Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Data gathering, surveillance and human rights: recasting the debate

Paul Bernal

To cite this article: Paul Bernal (2016) Data gathering, surveillance and human rights: recasting the debate, Journal of Cyber Policy, 1:2, 243-264, DOI: 10.1080/23738871.2016.1228990

To link to this article: https://doi.org/10.1080/23738871.2016.1228990

Published online: 16 Sep 2016.

JOURNAL OF CYBER POLICY, 2016
VOL. 1, NO. 2, 243–264
http://dx.doi.org/10.1080/23738871.2016.1228990

Routledge
Taylor & Francis Group

OPEN ACCESS

Data gathering, surveillance and human rights: recasting the debate

Paul Bernal

UEA Law School, University of East Anglia, Norwich, UK

ABSTRACT

The nature and depth of internet surveillance has been revealed to be very different from what had previously been publically acknowledged or politically debated. There are critical ways in which the current debate is miscast, misleading and confused. Privacy is portrayed as an individual right, in opposition to a collective need for security. Data gathering and surveillance are portrayed as having an impact only on this individual right to privacy, rather than on a broad spectrum of rights, including freedom of expression, of assembly and association, the prohibition of discrimination and more. The gathering and surveillance of 'content' is intrinsically more intrusive than that of 'communications' data or 'metadata'. The impact of data gathering and surveillance is often portrayed as happening only at when data are examined by humans rather than when gathered, or when examined algorithmically. Commercial and governmental data gathering and surveillance are treated as separate and different, rather than intrinsically and inextricably linked. This miscasting has critical implications. When the debate is recast taking into account these misunderstandings, the bar for the justification of surveillance is raised and a new balance needs to be found, in political debate, in law, and in decision-making on the ground.

ARTICLE HISTORY
Received 22 August 2016
Accepted 22 August 2016

KEYWORDS
Surveillance; human rights; privacy; political debate; law

The significance of communications surveillance was highlighted dramatically by the revelations of Edward Snowden – revelations that have triggered significant political and popular debate. The level of that debate, how it matches with the reality of surveillance in practice and the implications of that surveillance, can be characterised by misunderstanding and oversimplification. If appropriate decisions are to be made about the practice of surveillance, and the laws that govern surveillance, then the debate needs to be recast to give a better understanding of the nature and impact of surveillance.

There are critical questions upon which there is a mismatch between the views of those advocating and supporting the new forms of surveillance and those critical of it.

(1) What constitutes 'surveillance' and when does it occur? When data are gathered – when data are algorithmically analysed, or when it is viewed or analysed by humans?

CONTACT Paul Bernal paul.bernal@uea.ac.uk

(2) Is there a 'balance' to be found between competing rights of privacy and security – or is the setting up of such a balance misleading? Does surveillance have an impact beyond what is traditionally seen as 'privacy' – and can surveillance itself have a negative effect on security?

There are further crucial issues upon which there are disagreements; perhaps most importantly the question of whether surveillance by the state can be considered separately from surveillance by commercial organisations, or whether the two need to be considered together.

The answers to these questions are not as clear as they might immediately appear – they need careful unpicking. To help to achieve more clarity, this article looks at internet surveillance from a human rights perspective, using the framework of the European Convention of Human Rights ('ECHR') – a framework appropriate for analysis of UK surveillance as the convention rights are incorporated into UK law through the Human Rights Act 1998, and one of the most comprehensive and accepted formulations of human rights worldwide. It examines the impact that surveillance has upon the ways that people use communications and the internet, and hence upon how people live, and suggests that this impact has the potential to be far more significant than is commonly presented. Further, it suggests that the idea of a 'balance' between 'privacy' and 'security' is a misleading idea in itself: firstly because surveillance impacts upon far more than traditional privacy, and secondly because neither the concept of privacy, nor that of security, is as simple as it is often portrayed. Measures to protect privacy may improve security – and measures that purport to improve security may in other ways actually reduce that security.

This article is not intended as an exhaustive or detailed legal analysis. Indeed, legal analysis can only ever be part of the debate, particularly as it is questionable whether the law is ever really able to keep pace with either the technology or the way that people use it.[1] Rather, the article is intended to raise questions and open up debate. The examples used are not restricted to one state or jurisdiction; much of the best analysis and research, for example, comes from the US while the use by UK authorities of a 'neither confirm nor deny' policy, along with the natural secrecy associated with intelligence work, makes garnering information from the UK harder than it might be. The internet, moreover, is by its nature international – surveillance needs to be considered in that context, and the debate over it needs to be one that is not confined to individual states and their particular circumstances and particular laws. It is not just law but principles that are at stake, and the policies and practices of global corporations as well as government authorities.

1. A miscast debate

Communications surveillance had become a significant topic of political conversation, particularly in the UK, even before Edward Snowden made his leaks. The Communications Data Bill in 2012, dubbed by campaigners the 'snooper's charter', failed to make its way through Parliament after much debate and a highly critical analysis by the Joint Parliamentary Committee appointed to scrutinise it.

Since Snowden's revelations six months later, though there has been considerable debate on the subject, it has to a great extent been limited and miscast. When Sir Malcolm Rifkind, Chair of the Intelligence and Security Committee (ISC), announced the

first 'public' hearing of that committee, he said, 'There is a balance to be found between our individual right to privacy and our collective right to security.'[2]

This comment was repeated directly in the ISC's call for evidence in its inquiry into the intelligence services' interception of communications in December 2013 (ISC 2013) and remains a common argument. Andy Burnham MP, the Shadow Home Secretary, used it as the basis of his speech in the second reading of the Investigatory Powers Bill in March 2016.[3] It is not restricted to the UK. The 2016 Intelligence and Security Review in New Zealand, for example, repeated it in very similar terms: 'The debate about how best to balance the need for security and the privacy of individuals will continue for as long as both are seen as essential to a free society' (Cullen and Reddy 2016).

It is not just a theoretical discussion; in relation to the Investigatory Powers Bill, the bulk powers Codes of Practice explicitly discuss interference only with 'an individual's rights under Article 8' of the ECHR, not other rights, individual or collective.[4] These ideas reflect a relatively common misunderstanding of the issues at the heart of the debate over surveillance. Surveillance impacts not just upon individual privacy, but upon a wide range of human rights, from freedom of expression and freedom of association and assembly, to protection from discrimination – some because privacy acts as a gateway or guardian to those rights, and some independently of what is generally thought of as privacy. The impact is not just on individuals but on communities and other groups – and casting the debate as one of individual vs. collective rights is misleading, as it inappropriately downplays the significance of surveillance. The nature of the impact of surveillance needs to be understood better if a more appropriate balance is to be found between people's rights and liberties and the duties of states both to provide security and to protect freedoms for their citizens.

