015, 190–191). The ECtHR has a clear preference for

entrusting supervisory control to members of the judiciary, but have accepted alternatives where they are adequately independent of the executive (McIntyre 2016).[35] The review of algorithmic surveillance may be a sensible case for a modified approach where an independent expert group with technical and legal expertise could review the operation of the system and report on its workings. A condition for the effectiveness of such a review system would require immutable audit logs to be generated automatically. Access to this information would enable the reviewing authority to interrogate whether the system was operating effectively and appropriately (Citron and Pasquale 2011, 1473). Not only is such informed review important to ensure that surveillance powers are not being arbitrarily exercised, but it is also essential to enable individual targets to pursue redress (Citron 2007).[36]

The ECtHR has grown increasingly supportive of the need to notify surveillance targets subsequent to the cessation of surveillance where possible.[37] Where an activity is carried out in secret, subsequent notification is 'inextricably linked to the effectiveness of remedies' and to the effectiveness of safeguards against abuse.[38] If an individual has been targeted for additional surveillance based on an algorithmic determination, that decision should not be immune from scrutiny. It has been pointed out that determinations based on algorithmic processes are extremely difficult to contest and can in fact become 'effectively unchallengeable if the underlying "intelligence" and the evaluations of the "intelligence" and the precise algorithm used to weigh the various elements of the "intelligence" cannot be challenged' (Korff 2015, 21–22). As this is an issue with mere commercial algorithms, vigorously guarded by trade secrets, problems of transparency are only magnified in the covert surveillance context. Furthermore, there are significant practical reasons that hinder transparency and the potential for effective remedies in the algorithmic surveillance context.

When dealing with modern algorithmic processes, the interpretability of their operation is a substantial barrier to effective oversight. This may be true at the point where the systems are designed – for example if reviewers do not have sufficient technical expertise – and there may also be challenges once the system is in effect and general oversight of its operation is being carried out. Such issues will also exist wherever a reviewing or remedial body must assess whether the algorithmic targeting of a specific individual was reasonable. Where automated predictions are not explainable in human language it is difficult to justify why a particular individual was targeted for 'differentiated treatment' (Zarsky 2013, 1519–1520). At a general level, the opacity of such determinations can shield a surveillance system from scrutiny and hinder the public access and debate that is an essential bulwark against arbitrary use (Citron 2007, 1254–1258; De Zwart, Humphreys, and Van Dissel 2014, 714–715).

Even setting aside the many challenges discussed so far, algorithmic surveillance – relying as it does on the analysis of massive datasets – still faces the thorny problem of initial generalised collection (Murphy 2016). A crucial question at the heart of this issue is how the intrusion formed at the various stages of data collection is categorised. European jurisprudence appears to recognise that intrusion repeatedly occurs at the points of collection, retention, and use – even where no human scrutiny is involved.[39] Some intelligence agencies, on the other hand, maintain that the solely algorithmic processing of personal data involves minimal if any interference with privacy rights (EFF n.d.; Corera 2015). Former Director of National Intelligence, James Clapper, equates mass retention

of data to a library which contains many books, most of which are never read. According to Clapper's reasoning, the protection of rights only becomes important at the point where the authorities decide which books to 'open up and actually read' (Schneier 2015, 129).

Historically, distinctions between different types of data and different uses of data have been readily accepted by the ECtHR. For example, as early as *Malone v UK* and more recently in cases such as *Uzun v Germany*, there has been clear acknowledgement from the Court that the collection of non-content data requires less safeguards than the collection of content data.[40] While mass surveillance and algorithmic processing is not solely carried out using metadata, it is very often the case that metadata is most useful to these techniques.[41] Historically, individuals may not have felt that their telecommunication records constituted sensitive personal information. The increased generation and granularity of such data, combined with sophisticated data mining capabilities, has made the naivety of that position apparent. In the aftermath of the Snowden revelations, the position of the two major European courts appears to have evolved. The first post-Snowden privacy decision of the CJEU appeared to reflect a shift in perception on this issue.

Recent developments at the CJEU and the ECtHR

In the ruling in *Digital Rights Ireland*, the European Union's highest court examined the validity of the Data Retention Directive[42] which had mandated that Member States require the retention of all communications metadata for between 6 and 24 months.[43] The CJEU demonstrated awareness of the potentially exposing nature of metadata and stated that the retained data had the potential to

> allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[44]

The CJEU found the general application of the Data Retention Directive to be incompatible with the right to respect for private life and the right to protection of personal data as protected by Articles 7 and 8 of the EU Charter. In particular, the CJEU criticised the Directive for requiring the collection of metadata on 'all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made'.[45] The CJEU was especially critical of the blanket application of the Directive and pointed out that the Directive did 'not require any relationship between the data whose retention is provided for and a threat to public security'.[46] The CJEU accepted that data retention could be an appropriate means to achieve the legitimate prevention of serious crime and terrorism,[47] but clarified that mass data retention could only be justified where 'strictly necessary'.[48] Accordingly, the CJEU asserted that data retention legislation must contain

> clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.[49]

There is a degree of uncertainty as to the precise intention of the ruling in *Digital Rights Ireland*. While the immediate invalidity of the Data Retention Directive was clear, there is some disagreement as to whether the decision allows for the generalised collection

of data on all individuals where rigorous safeguards are in place. While the CJEU openly criticised the legislation for not limiting retention to data 'pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime',[50] it is possible that the CJEU would accept the compatibility of such a system where extensive safeguards were provided in the form of strong review, accountability, security requirements, and access restrictions.[51] This interpretation gained support recently with the release of an advisory Opinion where Advocate General Saugmandsgaard Øe endorsed the contention that general data retention obligations 'do not go beyond the bounds of what is strictly necessary, provided that they are accompanied by certain safeguards concerning access to the data, the period of retention and the protection and security of the data'.[52] The dearth of specific safeguards in the text of the Data Retention Directive obviated the need to decide this point explicitly in *Digital Rights Ireland* as the legislation was clearly unsatisfactory. While further clarification from the CJEU is awaited, it is certainly clear that the Court has strong misgivings about generalised collection and has signalled the fact that bulk surveillance programmes will be subject to heightened scrutiny going forward.

The remaining ambiguity regarding the application of the EU Charter to domestic surveillance operations combined with the human rights mandate and broad membership of the Council of Europe means that the ECtHR will continue to play an essential role in the limitation of surveillance powers in Europe.[53] While the ECtHR has previously been influenced by data protection law developments in its jurisprudence, the impact of the CJEU and the Charter is strikingly apparent in two recent decisions of the ECtHR, *Zakharov* and *Szabó* (De Hert and Gutwirth 2009, 18). Both decisions cited the ruling in *Digital Rights Ireland* and in both cases the ECtHR recognised that general surveillance programmes represent a significant threat to the protection of privacy. Of particular note is the statement from the Grand Chamber in *Zakharov* that interception authorisations must

> clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information.[54]

This point, combined with the assertion that surveillance authorising bodies must be 'capable of verifying the existence of a reasonable suspicion against the person concerned',[55] could be read to render generalised surveillance techniques inherently at odds with the ECHR.

While some have interpreted the subsequent decision in *Szabó* to constitute evidence of a fundamental incompatibility of mass surveillance with human rights, certain aspects of that decision suggest otherwise (St Vincent 2016). While the Fourth Section Court cited the Grand Chamber judgment in *Zakharov* extensively,[56] the majority ruling also indicated openness to the potential remediating effect of an extensive system of safeguards. Notably, the ECtHR stated that it is 'a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents'.[57] The ECtHR has a record of avoiding in depth consideration of the reasonableness of surveillance measures and has instead required states to provide rigorous safeguards. While the regime examined in *Szabó* was easily found to be in violation of Article 8 under the existing standards, the ECtHR

also speculated on the need to develop further safeguards sufficient to secure privacy rights.[58] Even though the decision in *Szabó* recognises mass surveillance as a particularly intrusive form of surveillance, it is not improbable that the ECtHR may choose to develop a newly enhanced system of safeguards in an effort to prevent abuse of mass surveillance capabilities.[59] It is possible that an enhanced role for data minimisation and filtering algorithms could be an aspect of such a development. On the positive side, it appears likely that if the ECtHR does sanction a role for mass surveillance in democratic societies, it is also likely to revise its finding in *Liberty v the United Kingdom* and find that different, more stringent standards for accessibility and clarity will be necessary to ensure compliance.[60]