That such a rebalancing exercise is necessary has been emphasised by the ruling of the Court of Justice of the European Union ('CJEU') in the Digital Rights Ireland case in April 2014, that the Data Retention Directive (Directive 2006/24/EC) was invalid. The Data Retention Directive effectively required communications providers to retain specified communications data (as defined within the directive) for a period of between 6 and 24 months, as determined by the member state, and to make that data available to 'competent national authorities'. As the CJEU put it, referring to the rights set out in Articles 7 and 8 of the Charter (rights to respect for private and family life and to protection of personal data):

> … Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.[5]

Article 7 of the Charter is the equivalent of Article 8 of the ECHR, whilst Article 8 of the Charter confirms that protection of personal data is itself a fundamental right – a point which is critical to understanding the significance of the gathering and retention of such personal data.

Effectively, the CJEU ruled that the interference with these fundamental rights was disproportionate, noting for example that it 'applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime'[6] and that it 'fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data'.[7] In essence, the CJEU could be viewed as asking for the balancing exercise to

be made explicit and appropriate. The full impact of the Digital Rights Ireland case is still not clear – particularly with a legal challenge to the UK's replacement of their implementation of the Data Retention Directive currently being reviewed by the CJEU.[8] The success or failure of that challenge, however, will not alter the CJEU's analysis that the retention of data itself engages these fundamental rights.

2. 'New' forms of surveillance

The various leaks by Edward Snowden revealed some of what can be described as 'new' forms of surveillance, as have recent legislative measures in the UK, from 2012's failed Draft Communications Data Bill to the Investigatory Powers Bill proceeding through parliament in 2016.[9] Much of this had been previously a matter primarily of speculation – that speculation driven in the UK, to an extent, by the 'neither confirm nor deny' policy of the intelligence and security agencies. Now, however, more is being revealed and there do appear to be some identifiable characteristics that differentiate these forms of surveillance from the more 'traditional' techniques such as analogue phone-tapping, photography, listening devices and so forth:

(1) The focus of surveillance activities is on 'metadata' or 'communications data' as much as on 'content' – though these terms are far from clear or separate. This focus appears not to be out of a desire to protect privacy, though the need to comply with what might loosely be described as 'traditional' laws protecting the privacy of communications appears to play a role, but because the metadata/communications data can be just as revealing, though in different ways, and is more easily analysed and processed.
(2) They operate on a 'gather in bulk, access in detail' basis. The question of whether this constitutes 'mass surveillance' is one of the key parts of the debate, but may as discussed below, be a largely semantic argument. What is clear is that surveillance law and practice as it currently exists, and is being legally proposed, involves gathering of massive amounts of data. In the Investigatory Powers Bill, for example, there are a whole series of 'bulk powers'[10] – bulk interception, bulk acquisition of communications data, bulk equipment interference, 'bulk personal datasets' ('BPDs') – where there are no limits on how 'bulky' the bulk might be.[11] The Investigatory Powers Bill also allows for 'thematic warrants'. As the Home Office's Operational Case for Bulk Powers set out: '[i]t is entirely possible for a targeted "thematic" [equipment interference] warrant to cover a large geographic area or involve the collection of a large volume of data' (Home Office 2016). The Investigatory Powers Bill considers this to be 'targeted' rather than bulk, but the volume of data makes that argument a largely semantic one. Some of these powers would have been considered 'surveillance' in the past – interception, for example – but some would not, such as the acquisition of BPDs directly from commercial operators.
(3) They work *with* commercial data gatherers. Through the PRISM programme, for example, the NSA claimed to have 'direct access' to the servers of nine of the big commercial operators: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. How this takes place and the extent of the cooperation and knowledge of the commercial operators remains unclear. What is clear, however, is that the newer

forms of surveillance access and use commercially gathered data and commercial surveillance – and that they benefit from the profiling and analysis methods of commercial operators. The 'bulk powers' in the Investigatory Powers Bill include acquisition of communications data directly from commercial data gatherers, whilst the BPDs in the same bill would often be acquired directly from these commercial data gatherers.

These issues are not of themselves new – commercial operators have cooperated with government surveillance since the earliest days of telecommunications for example – it is the combination of these factors that creates the 'new' kind of surveillance.

2.1. Surveillance in a new internet

What also makes this kind of surveillance new is the way that we use the internet. In particular the way that the internet is used for almost every aspect of our lives. It is not just a means of communication, it is a way that we manage our social lives, apply for jobs, seek information about our health, do our shopping, our banking, seek and find romance, choose and consume entertainment and much more. The implications of this are considerable: even to the extent that although surveillance techniques are not all new, their relationship to people's lives and their potential impact is new.

The growth of social networking sites and the development of profiling and behavioural tracking systems and their equivalents change the scope of the information available: it is not just information that we impart deliberately that is available, but information derived from analysis of that information and from our behaviour can also become available. In parallel with this, technological developments have changed the nature of the data that can be obtained by surveillance – for example the increased use of smartphones and related technologies provides new dimensions of data such as geolocation data and biometric data including facial recognition and fingerprints, and allows further levels of aggregation and analysis.

This combination of factors means that the 'new' surveillance is both qualitatively and quantitatively different from 'traditional' surveillance or interception of communications. Where traditional 'communications' was seen as a subset of traditional privacy rights, as reflected in its part within Article 8 of the ECHR, the new form of communications has a much broader relevance, a wider scope, and brings into play a much broader array of human rights.[12] The surveillance too is different – and the impact that it can have is different: more extensive, more multifaceted and with a greater impact on the people subjected to it.

The nature of the technology also means that surveillance that would have been overwhelmingly expensive, as well as immensely challenging on a practical level, has now become relatively simple and inexpensive, and hence, for governments, attractive. Programmes that work along these lines are widespread. In France, what was described by *Le Monde* in 2013 as 'le Big Brother français' was passed in 2015[13] – an intelligence-gathering law which includes provisions for mass retention of communications metadata – whilst in Australia, the Telecommunications (Interception and Access) Amendment (Data Retention) Act of 2015 works upon essentially the same basis. The controversial FRA:Lagen in Sweden includes similar provisions (Klamberg 2010) and in Belgium a 'Royal Degree' in September 2013 appears to provide equally extensive powers. India's 'Central Monitoring

System' – perhaps even more intrusive – is reported to be rolling out in 2016. The extent to which more seemingly repressive regimes utilise these kinds of technologies is largely a subject of conjecture; it is a reasonable assumption that it is used extensively.

2.2. Metadata vs. content

Politicians and members of the intelligence community have been at pains to point out that these programmes do not involve the content of communications. US President Barack Obama made it the focus of his first address after the revelations of Edward Snowden, on 7 June 2013. 'Nobody is listening to your telephone calls', was a point he emphasised. William Hague, then UK Foreign Secretary, addressing Parliament about the UK's involvement with PRISM and related programmes, was similarly adamant and similarly focused: '[o]ur laws do not provide for indiscriminate trawling for information through the contents of people's communications'.[14] Former GCHQ Director Sir David Omand told the BBC on 8 October 2013 that 'nobody is reading all your emails'.