Conclusion

Following a successful terrorist attack, frightened citizens and embattled governments often seek to understand, to investigate, to cast blame, and to shield themselves from accusations that they failed to act in response. In the face of incomprehensible loss and violence, a desire to know more can lead to a call to know a notional 'everything'. It is this desire that can partially explain unscientific positions such as that expressed by former Director of the National Security Agency (NSA), General Keith Alexander, 'you need the haystack to find the needle' (Gellman and Soltani 2013a). While investigatory authorities may be tempted to 'collect it all' (Nakashima and Warrick 2013a), there is a clear risk that accumulating masses of data from multiple sources over extended periods of time will result in an unmanageable glut of information beyond the comprehension of those tasked to act on the intelligence (De Zwart, Humphreys, and Van Dissel 2014, 717). The Snowden leaks indicated that this has been acknowledged as a very real issue by some within the NSA (Maass 2015; Rowley 2014).

Increased processing power and more finely tuned algorithms are often portrayed as the solution to the haystack conundrum. While a human may struggle with an overflowing haystack, powerful computers can take a logical and structured approach that will make the haystack eminently more searchable (Wells 2016).[61] This article discussed some of the key flaws in this argument and also highlighted how human rights issues will persist even in the event of a significant technological breakthrough. It is difficult to dismantle a complex apparatus once it has been constructed, particularly when that apparatus has – at least in part – been driven by the interests of the modern government surveillance industrial complex (O'Harrow, Priest, and Censer 2013; Mueller 2006). Indeed, advocates for increased collection and retention are prone to argue that 'any failures of intelligence simply indicate underinvestment' rather than any flaws in the approach (Citron and Pasquale 2011, 1475). This is why it is so critical that the implications of algorithmic surveillance are considered at the earliest possible point.

Both the CJEU and the ECtHR have recognised that greater safeguards are required where personal data are subject to automatic processing.[62] While this position is logical in light of the increased risks of such processing, it is necessary to confront the supposition that an upgrade of existing safeguards can address the unique issues created by mass collection and algorithmic processing of citizen information. It is difficult to predict the scope of potential harms at this early stage and it is challenging to fully grasp the risk due to the complexity of the technologies and techniques underlying the simple promise of

enhanced safety. This article maintains that caution as opposed to haste is the appropriate mindset at this crucial stage.

While technology evangelists may argue that existing human rights standards are outdated and antagonistic to our information driven futures and champions of surveillance may contend that human rights are secondary to security, it is important to remember that human rights standards were not created in a vacuum (Plouffe 2016; Schneier 2008). They were developed in order to protect fundamental democratic values deemed necessary to protect essential freedoms (Weil 1963, 27).[63] Where traditional safeguards, designed to protect human rights, hinder the development or use of a new technology, the reasons for that conflict must be fully examined. As human rights bodies continue to reckon with the risks of mass data collection and the relationship of algorithmic processing to that practice, the response should not be a rushed search for a workaround or an attempt to shoehorn new controls into traditional categories. If it appears that the new technologies cannot work within the boundaries of human rights law, society should first revaluate the use of the technology before reformulating fundamental ideals (Murphy 2016).

Notes

1. *Roman Zakharov v Russia* [2015] ECHR 1065; *Szabó and Vissy v Hungary* [2016] App 37138/14; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164.
2. *United States v Sokolow* 490 US 1, 9 (1989) as discussed in Rich (2015–2016, 902–903).
3. *United States v Sokolow* 490 US 1, 9 (1989) as discussed in Rich (2015–2016, 902–903).
4. The author does not discount the targeted nature of some *post hoc* information requests that are common in many data retention regimes. Of course, such systems only consider the existence of individualised suspicion at the point of access and not at the point of collection and retention.
5. Article 8 of the Convention states:

   > 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

6. *Peck v The United Kingdom* (2003) 36 EHRR 41, 57; *Niemietz v Germany* (1992) 16 EHRR 97, 29; *Pretty v The United Kingdom* [2002] ECHR 427, 61; *PG and JH v The United Kingdom* [2001] ECHR 550, 56.
7. *Silver v The United Kingdom* [1983] ECHR 5, 86; *Malone v The United Kingdom* [1984] ECHR 10, 67.
8. *Silver v The United Kingdom* [1983] ECHR 5, 87.
9. *Silver v The United Kingdom* [1983] ECHR 5, 88. See also, *Klass v Germany* (1979–1980) 2 EHRR 214, 55.
10. *Weber and Saravia v Germany* [2006] ECHR 1173, 93; *Leander v Sweden* (1987) 9 EHRR 433, 51.
11. *Weber and Saravia v Germany* [2006] ECHR 1173, 93; *Malone v The United Kingdom* [1984] ECHR 10, 67; *Huvig v France* (1990) 12 EHRR 528, 29; *Rotaru v Romania* [2000] ECHR 192, 55; *Kopp v Switzerland* (1998) 27 EHHR 93, 64, 72; *Valenzuela Contreras v Spain* (1999) 28 EHRR 483, 46.
12. *Weber and Saravia v Germany* [2006] ECHR 1173, 94–95.
13. *Huvig v France* (1990) 12 EHRR 528, 30.

14. *Szabó and Vissy v Hungary* [2016] App 37138/14, 56; *Weber and Saravia v Germany* [2006] ECHR 1173, 95; *Valenzuela Contreras v Spain* (1999) 28 EHRR 483, 46 *Huvig v France* (1990) 12 EHRR 528, 46.
15. *Weber and Saravia v Germany* [2006] ECHR 1173; *Liberty v The United Kingdom* [2008] ECHR 568, 65.
16. *Weber and Saravia v Germany* [2006] ECHR 1173; See also, *Liberty v The United Kingdom* [2008] ECHR 568, 65; *Roman Zakharov v Russia* [2015] ECHR 1065 and *Szabó and Vissy v Hungary* [2016] App 37138/14.
17. See, for example, *Liberty v The United Kingdom* [2008] ECHR 568, 63; *Roman Zakharov v Russia* [2015] ECHR 1065, 229; *Szabó and Vissy v Hungary* [2016] App 37138/14, 57.
18. *Weber and Saravia v Germany* [2006] ECHR 1173, 4.
19. *Weber and Saravia v Germany* [2006] ECHR 1173, 4.
20. *Weber and Saravia v Germany* [2006] ECHR 1173, 101.
21. *Szabó and Vissy v Hungary* [2016] App 37138/14, 56; *Weber and Saravia*, 95; *Valenzuela Contreras v Spain* (1999) 28 EHRR 483, 46; *Huvig v France* (1990) 12 EHRR 528, 46.
22. *Weber and Saravia v Germany* [2006] ECHR 1173, 97. While this could potentially be a very large category of people, it is important to note that at the relevant time, wireless communications constituted just 10% of all telecommunications. *Weber and Saravia v Germany* [2006] ECHR 1173, 110.
23. *Weber and Saravia v Germany* [2006] ECHR 1173, 97.
24. *Weber and Saravia v Germany* [2006] ECHR 1173, 32.
25. *Weber and Saravia v Germany* [2006] ECHR 1173, 32.
26. *Liberty v The United Kingdom* [2008] ECHR 568, 68–69. A focus on remediating safeguards appeared to gain support in the recent Opinion of AG Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* Opinion of AG Saugmandsgaard Øe, 226, 259.
27. Many of the same issues arise when surveillance data are collected via CCTV and subsequently algorithmically processed as when communications data are subject to such algorithmic processing.
28. In his article, Michael Rich considers whether 'Automated Suspicion Algorithms' can meet the US constitutional law standards of probable cause and reasonable suspicion (2015–2016, 877); *Brinegar v United States* 338 US 16o, 175 (1949).
29. It has been established that from the Article 8 requirement that privacy intrusive measures be 'in accordance with the law' 'stems the need for the law to be accessible to the person concerned, who must moreover be able to foresee its consequences for him'. *Ekimdzhiev v Bulgaria* [2007] ECHR 533, 71; *Huvig v France* (1990) 12 EHRR 528, 26; *Kruslin v France* (1990) 12 EHRR 547, 27; *Malone v The United Kingdom* [1984] ECHR 10. In addition to requiring that the law be accessible and foreseeable, the law must also be compatible with the rule of law generally. In the case of serious privacy interferences, such as telephone tapping, the ECtHR has stated the requirement that 'minimum safeguards' should be set out in statute in order to avoid abuses of power. *Huvig v France* (1990) 12 EHRR 528, 34; *Kruslin v France* (1990) 12 EHRR 547, 35; *Valenzuela Contreras v Spain* (1999) 28 EHRR 483, 46.
30. According to the ECtHR '"necessary" … implies the existence of a "pressing social need" for the interference in question and the interference must be proportionate to the legitimate aim pursued'. *Dudgeon v The United Kingdom* [1981] ECHR 5, 51; *Silver v The United Kingdom* [1983] ECHR 5, 97; *Handyside v The United Kingdom* [1976] ECHR 5, 48–49.
31. In the CJEU context, proportionality requires actions to be 'appropriate for attaining the legitimate objectives pursued' and not excessive to what is 'appropriate and necessary in order to achieve those objectives'. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 46.
32. There is support, however, for the argument that bulk interception can play a valuable, if not proportionate, role in the protection of national security (Anderson 2015, 130).

33. *Roman Zakharov v Russia* [2015] ECHR 1065, 232; *Kennedy v The United Kingdom* [2010] ECHR 682, 153; *Malone v The United Kingdom* [1984] ECHR 10; *Leander v Sweden* (1987) 9 EHRR 433, 60; *Iordachi v Moldova* [2009] ECHR 256, 53.
34. *Klass v Germany* (1979–1980) 2 EHRR 214, 50; *Roman Zakharov v Russia* [2015] ECHR 1065, 232; *Weber and Saravia v Germany* [2006] ECHR 1173, 106.
35. *Roman Zakharov v Russia* [2015] ECHR 1065, 233.
36. Citron has highlighted the challenges of algorithmic accountability with particular focus on the difficulty of applying a traditional 'due process' model to algorithmic decisions. Recognising these challenges, Citron endorses a new model of 'technological due process' which does not rely on traditional due process and proposes to require a battery of mechanisms 'capable of enhancing the transparency, accountability, and accuracy of rules embedded in automated decision-making systems'.
37. *Szabó and Vissy v Hungary* [2016] App 37138/14, 86. See also, *Roman Zakharov v Russia* [2015] ECHR 1065, 300.
38. *Roman Zakharov v Russia* [2015] ECHR 1065, 234.
39. The ECtHR has interpreted 'private life' broadly, recognising the simple storing of data relating to the private life of an individual falls within the scope of Article 8. *Lundvall v Sweden* [1985] App 10473/83, 3; *Leander v Sweden* (1987) 9 EHRR 433, 48; *Amann v Switzerland* (2000) 30 EHRR 843, 65.
40. Telephone metering information was considered in *Malone v UK* and location data were considered in *Uzun v Germany*. *Malone v The United Kingdom* [1984] ECHR 10, 84; *Uzun v Germany* [2010] App 35623/05, 52. At the same time, it is important to note that in both cases the ECtHR did note that an interference with privacy – even if on the lower level of seriousness – had occurred. Due to the lack of accessible legislation governing the access to metering information, the UK was found in violation on this point.
41. As pointed out by AG Saugmandsgaard Øe, metadata can be used to 'facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not'. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* Opinion of AG Saugmandsgaard Øe, 259.
42. Reference for a preliminary ruling from High Court of Ireland made on 11 June 2012. See *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney* [2012] O.J. C258/11; Request for a preliminary ruling from the Verfassungsgerichtshof (Austria) lodged on 19 December 2012 — Kärntner Landesregierung and Others [2013] O.J. C79/7.
43. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC [2006] O.J. L-105/54. The Directive frequently asserted that the 'content' of communications cannot be retained under the authority of the Directive. See art. 1(2), art. 5(2), and Recital 13 of the Directive.
44. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 27. While the CJEU did find the retention of information under the Directive to constitute a 'particularly serious interference' with privacy and personal data rights, the CJEU also held that the Directive did not violate 'the essence' of those rights. The Court justified this distinction by recognising that the Directive did not permit the retention of content data and the Directive required respect for 'certain principles of data protection'. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 39–40.
45. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 57.
46. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 59.

47. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 49–50.
48. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 51–52.
49. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 54 citing, *Liberty v The United Kingdom* [2008] ECHR 568, 62–63; *Rotaru v Romania* [2000] ECHR 192, 57–59; and *S and Marper v the United Kingdom* [2008] ECHR 1581, 99. According to the Court, there is an increased requirement for safeguards where the retained data are subject to automatic processing and there is a significant risk of unlawful access. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 55.
50. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 59.
51. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 29–30, 65.
52. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* Opinion of AG Saugmandsgaard Øe, 192–195.
53. It should be noted that Advocate General Saugmandsgaard Øe recently stated that 'it is not possible to interpret the provisions of the Charter differently depending on whether the regime under consideration was established at EU level or at national level'. Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* Opinion of AG Saugmandsgaard Øe, 191. Of course, if the UK continues on its current course to leave the EU, the importance of the Convention system will increase further (so long as the UK remains a Party to the ECHR).
54. *Roman Zakharov v Russia* [2015] ECHR 1065, 264; *Klass v Germany* (1979–1980) 2 EHRR 214, 51; *Liberty v The United Kingdom* [2008] ECHR 568, 64–65; *Ekimdzhiev v Bulgaria* [2007] ECHR 533, 80; and *Kennedy v The United Kingdom* [2010] ECHR 682, 160.
55. *Roman Zakharov v Russia* [2015] ECHR 1065, 260–264.
56. *Szabó and Vissy v Hungary* [2016] App 37138/14, 171. *Roman Zakharov v Russia* [2015] ECHR 1065, 259 and 261.
57. *Szabó and Vissy v Hungary* [2016] App 37138/14, 68.
58. *Szabó and Vissy v Hungary* [2016] App 37138/14, 68–70.
59. *Szabó and Vissy v Hungary* [2016] App 37138/14, 68–70.
60. *Liberty v The United Kingdom* [2008] ECHR 568, 63.
61. In fact, Wells decries the haystack analogy altogether (2016).
62. Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164, 49, 55; *S and Marper v the United Kingdom* [2008] ECHR 1581, 103; *Szabó and Vissy v Hungary* [2016] App 37138/14, 56; *Weber and Saravia v Germany* [2006] ECHR 1173, 68–70.
63. See also, the preamble to the ECHR, which states that '[f]undamental freedoms … are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the human rights upon which they depend'.

Disclosure statement

No potential conflict of interest was reported by the author.

References

Alpaydin, Ethem. 2014. *Introduction to Machine Learning*. Cambridge: MIT.
Amoore, Louise. 2014. "Security and the Claim to Privacy." *International Political Sociology* 8 (1): 108–112.

Anderson, David. 2015. *A Question of Trust: Report of the Investigatory Powers Review Presented to the Prime Minister Pursuant to Section 7 of the Data Retention and Investigatory Powers Act 2014*. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

Andrejevic, Mark. 2013. *Infoglut: How Too Much Information Is Changing the Way We Think and Know*. New York: Routledge.

Arai-Takahashi, Yutaka. 2002. *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of ECHR*. Antwerp: Intersentia.

Bosco, Francesca, Niklas Creemers, Valeria Ferraris, Daniel Guagnin, and Bert-Jaap Koops. 2015. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities." In *Reforming European Data Protection Law*, edited by Serge Gutwirth, Ronald Leenes, and Paul de Hert, 3–33. Dordrecht: Springer.

Cheney-Lippold, John. 2011. "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control." *Theory, Culture & Society* 28 (6): 164–181.

Christoffersen, Jonas. 2009. *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights*. Leiden: Martinus Neijhoff.

Citron, Danielle. 2007. "Technological Due Process." *Washington University Law Review* 85: 1249–1313.

Citron, Danielle, and Frank Pasquale. 2011. "Network Accountability for the Domestic Intelligence Apparatus." *Hastings Law Journal* 62: 1441–1494.

Citron, Danielle, and Frank Pasquale. 2014. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89 (1): 1–33.

Corera, Gordon. 2015. "UK Surveillance 'Lacks Transparency' ISC Report Says." *BBC*, March 12. www.bbc.com/news/uk-31845338.

Cormen, Thomas, Charles Leiserson, Ronald Rivest, and Clifford Stein. 2009. *Introduction to Algorithms*. Cambridge: Massachusetts Institute of Technology.

Crampton, Jeremy. 2015. "Collect It All: National Security, Big Data and Governance." *GeoJournal* 80 (4): 519–531.