In human rights law, however, the significance of metadata has been noted since 1984. In Malone,[15] the European Court of Human Rights ('ECtHR') ruled that release of records of 'metering' – the analogue telephony equivalent of metadata – to the police amounted to interference with Article 8 of the ECHR. In practice, furthermore, metadata can be more helpful for surveillance than content. Metadata by its nature is more easily analysed and aggregated. The formats are standardised, much of it is numeric and can be subjected to quantitative analysis – particularly significant in the 'big data'. Moreover, content can be written in indirect forms, working by innuendo or in language not easily or automatically understandable. On the kinds of scales envisaged by mass surveillance, the idea of actually 'reading' or 'listening' to content is not practical until the very latest stages of analysis. Content is much more easily and regularly encrypted than metadata. Finally, metadata can include new types of data such as geolocation data, data about devices used and so forth. Metadata is not less intrusive than content: it might best be described as 'differently intrusive'.

2.3. What is 'Surveillance' and when does it occur?

In her evidence to the Joint Parliamentary Committee on the Draft Investigatory Powers Bill in January 2016, the then Home Secretary Theresa May stated categorically that the UK does not engage in mass surveillance (JPCIPB 2016). The Investigatory Powers Bill uses the word 'bulk' rather than 'mass' – and quite how 'bulky' these 'bulk' powers really are remains less than clear, despite the issuance of detailed codes of practice. A similarly semantic argument was the key element in the CJEU's striking down of the 'Safe Harbour' agreement over data sharing between the European Union and the United States in the Schrems case.[16] Advocate General Bot said that 'interference with fundamental rights is contrary to the principle of proportionality, in particular because the surveillance carried out by the United States intelligence services is mass, indiscriminate surveillance' (CJEU 2015). The US response was immediate: its Mission to the European Union stated that '[t]he United States does not and has not engaged in indiscriminate surveillance of anyone, including ordinary European citizens' (US Mission 2015).

David Lyon, in *Surveillance Studies: An Overview* defined surveillance as 'the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction' (Lyon 2007), a description which captures the essence of surveillance but still leaves significant questions to be answered. What is 'attention' and when can it be 'focussed' – and by whom or what? In the context of data surveillance there are, very broadly speaking, three stages: the gathering or collecting of data, the automated analysis of data (including algorithmic filtering), and then the 'human' examination of the results of that analysis of filtering.

This is where the difference in views as to whether the UK and US engage in 'mass surveillance' lies: the CJEU and privacy advocates could argue that the 'surveillance' happens at the first stage – when data are gathered or collected – while the UK and US governments could argue that it happens at the third stage – when human beings are involved.

If the surveillance occurs when data are gathered, there is little doubt that many of the modern forms of surveillance, including powers envisaged by the Investigatory Powers Bill, would constitute mass surveillance. Data are gathered in massive quantities through the various 'bulk' powers, as well as the 'Internet Connection Records' – effectively a truncated form of browsing history, to be created and retained by communications providers on all their subscribers.[17] If, however, surveillance only occurs when human beings are involved in the process, then Theresa May can argue her point, as can the US Mission to the European Union: the amount of information looked at by humans may well not be 'massive' or 'indiscriminate' regardless of how much data are gathered.

In Lyon's terms, the answer may lie more accurately in the complex, multifaceted second stage of the process, where automated algorithmic analysis is applied. What an algorithm does could be described as 'focused, systematic and routine attention' to data. In the future this is likely to be more significant; in commercial terms surveillance by algorithm is already more important than surveillance by human eyes, ears and minds, as the business models of Google, Facebook and others demonstrate. Algorithmic analysis, however, depends on the prior gathering of data on a large scale – something, therefore, in which governments and businesses have a shared interest.

In the end, however, the question of whether data gathering or algorithmic analysis constitutes 'surveillance' is largely a semantic point. Many of the key risks occur when data are gathered – the existence of data creates the risk. As a consequence it is at the data-gathering phase that the first privacy invasion occurs, regardless of whether that phase is described as surveillance or not. This has been reflected consistently in rulings at both the CJEU[18] and of the ECtHR.[19]

2.4. Overt and covert surveillance

Overt surveillance brings the Panopticon effect into play. The premise of Bentham's Panopticon was not that prisoners would be observed all the time, but that they would be aware that they might be observed at any time, and would curb their behaviour accordingly. That, in effect, is exactly what the kind of internet surveillance systems being discussed here would do. The idea that the authorities would be able to look at anything, either through access to archives or access to real time feeds, precisely mirrors Bentham's envisaged observation capabilities of prison guards. From Bentham's perspective, the Panopticon was an appropriate way to deal with potentially violent offenders. The

problem with the internet surveillance Panopticon is that it treats all people as potentially violent offenders.

Covert surveillance has risks that are qualitatively different. In *The Dangers of Surveillance* Richards outlines what is perhaps the most significant aspect: the way that surveillance, and covert surveillance in particular, gives the watchers power over those who they watch.

'It might sound trite to say that "information is power," but the power of personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion' (Richards 2013).

These three dangers are representative of one of the key aspects of surveillance: it provides tools to enable influence and control. They help explain why authoritarian regimes have used data gathering as one of the key tools to create conformity and reduce the risk of dissent.[20] It is an effect recognised both in the past and present, and with implications for the future. Emily Taylor notes that, 'The human rights impact of data retention on the ability to create profiles, or to confirm a future suspicion, has rightly been highlighted as a human rights risk by commentators as diverse as Cardinal Richelieu and Evgeny Morozov' (Taylor 2016, referring to Morozov 2014).[21]

This 'power effect' applies to overt as well as covert surveillance, though not in exactly the same way; having information gives power, but having information that the subject does not know that you have gives a different kind of power. This applies particularly to the discrimination and persuasion aspect: the subject might not know either that they are being discriminated against or persuaded or that it is possible for that to happen.

2.5. Surveillance as a harm in itself

One of the conclusions of Richards' analysis is to recognise that surveillance is harmful in itself. This is a fundamental issue, hitting at the ideas of liberty that have been discussed for many centuries. This is historian Quentin Skinner:

> I think it very important that the mere fact of there being surveillance takes away liberty. The response of those who are worried about surveillance has so far been too much couched, it seems to me, in terms of the violation of the right to privacy. Of course it's true that my privacy has been violated if someone is reading my emails without my knowledge. But my point is that my liberty is also being violated, and not merely by the fact that someone is reading my emails but also by the fact that someone has the power to do so should they choose.[22]

Skinner's argument is about the existence of the system – and hence about the data gathering rather than the human examination. That is the logic behind the recognition by the ECtHR that data gathering in itself engages Article 8 of the ECHR directly. This can be traced back to Klass v. Germany in 1978, where it was ruled that:

> … in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence.[23]

The conclusion drawn by the court in *S and Marper v. the United Kingdom* in 2009, that 'the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data'[24] is a logical extension of this analysis. It is the development of systems and laws to allow *the gathering* of that data that produces the menace of surveillance, not that allows the *examination or use* of the data gathered. It is the gathering stage, therefore which should start the rights-balancing exercise. This understanding underlies subsequent rulings of both the ECtHR[25] and the CJEU.[26] In Szabo v Hungary in 2016, the ECtHR noted that this point was becoming increasingly significant:

> Given the technological advances since the Klass and Others case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life even more acutely.[27]

Not only are the risks and harms already in play by the gathering stage, but the key possibilities of data vulnerability and function creep come to the fore. Once the data have been gathered or the surveillance system put in place, both data and systems are vulnerable to 'intentional' or accidental misuse or loss by authorities or vulnerability to misuse by others.