Crawford, Kate, and Jason Schultz. 2014. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review* 55 (1): 93–128.

Danezis, George. 2016. "A Technical Reading of the 'HIMR Data Mining Research Problem Book.'" *Conspicuous Chatter*, February 3. https://conspicuouschatter.wordpress.com/2016/02/03/a-technical-reading-of-the-himr-data-mining-research-problem-book/.

De Hert, Paul, and Serge Gutwirth. 2009. "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul de Hert, Sjaak Nouwt, and Cécile de Terwangne, 3–44. Dordrecht: Springer.

De Zwart, Melissa, Sal Humphreys, and Beatrix Van Dissel. 2014. "Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK." *University of New South Wales Law Journal* 37 (2): 713–747.

Electronic Frontier Foundation. n.d. "The Government's Word Games When Talking About NSA Domestic Spying." *EFF*. https://www.eff.org/nsa-spying/wordgames.

Eligon, John, and Timothy Williams. 2015. "Police Program Aims to Pinpoint Those Most Likely to Commit Crimes." *New York Times*, September 24. http://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html?_r=0.

European Commission for Democracy Through Law (Venice Commission). 2015. *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies Study No. 719/2013 (CDL-AD(2015)006)*. Strasbourg: Council of Europe. http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e.

Felten, Edward. 2013. "Declaration of Professor Edward W Felten." Submission in American Civil Liberties Union v Office of the Director of National Intelligence, 13-cv-03994 (WHP), August 26. https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.

Flach, Peter. 2012. *Machine Learning: The Art and Science of Algorithms That Make Sense of Data*. Cambridge: Cambridge University Press.

Gellman, Barton, and Ashkan Soltani. 2013a. "NSA Collects Millions of E-Mail Address Books Globally." *Washington Post*, October 14. https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

Gellman, Barton, and Ashkan Soltani. 2013b. "NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show." *The Washington Post*, December 4. http://wapo.st/1laYWp.

Gerards, Janneke. 2012. "The Prism of Fundamental Rights." *European Constitutional Law Review* 8 (2): 173–202.

Gibbs, Samuel. 2014. "Gmail Does Scan All Emails, New Google Terms Clarify." *The Guardian*, April 15. https://www.theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify.

Gillespie, Tarleton. 2016. "Algorithm." In *Digital Keywords*, edited by Ben Peters, 18–30. Princeton, NJ: Princeton University Press.

Grothoff, Christian, and J. M. Porup. 2016. "The NSA's SKYNET Program May Be Killing Thousands of Innocent People." *Ars Technica UK*, February 16. http://arstechnica.co.uk/security/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/.

Harcourt, Bernard. 2007. *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age*. Chicago, IL: University of Chicago Press.

Heumann, Milton, and Lance Cassak. 2001. "Profiles Injustice? Police Discretion, Symbolic Assailants, and Stereotyping." *Rutgers Law Review* 53: 918–978.

Johns, Fleur. 2015. "Global Governance Through the Pairing of List and Algorithm." *Environment and Planning D: Society and Space* 33 (1): 126–149.

Korff, Douwe. 2010. "Technologies for the Use of Images: Automated Processes of Identification, Behavioural Analysis and Risk Detection Control at the Airports." Seminar presentation at Spanish Data Protection Agency Seminar, Madrid, June 9–11.

Korff, Douwe. 2012. "Comments on Selected Topics in the Draft EU Data Protection Regulation." London Metropolitan University, September 18. http://ssrn.com/abstract=2150145.

Korff, Douwe. 2015. *Passenger Name Records, Data Mining and Data Protection: The Need for Strong Safeguards*. Strasbourg: Council of Europe. https://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2015)11_PNR%20draft%20report%20Douwe%20Korff%20&%20Marie%20Georges_15%2006%202015.pdf.

Maass, Peter. 2015. "Inside NSA, Officials Privately Criticize 'Collect It All' Surveillance." *The Intercept*, May 28.

MacCormick, John. 2012. *Nine Algorithms That Changed the Future*. Princeton, NJ: Princeton University Press.

McIntyre, T. J. 2016. "Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective." In *Judges as Guardians of Constitutionalism and Human Rights*, edited by Martin Scheinin, Helle Krunke, and Marina Aksenova, 136–162. Cheltenham: Edward Elgar.