Data gathered by surveillance is vulnerable in all the same ways that other data are vulnerable: vulnerable to misuse, to misappropriation, to hacking, to loss, to corruption and error, and to what is loosely described as 'function creep'. Security services and other authorities are not immune to that vulnerability – as the leaks through WikiLeaks, the revelations of Edward Snowden, the numerous data losses by the Ministry of Defence and others have demonstrated (Bernal 2014, Chap. 7). The surveillance systems themselves are vulnerable: build a back door into a system and it is not only those who are intended to use it who can use it as a way to access that system. Install a 'black box' into an internet service provider's premises and that black box can itself be hacked and accessed.

2.6. Surveillance damaging security?

This also means that though the general argument made is that building surveillance systems and gathering data is to improve security – a term that is itself very hard to define – it can also both in practice *damage* security and increase risks. There are further arguments in that direction. Former NSA Technical Director William Binney noted in his evidence to the Joint Parliamentary Committee on the Investigatory Powers Bill that:

> … over the last fifteen years, the bulk collection approach has cost lives, including lives in Britain, because it inundates analysts with too much data. It is 99 per cent useless, as attacks occur when intelligence and law enforcement lose focus on previously suspected terrorists and fail to find accomplices or others enabling fresh attacks. (JPCIPB 2016)

This is Bruce Schneier in Data and Goliath in 2015:

> Terrorist plots are different [from the kind of commercial fraud that data mining has worked well in detecting], mostly because whereas fraud is common, terrorist attacks are very rare. This means that even highly accurate terrorism prediction systems will be so flooded with false alarms that they will be useless.

> … In the years after 9/11, the NSA passed to the FBI thousands of tips per month; every one of them turned out to be a false alarm. The cost was enormous, and ended up frustrating the FBI agents who were obliged to investigate all the tips. (Schneier 2015)

Former Shadow Home Secretary, David Davis MP, made a similar point in the House of Commons debate on the Investigatory Powers Bill in March 2016: '[t]here are genuine concerns that the collect-it-all approach actually makes things worse'.[28]

These views are contested – not least by GCHQ – but they do open the question as to whether the bulk data collection approach is straightforwardly positive for security from terrorism and similar dangers. That in turn adds doubt to the 'privacy vs. security' dichotomy, and the possibility that data gathering and surveillance could do harm to both privacy *and* security. There are further, more abstract arguments in the same area, with some backing from history: where excessive 'security' measures are brought in they can lower the level of trust and, as a consequence, lower levels of cooperation with authorities, which again could damage rather than help security. The idea that 'tightening' security actually improves security is one that should not be taken at face value.

3. The impact on human rights

Surveillance in its new form has human rights implications beyond the obvious-seeming intrusions into privacy of correspondence – one aspect of Article 8 (1) of the ECHR – into people's private lives themselves, and further, upon Articles 6, 9, 10, 11 and 14 of the ECHR. Privacy is not the only issue – partly because privacy underpins other rights (and in particular rights that are very much not individual, such as freedom of association and assembly) and partly because of the nature of the internet and how we now use it. To focus only on privacy can make the risks of surveillance seem less significant than they are and hence set the criteria upon which it is decided whether surveillance is appropriate or legitimate, too low.

3.1. Article 8: right to respect for private and family life

> Everyone has the right to respect for his private and family life, his home and his correspondence.[29]

Great play has been made by politicians that the new surveillance does not include the 'content' of calls, just the metadata. As computer scientists and others have pointed out, this largely misses the point. As Professor Edward Felten put it in the context of telephony:

> … analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the content of communications. That is, metadata is often a proxy for content.[30]

Felten was writing about telephony metadata, but the data gathered by internet surveillance covers far more than that, and can be even more revealing. Internet surveillance can, without even considering content, provide more information about someone's communications, and in a far more accessible form, than conventional wiretapping even where that conventional wiretapping would have included contents.

Article 8 provides for protection for private and family life as well as for correspondence. On the surface, it might appear that 'communications data' relates to the 'correspondence' part of Article 8 – communications like telephone calls, emails, text messages and tweets fit into this category – but internet communications data have a broader impact upon the 'private life' aspect of the Article. Web-browsing data can be used to uncover far more intimate, important and personal information than is immediately obvious. It shows which websites are visited, which search terms are used, which links are followed, which files are downloaded – and also when, and how long sites are perused, using what kind of computer, phone or other device and so forth. When the other data that is being gathered through commercial and governmental internet surveillance – from traditional communications data like email, text messages and phone calls to music listened to on Smartphones, geolocation data, etc. – is added to this, aggregated and analysed, the potential becomes even greater.

This data can reveal habits, preferences and tastes – and can uncover, to a reasonable probability, religion, sexual preferences, political leanings and more. It can dig deep into personal lives. People use the internet to establish and support personal relationships, to find jobs, to bank, to shop, to gather the news, to decide where to go on holiday, to concerts, museums or football matches. Some use it for education and for religious observance – checking the times and dates of festivals or details of dietary rules. There are very few areas of peoples lives that remain untouched by the internet.

Furthermore, analytical methods through which more personal and private data can be derived from browsing habits have already been developed, and are continuing to be refined and extended, for example by the behavioural advertising industry. Significant amounts of money and effort are being spent in this direction – it is a key part of the business models of Google, Facebook and others. The profiling and predictive capabilities will develop further both in scope and in accuracy in the future.

This is not profiling in the conventional 'psychological' form, based on educated guesses and theoretical associations: it is mathematical profiling, based on correlations determined by comparisons of massive amounts of data. The techniques and technologies developed to profile for advertising can be applied just as easily to other forms of profiling, whether they be political, religious, ethnic or any other kind. Data gathering can therefore impact upon any aspect of a private life.[31]

3.2. Article 9: freedom of thought, conscience and religion

> Everyone has the right to freedom of thought, conscience and religion … [32]

This kind of profiling can also bring Article 9 into play. It can be possible to determine (to a reasonable probability) individuals' religions, politics and philosophy, the languages they use and even their ethnic origins,[33] and then use that information to monitor them both online and offline. It could potentially be used to limit or control the activities of people that fit within a particular religious outlook – and it can also be used to limit the related rights to freedom of association and assembly.

Although it could be seen as a stretch to suggest that such profiling might allow a profiler to know what someone is thinking, that, effectively, is its aim. Apple Google and Microsoft's 'digital assistants', Siri, Now and Cortana respectively, all aim to predict what

you want to know.[34] Indeed, it has been argued that Google and Facebook can know people better than they know themselves, as they are free from 'self-deception'.[35] From the perspective of the profiler (and the commercial profiler in particular) precise accuracy may not be crucial; a reasonable probability may be all that is needed. From the perspective of those being profiled, the situation is very different – and problems may arise from both accurate and inaccurate profiling. A real 'dissident', for example, may be located and imprisoned by an accurate profile, while an 'innocent' may be unfairly punished by an inaccurate profile.[36] Further, as discussed in more depth in Section 3.6 below, there is a growing potential for discrimination on the basis of these profiles.

3.3. Article 10: freedom of expression

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers … [37]

Though the connection between freedom of expression and privacy may not be obvious – indeed, the two may appear at times to be in conflict – for freedom of expression to function properly there must be a degree of privacy. There are direct impacts on journalism – as US journalism professors noted in their 'Comment to the Review Group on Intelligence and Communications Technologies',[38] including reducing the trust required for confidential discussions with sources, chilling effects not just in terms of the output of journalism but the correspondence and communications – the research – that is fundamental to that journalism.

There are particular issues in relation to sources. As Lord Woolf CJ put it, 'The fact that journalists' sources can be reasonably confident that their identity will not be disclosed makes a significant contribution to the ability of the press to perform their role in society of making information available to the public.'[39]

After revelations involving the Metropolitan Police and Kent Police Service in 2014, the Interception of Communications Commissioner's Office (IOCCO) undertook an inquiry into the use of the Regulation of Investigatory Powers Act to identify journalistic sources. This inquiry revealed that in a three-year period '19 police forces reported undertaking 34 investigations which sought communications data in relation to suspected illicit relationships between public officials (sources) and journalists. The 34 investigations concerned relationships between 105 journalists and 242 sources' (IOCCO 2015). IOCCO noted that:

> … even though the requirement to identify the source may appear, taking account of the requirements of Article 10, legitimate in order to investigate a serious crime or address matters relating to national security, the chilling effect or collateral impact is ever present.

IOCCO is not suggesting that this means that use of surveillance to identify journalistic sources is necessarily inappropriate, rather that the chilling effect needs to be part of the balancing exercise.

Privacy is not just important for journalists, but crucial for free expression in a wide range of other situations, from those dissenting against oppression, to those threatened by abusive spouses, to whistle-blowers and so forth. Without a reasonable expectation of privacy, many of these would simply choose not to speak out. Further, surveillance chills not only those *imparting* but those *receiving* information – both sides of the

Article 11 rights. If someone knows that their web browsing is monitored, the Panopticon effect will make them less likely to visit sites they believe the authorities might deem subversive or inappropriate.

UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, set out the issue in his report to the Human Rights Council in April 2013:

> States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy. Privacy and freedom of expression are interlinked and mutually dependent; and infringement upon one can be both the cause and consequence of an infringement upon the other. (La Rue 2013)

La Rue was writing before the Snowden's revelations; the scale of the surveillance subsequently revealed makes his comments even more apt. There is growing empirical evidence to support the existence of this kind of a chill in practice. In 2013, a report by PEN America, based on a detailed survey of writers in the light of the Snowden revelations, found amongst other things that 28% had 'curtailed or avoided social media activities' and another 12% had 'seriously' considered doing so, 24% had deliberately avoided certain topics in phone or email conversations. That survey data are reinforced by more recent academic analysis. In 2016 Jonathon Penney analysed traffic to privacy-sensitive Wikipedia articles and found statistically significant declines not only in the immediate aftermath of the Snowden revelations but in the long term. The chilling effect in terms of access to information is not just theoretical but empirically evidenced (Penney 2016). Further, Elizabeth Stoycheff's 2016 study of Facebook activity revealed that, ' … knowing one's online activities are subject to government interception and believing these surveillance practices are necessary for national security play important roles in influencing conformist behavior' (Stoycheff 2016).

That influence, Stoycheff concludes, is in effect a chilling of speech, particularly of minority opinion. Again it is important to note that this does not necessarily mean that surveillance is inappropriate – indeed, for security purposes a chill may be both intentional and desirable, such as the chilling of extremist speech – but nonetheless it should be considered when looking at the balancing exercise. Moreover, this tendency to conformity is not something new: Timothy Garton Ash noted it was part of the effect (and possibly the purpose) of Stasi data gathering and surveillance:

> More typical were the nice couple from whom the University had rented my room. Intelligent, well-educated, well-informed through watching Western television, they nonetheless devoted virtually all their energies to their private lives, and particularly to extending, decorating and maintaining their cottage on a small lake some half-an-hour's drive from Berlin. (Garton Ash 2009)

3.4. Article 6: the right to a fair trial

> In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law.[40]

Surveillance can interfere with legal processes in a number of ways. In a similar fashion to its interference with journalists' communications with their sources, surveillance can

interfere with lawyers' correspondence with their clients. As the Bar Council pointed out in their press release in relation to the Investigatory Powers Bill in March 2016:

> The fact that a person suspects that communications with his or her legal adviser may find their way to the opposing party, or may be subject to surveillance by intelligence agencies, means that they may then be inclined to tell only part of the truth. This has a 'chilling effect' on free and frank lawyer-client communication. (Bar Council 2016)

There is a potential for further impact: the power effect of covert surveillance applies directly in relation to both the police and prosecuting authorities. Access to information, and the ability to utilise that information, can directly and potentially prejudicially influence justice.

3.5. Article 11: freedom of assembly and association

> Everyone has the right to freedom of peaceful assembly and to freedom of association with others … [41]

The internet offers previously unimaginable tools for groups – and for assembly and association of all kinds. Online communities have developed, using services like social networking, instant messaging and message boards, and 'real world' groups have used the same tools to facilitate their 'real world' meetings and communications. In this way, the internet can often be seen as a force for 'good', for 'democracy'. Many commentators suggested that the internet played a key role in the Arab Spring – and though its role may well have been exaggerated, the internet was certainly used by many of those organising the resistance in Tunisia and Egypt in particular.

However, when communications, and in particular the internet, are used to organise meetings, to communicate as groups, and to assemble both offline and online, internet surveillance can become significant and dangerous. Meetings can be monitored or even prevented from occurring, groups can be targeted and members identified. Oppressive regimes throughout the world have recognised and indeed used this ability – in Tunisia, for example the former regime hacked into both Facebook and Twitter to attempt to monitor the activities of potential rebels.[42] The knowledge of the existence of surveillance, as Stoycheff noted, also tends to produce more conformist behaviour, which would impact directly on willingness to exercise freedom of both assembly and association and hence those freedoms themselves.

It is not just in extreme situations such as a political uprising that internet surveillance is relevant to association and assembly. Authorities in the UK, for example, have argued that it would be right to monitor social media during a riot – and with some justification – but what about a peaceful protest? Then what about those organising a protest, before the event? How about a trade union? It is easy to make a decision on an extreme case – but there are grey areas and the temptation for authorities to use tools once they are in place can be hard to resist.[43] In June 2013, for example, the UK government monitored social media activities concerning the controversial cull of badgers. With headlines such as that from the BBC that read, 'Whitehall chiefs scan Twitter to head off badger protests'[44] it is easy to see how this kind of surveillance can interfere with Article 11 rights.[45] When technologies like geolocation data are taken into account, allowing authorities to locate physically those wishing to assemble, that potential becomes even more significant and

relevant. In 2013 Electronic Frontier Foundation filed with a federal judge 22 separate examples from advocacy groups of how mass surveillance of telecoms data has 'impeded the groups' work, discouraged their members and reduced the numbers of people seeking their help via hotlines' (EFF 2013).