Miller, Gabriel. 2013. "Activity-based Intelligence Uses Metadata to Map Adversary Networks." *Defense News*, July 8.

Moody, Glyn. 2016. "GCHQ's Data-mining Techniques Revealed in New Snowden Leak." *Ars Technica UK*, February 3. http://arstechnica.co.uk/tech-policy/2016/02/gchqs-data-mining-techniques-revealed-in-new-snowden-leak/.

Moraes, Claude (Committee on Civil Liberties, Justice and Home Affairs). 2014. *Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs*. Brussels: European Parliament. https://polcms.secure.europarl.europa.eu/cmsdata/upload/73108fba-bb11-4a0b-83b8-54cc99c683b5/att_20140306ATT80632-1522917198300865812.pdf.

Mueller, John. 2006. *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, And Why We Believe Them*. New York: Free Press.

Murphy, Maria Helen. 2016. "Algorithmic Surveillance: True Negatives." *Computers and Law* 27 (3): 10–13.

Nakashima, Ellen, and Joby Warrick. 2013. "For NSA Chief, Terrorist Threat Drives Passion To 'Collect It All.'" *Washington Post*, July 14. https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html.

Neyland, Daniel. 2016. "Bearing Account-able Witness to the Ethical Algorithmic System." *Science, Technology & Human Values* 41 (1): 50–76.

O'Harrow, Robert, Dana Priest, and Marjorie Censer. 2013. "NSA Leaks Put Focus on Intelligence Apparatus's Reliance on Outside Contractors." *Washington Post*, June 10. https://www.washingtonpost.com/business/nsa-leaks-put-focus-on-intelligence-apparatuss-reliance-on-outside-contractors/2013/06/10/e940c4ba-d20e-11e2-9f1a-1a7cdee20287_story.html.

Plouffe, Jim. 2016. "Privacy Is Dead, Tech Evangelist Tells Entrepreneurs." *InDaily*, June 14. http://indaily.com.au/business/2016/06/14/privacy-is-dead-tech-evangelist-tells-entrepreneurs/.

Rich, Michael. 2015–2016. "Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment." *University of Pennsylvania Law Review* 164: 871–930.

Richards, Neil, and Jonathan King. 2013. "Three Paradoxes of Big Data." *Stanford Law Review Online*, September 3.

Rowley, Coleen. 2014. "The Bigger the Haystack, the Harder the Terrorist Is to Find." *The Guardian*, November 28. https://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks.

Schneier, Bruce. 2006. "Terrorists, Data Mining, and the Base Rate Fallacy." *Schneier on Security*, July 10. https://www.schneier.com/blog/archives/2006/07/terrorists_data.html.

Schneier, Bruce. 2008. "Security Vs. Privacy." *Schneier on Security*, January 29. https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html.

Schneier, Bruce. 2015. *Data and Goliath*. New York: WW Norton & Company.

"Secret Services Ramp Up Online Surveillance." 2012. *The Local*, February 25. http://www.thelocal.de/sci-tech/20120225-40975.html.

St Vincent, Sarah. 2016. "Did the European Court of Human Rights Just Outlaw 'Massive Monitoring of Communications' in Europe?" *CDT*, January 13. https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/.

Thomson, Iain. 2016. "GCHQ Mass Spying Will 'Cost Lives in Britain,' Warns Ex-NSA Tech Chief." *The Register*, January 6. http://www.theregister.co.uk/2016/01/06/gchq_mass_spying_will_cost_lives_in_britain/.

Weil, Gordon. 1963. *The European Convention on Human Rights: Background, Development and Prospects*. Leiden: AW Styhoff.

Wells, David. 2016. "Forget Needles and Haystacks – It's more Complicated than that" *Counter-terrorism Matters*, March 3. https://counterterrorismmatters.wordpress.com/2016/03/03/forget-needles-and-haystacks-its-more-complicated-than-that/.

Witten, Ian, Eibe Frank, and Mark Hall. 2011. *Data Mining: Practical Machine Learning Tools and Techniques*. Burlington, VT: Elsevier.

Zarsky, Tal. 2013. "Transparent Predictions." *University of Illinois Law Review* 4: 1503–1569.