Another graphic example took place in Ukraine in January 2014. Whilst a protest was taking place in Kiev,[46] people whose mobile phones indicated that they were in the vicinity of the protest, were sent text messages saying that they 'ha[d] been registered as participating in mass disturbance'. Surveillance was used to locate the people, the phones themselves used to communicate that fact – as well as to attempt to intimidate people into not participating in further protests. There are many implications of this; interference with the rights of freedom of assembly and association is only part of the problem. The assumptions that being in the vicinity makes a person part of the protest, and that the owner of a phone is the person in possession of that phone at that moment are both problematic – that they have been 'registered' onto a database opens up further opportunities for abuse. This 'SMS bombing' might also have been intended to deter any further such protests – the 'conformity' effect noted by Stoycheff and Garton Ash. Both the Panopticon effect and the power effect apply in situations like this. Surveillance of this kind both chills expression and assembly, and increases the level of power that can be exerted by authorities over those involved, directly or indirectly. The increasing interactions between technologies – here the geolocation plus the communication capabilities of mobile phones – creates more possibilities. The internet of things and other new technologies will make this even more significant.

The interaction between governments and commercial and other organisations adds another dimension to this. Data gathered by governments may be passed on to, or be hacked or otherwise obtained by, other interested parties. If arms manufacturers get hold of data about anti-arms trade meetings, protests and protesters, they could stop the meetings or protests. In relation to the badger cull protests, for example, UK police suggested that they can and will pass personal information on protestors to the National Farmer's Union who represent the farmers supporting the cull.[47]

Surveillance need not invade privacy to infringe on Articles 10 and 11. Monitoring Twitter, as for the badger cull, does not directly invade privacy, as in general, tweets are public rather than private, but performing surveillance of those public tweets in order to 'head off' protests could potentially interfere with the expression, association and assembly rights involved in public protest. This hints at a more significant point: the power effect of gathering and holding data does not, primarily, impact upon *privacy* but autonomy. Whether data gathered are private is not the significant part; it is how the data may be used that matters.

3.6. Article 14: prohibition of discrimination

> The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.[48]

Not only can surveillance and profiling enable discrimination – it can potentially automate it. It may be possible to determine almost any kind of detail about a person online through

profiling: their age, religion, nationality, ethnic origin and more. Decisions and options available to a person may then be automatically controlled on the basis of that profiling – and the person involved may never even know what is happening. A website could assess the profile of the person visiting and change the options displayed dependent on any aspect of that profile – and this kind of 'personalisation' is being most actively developed by some key players on the internet.[49] In March 2016, for example, it was revealed that Facebook was showing different trailers for the same film based on the race to which it assessed the user belonged; not self-declared race, but assessed algorithmically using a system Facebook calls 'affinity groups'.[50]

In a similar way, automated processes and filters could pick out people whose profile suggests authority might want to examine them more closely – by religion, political views, union membership and so forth – engaging Article 8 in a discriminatory way. Similarly, people could be prevented from accessing information or even commenting on particular internet forums based on their profiles, impacting upon their Article 10 rights in a discriminatory way. The same is possible for Article 11 rights to assemble and associate – and all without direct human involvement.

Two 2014 reports following parallel reviews of 'big data practices' for the White House raised discrimination as an issue. John Podesta, whose task force put together one of the reports, *Seizing Opportunities, Preserving Values* (Podesta 2014), told Associated Press that he had 'newfound concern' over how big data 'could be used to target consumers and lead to discriminatory practices'. Concern over the potentially discriminatory effects of 'big data' practices is a key finding of the report, and addressing them one of its six recommendations.

Seizing Opportunities, Preserving Values and its parallel report, 'Big Data and Privacy: A Technological Perspective' (PCAST 2014), detail a number of such possibilities, including the suggestion that differential pricing is likely to become more prevalent and less transparent. That such opportunities arise from commercial practices means similar practices become equally possible for government agencies. As *Seizing Opportunities, Preserving Values* notes:

> Powerful private-sector profiling and data-mining technologies are not only used for commercial purposes. State, local and federal agencies purchase access to many kinds of private databases for legitimate public uses, from land management to administering benefits … some legal scholars and privacy advocates have already raised concerns about the use of commercial data service products by the government, including law enforcement and intelligence services.

It would be naïve to suggest that government agencies would only use data mining, profiling and related processes for transparent and clearly legitimate purposes – and not in more opaque circumstances and for less obviously legitimate purposes. One of the most notable features of the programmes revealed has been their lack of transparency; even people who are experts in the field seemed to have been genuinely surprised by their existence.

3.7. Necessary in a democratic society?

The key ECHR Articles referred to above are subject to qualifications. This is Article 8 (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.[51]

There are similar caveats in articles 6, 9, 10 and 11. The reference to data gathering and surveillance being 'necessary in a democratic society' is the crux of the issue. In what way and to what extent, can they be considered 'necessary' in a democratic society?

Data gathering and surveillance can interfere significantly with a wide spectrum of individual human rights. Given this, the bar should be very high in terms of the 'need' for that surveillance – and proper evidence should be presented and scrutinised before that 'need' is accepted. The evidence provided by the US and UK authorities in public, has been very limited to date. In the US it has tended to collapse under close scrutiny[52] whilst in the UK the combination of the government policy of 'neither confirm nor deny' and the private hearings of both the Investigatory Powers Tribunal and the Parliamentary ISC means that verification of claims of the effectiveness and need for surveillance, and mass data gathering in particular, is very difficult

It is becoming insufficient for the authorities to say, 'Trust us' when this level of interference with human rights is possible. Indeed, the prime motivation for the establishment of the various human rights treaties and conventions was precisely because authorities had demonstrated that they could not be trusted, and that they needed to be able to be held accountable. As David Anderson QC, the Independent Reviewer of Terrorism Legislation, put it, 'the road to a better system must be paved with trust' (Anderson 2015).

A key difference between a 'democratic society' and an authoritarian society – or even what might be labelled a 'police state' – is related to assumptions and defaults. In a police state the assumption is one of suspicion and distrust. People are assumed to be untrustworthy and generalised and universal surveillance makes sense; the legal, technical and bureaucratic systems are built with that universal surveillance in mind. The police states with which most people are familiar demonstrate this graphically: former communist countries, such as East Germany and Romania, relied on the most extensive secret police systems possible at the time: the Stasi and Securitate. They gathered data on a massive scale, using whatever methods were available at the time.[53] As Vaizey put it, ' … the Stasi had observed and photographed people's movements, secretly searched their homes, listened in to their telephone conversations, and even collected smell samples in jars, the idea being that trained sniffer dogs could tell where a person had been' (Vaizey 2014).

The parallels between this and the current data-gathering practices on the internet should be clear. The more despotic regimes currently holding power around the world follow that kind of logic; monitoring social networks and controlling the internet is a key part of that.[54] Everyone is a suspect: everyone might be a terrorist, a subversive, a paedophile, a criminal.

In a democratic society, the reverse should be true – people generally assumed to be trustworthy and worthy of respect, with the 'criminals', 'subversives' and 'terrorists' very much the exception. The powerful idea of 'innocent until proven guilty' is a reflection of this. The key to a democratic society is not that the people should 'trust' the authorities – but that the institutions are set up with sufficient limitations in their power: with

oversight, accountability and transparency. It is not the authorities themselves that need to be trusted, but those systems, checks and balances. Further, in a democratic state, policing is intended to be by consent, as set out in the 'Peelian Principles' established by Sir Robert Peel, the founder of the original Metropolitan Police. The police 'represent' the people, enforcing rules and laws that the people generally believe in and support.[55]

If it is understood that the gathering of data has an impact on a broad range of the rights of citizens, then the consequence is direct: gathering data on citizens as a matter of course, regardless of guilt or innocence, fits much more closely with the methods of the Stasi than it does with a classically democratic society. Gathering data on a massive scale – whether it is to be considered to amount to surveillance or not – cannot therefore be said to be 'necessary in a democratic society' without cause.

4. Recasting the debate

Arguments over surveillance will remain critical for the foreseeable future. There is no prospect either of mass internet surveillance being accepted by all, or of being abandoned by the authorities in any modern state. That makes the debate over how that surveillance should happen, what limits should be placed upon it, how it should be overseen and the legislation under which it operates, a crucial one – and means that the terms under which the debate takes place need to be appropriate.

- First of all, the debate over what *is* or *is not* surveillance needs to be put to one side. It is largely a semantic argument once it is understood that the gathering of data itself has an impact. The argument that controls only need applying at the stage where 'human eyes' are involved is no longer tenable.
- Secondly, that this impact is not just on privacy but on a broad range of rights – and indeed on autonomy and freedom in almost every aspect of our lives.
- Thirdly, these are not just 'individual' rights, but rights that relate to our functioning as a community, such as freedom of association and assembly, as well as freedom of expression.
- Fourthly, the idea that data-gathering and surveillance activities are necessarily positive for security is challengeable.
- Fifthly, metadata or communications data is not *less* intrusive than 'content', but *differently* intrusive. The legal approach to surveillance and data gathering should not assume that collection or examination of metadata requires a lower level of scrutiny or accountability.
- Sixthly, data gathering and surveillance involves both commercial and governmental organisations, and to consider them separately is to misunderstand the nature of both. The government uses data gathered by commerce, methods developed by commerce and piggyback on systems used by commerce.

The result of all this is that the balancing exercise required to determine whether data gathering and surveillance is justified needs to be recalibrated: the benefits of that surveillance need to be much greater than if they were only impacting upon individual privacy. Perhaps most importantly this means that the gathering and holding – or requiring of others to hold – communications data needs to be taken more seriously. To put the

primary controls in place only at the accessing stage – and to consider the balancing exercise only at that stage – is to misunderstand the risks associated with the gathering and holding of this data. As the UN Special Rapporteur on the right to privacy put it, when assessing the Investigatory Powers Bill: 'It would appear that the serious and possibly unintended consequences of legitimising bulk interception and bulk hacking are not being fully appreciated by the UK Government' (Cannataci 2016).

Statements such as Theresa May's that 'the UK does not engage in mass surveillance' though semantically arguable, are in effect deeply unhelpful. A more accurate statement would be that

> the UK engages in bulk data gathering that interferes not only with privacy but with freedom of expression, association and assembly, the right to a free trial and the prohibition of discrimination, and which puts people at a wide variety of unacknowledged and unquantified risks.

Whether the benefits from this bulk data gathering are sufficient to outweigh this interference with rights and generation of risks can only be assessed if the interference with rights and level of risk is appropriately acknowledged.

Finding a more appropriate balance does not just matter at the level of lawmaking. Decisions about surveillance and data-gathering activities are made at many levels, including the practical and operational level, based on the understanding that the authorising person has of the impact of those activities. Whilst that understanding underestimates the impact of the data gathering or surveillance, those decisions may be misjudged, again at every level, from the most strategic policy level to the most practical and operational.

All the factors discussed in this article are increasing in importance and in impact. As technology develops, as algorithms improve, as the volume and nature of the data increases so do all these pressures, and the current miscasting becomes more significant. Add into the picture developments such as the Internet of Things and this accelerates even faster. Laws and policies based on the current understanding and debate will become even less relevant, even less manageable and even less effective than they are now. That, in the end, is not sustainable.

Notes

1. See, for example, Reed (2012).
2. Quoted by the BBC (17 October 2013).
3. Parliamentary Debates, Commons, 6th series, vol. 607 (825).
4. For example the Bulk Acquisition Draft Code of Practice 3.8, the Security and Intelligence Agencies' retention and use of bulk person datasets 4.11. https://www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice.
5. In *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, Court of Justice of the European Union (8 April 2014).
6. Ibid. para 58.
7. Ibid. para 60.
8. Referred to the CJEU by the Court of Appeal in *the Secretary of State for the Home Office v. Davis, Watson and others* (2015). EWCA Civ 1185.
9. The version of the Investigatory Powers Bill referred to in this article is that passed by the House of Commons in its second reading in March 2016.
10. Set out in Parts 6 and 7 of the Investigatory Powers Bill (2016).

11. The 'Security and Intelligence Agencies' Retention and Use of Bulk Personal Datasets Draft Code of Practice' defines a BPD as follows:

> a set of data comprises a BPD where it includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the Security and Intelligence Agencies in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.

12. Arguments concerning the breadth of rights impacted upon by earlier forms of surveillance law were set out in Bernal (2012).
13. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Online at http://www.assemblee-nationale.fr/14/dossiers/renseignement.asp.
14. Parliamentary Debates, Commons, 6th series, vol. 564 (42).
15. Malone v. The United Kingdom, Application no. 8691/79 (2 August 1984).
16. In Case C-362/14, Maximillian Schrems v Data Protection Commissioner (6 October 2015).
17. Investigatory Powers Bill, Part 4 (Internet Connection Records), Parts 6 (Bulk Powers) and Part 7 (Bulk Personal Data Sets).
18. Most recently in Digital Rights Ireland (n4) and Schrems (n9).
19. Most recently in Zakharov vs. Russia, Application no. 47143/06 (December 2015).
20. See Sections 3.3 and 3.7.
21. The epigram attributed to Richelieu 'Only give me six lines written in the hand of the most honest man, and I will find something there to hang him by.'
22. Skinner (2013) interview with Richard Marshall: https://www.opendemocracy.net/ourkingdom/quentin-skinner-richard-marshall/liberty-liberalism-and-surveillance-historic-overview.
23. Klass and others v Federal Republic of Germany, ECtHR, 2 EHRR 214 (6 September 1978) para 41.
24. *S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, ECtHR, 48 EHRR. 50, (4 December 2008) para 121.
25. E.G. Zakharov (n19).
26. E.G. Digital Rights Ireland (n5) and Schrems (n16).
27. *Szabó and Vissy v. Hungary*, Application no. 37138/14, ECtHR (16 January 2016) para 53.
28. Parliamentary Debates, Commons, 6th series, vol. 607 (866).
29. ECHR Article 8 (1).
30. Declaration of Professor Edward W Felten in *ACLU v Clapper and others*, Case No. 13-cv-03994 (WHP) at the United States District Court, Southern District of New York, p14. Online at http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf.
31. See Bernal (2012) for earlier iterations of these arguments.
32. ECHR Article 9 (1).
33. This is already being done by Facebook – see n35.
34. See for example http://searchengineland.com/how-google-now-siri-cortana-predict-what-you-want-229799.
35. See for example James Carmichael in http://www.theatlantic.com/technology/archive/2014/08/google-knows-you-better-than-you-know-yourself/378608/ and Jon Evans in http://techcrunch.com/2015/10/24/when-facebook-knows-you-better-than-you-know-yourself/.
36. See Bernal (2012) for earlier iterations of these arguments.
37. ECHR Article 10 (1).
38. Bell et al. (2013).
39. In *Ashworth Hospital Authority v MGN Ltd [2002] 4 All ER 193, 210,* Quoted in IOCCO (2015).
40. ECHR Article 6 (1).
41. ECHR Article 11 (1).
42. For a general discussion of this role for the internet, see Morozov (2011).

43. See Bernal (2012) for an earlier iteration of this argument.
44. See http://www.bbc.co.uk/news/uk-politics-22984367.
45. See also Brown (2013).
46. See for example http://www.nytimes.com/2014/01/22/world/europe/ukraine-protests.html?_r=0.
47. See for example http://www.youtube.com/watch?v=6YimFEFvTzY.
48. ECHR Article 14.
49. See Bernal (2012).
50. See http://uk.businessinsider.com/why-straight-outta-compton-had-different-trailers-for-people-of-different-races?
51. ECHR Article 8 (2).
52. See for example Benkler (2013).
53. For descriptions of the methods of the Stasi, see for example Garton Ash (2009) or Vaizey (2014).
54. It is hard to measure 'internet freedom' in an objective way. But Freedom House's annual survey of internet freedom, gives some indication: the five countries rated 'least free' in 2015 were China (1st), Syria, Cuba, Bahrain and Vietnam (Freedom House 2015) whilst in Reporters Without Borders' 2013 special edition on Internet Surveillance listed the five 'State Enemies' as Vietnam, Bahrain, Syria, Iran and China (Reporters Without Borders 2013).
55. Set out in detail by the UK government in https://www.gov.uk/government/publications/policing-by-consent.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on contributor

Dr Paul Bernal is a Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School. He is the author of Internet Privacy Rights: Rights to Protect Autonomy, published by Cambridge University Press in 2014.

References

Anderson, David. 2015. *A Question of Trust, Report of the Investigatory Powers Review*. https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/.

Bar Council. 2016. *Press Release*. http://www.barcouncil.org.uk/media-centre/news-and-press-releases/2016/march/investigatory-powers-bill-second-reading/.

Bell, Emily, Ethan Zuckerman, Jonathan Stray, Sheila Coronel, and Michael Schudson. 2013. *Comment to Review Group on Intelligence and Communications Technologies Regarding the Effect of Mass Surveillance on the Practice of Journalism*. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf.

Benkler, Yochai. 2013. "Fact: The NSA Gets Negligible Intel from Americans' Metadata." http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

Bernal, Paul. 2012. *The Draft Communications Bill and the ECHR*. Blog: UK Constitutional Law Association. https://ukconstitutionallaw.org/2012/07/11/paul-bernal-the-draft-communications-bill-and-the-echr.

Bernal, Paul. 2014. *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge: Cambridge University Press.

Brown, Ian. 2013. *Online Freedom of Expression, Assembly, Association and the Media in Europe, Report to the Council of Europe*. http://www.coe.int/t/dghl/standardsetting/media/Belgrade2013/Online freedom of expression, assembly, association_MCM(2013)007_en_Report_IanBrown.pdf.

Cannataci, Joseph A. 2016. *Report of the Special Rapporteur on the Right to Privacy*. Human Rights Council. http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc.

CJEU. 2015. *Press Release*. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf.
Cullen, Sir Michael, and Dame Patsy Reddy. 2016. *Report of the First Independent Review of Intelligence and Security in New Zealand*. http://www.parliament.nz/en-nz/pb/presented/papers/51DBHOH_PAP68536_1/report-of-the-first-independent-review-of-intelligence.
EFF. 2013. *Press Release*. https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association.
Freedom House. 2015. *Annual Survey of Internet Freedom*. https://freedomhouse.org/sites/default/files/FOTN%202015%20Full%20Report.pdf.
Garton Ash, Timothy. 2009. *The File*. London: Atlantic Books.
Home Office. 2016. *Operational Case for Bulk Powers*. London: Home Office. https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents.
IOCCO. 2015. *The Report of the IOCCO Inquiry into the Use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to Identify Journalistic Sources*. http://www.iocco-uk.info/docs/IOCCO%20Communications%20Data%20Journalist%20Inquiry%20Report%204Feb15.pdf.
ISC. 2013. *Press Release*. http://isc.independent.gov.uk/news-archive/11december2013.
JPCCDB. 2012. *The Report of the Joint Parliamentary Committee on the Communications Data Bill*. http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7902.htm.
JPCIPB. 2016. *Written Evidence to the Joint Parliamentary Committee on the Investigatory Powers Bill*. http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written evidence-draft-investigatory-powers-committee.pdf.
Klamberg, M. 2010. "FRA and the European Convention on Human Rights – A Paradigm Shift in Swedish Electronic Surveillance Law." In *Nordic Yearbook of Law and Information Technology*, edited by D. W. Schartaum, 96–134. Bergen: Fagforlaget.
La Rue, Frank. 2013. "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression." (United Nations)
Lyon, David. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity Press.
Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. 1st ed. New York: Public Affairs.
Morozov, Evgeny. 2014. *To Save Everything, Click Here*. London: Penguin.
PCAST. 2014. *Report to the President, Big Data and Privacy: A Technological Perspective*. http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.
PEN America. 2013. *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN American Center.
Penney, Jonathon W. 2016. "Chilling Effects: Online Surveillance and Wikipedia Use." *Berkeley Technology Law Journal*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.
Podesta, John. 2014. *Big Data: Seizing Opportunities, Preserving Values*. http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
Reed, Chris. 2012. *Making Laws for Cyberspace*. Oxford: Oxford University Press.
Reporters Without Borders. 2013. *Special Edition on Internet Surveillance*. http://surveillance.rsf.org/en/category/state-enemies/.
Richards, Neil M. 2013. "The Dangers of Surveillance." *Harvard Law Review*: 126 (7): 1934–1965.
Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World*. New York: W.W. Norton and Company.
Stoycheff, Elizabeth. 2016. "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring." *Journalism and Mass Communication Quarterly* 93 (2): 296–311.
Taylor, Emily. 2016. *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*. GCIG Paper Series No. 23 referring to Morozov 2014.
UK Government. 2016. *Investigatory Powers Bill Codes of Practice*. https://www.gov.uk/government/publications/investigatory-powers-bill-codes-of-practice.
US Mission to the European Union. 2015. *Press Release*. http://useu.usmission.gov/st-09282015.html.
Vaizey, Hester. 2014. *Born in the GDR: Living in the Shadow of the Wall*. Oxford: Oxford University Press.