Privacy and Security Inquiry
Intelligence and Security Committee of Parliament
35 Great Smith Street
London, SW1P 3BQ

UEA Law School

University of East Anglia
Norwich Research Park
Norwich NR4 7TJ
United Kingdom

Tel: +44 (0) 1603 592520
Fax: +44 (0) 1603 250245

By email to: privacy@intelligenceandsecuritycommittee.org

6th February 2014

Submission to the Intelligence and Security Committee by Dr Paul Bernal

I am making this submission in response to the Privacy and Security Call for Evidence made by the Intelligence and Security Committee on 11th December 2013, in my capacity as Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School. I research in internet law and specialise in internet privacy from both a theoretical and a practical perspective. My PhD thesis, completed at the LSE, looked into the impact that deficiencies in data privacy can have on our individual autonomy. I have a book dealing with the subject, *Internet Privacy Rights*, which will be published by Cambridge University Press, in March 2014. The subject of internet privacy, therefore, lies precisely within my academic field. I would be happy to provide more detailed evidence, either written or oral, if that would be of assistance to the committee.

Executive summary

There are a great many issues that are brought up by the subject of communications surveillance. This submission does not intend to deal with all of them. It focuses primarily on three key issues:

1) The debate – and indeed the initial question asked by the ISC – which talks of a balance between ‘individual privacy’ and ‘collective security’ is a miscast one. Communications surveillance impacts upon much more than privacy. It has an impact on all the classical ‘civil liberties’: freedom of expression, freedom of assembly and association and so forth. Privacy is not a merely ‘individual’ issue. It, and the connected rights, are community rights, collective rights, and to undermine them does more than undermine individuals: it hits at the very nature of a free, democratic society.
2) The invasion of privacy, the impact on the other rights mentioned above, occurs at the point when data is gathered, not when data is accessed. The mass surveillance approach that appears to have been adopted – a ‘gather all, put controls on at the access stage’ is misconceived. The very gathering of the data has an impact on privacy, and leaves data open for misuse, vulnerable to hacking, loss or misappropriation, and has a direct chilling effect.
3) In terms of mass surveillance, meta-data can in practice be more useful – and have more of an impact on individual rights and freedoms – than content data. It can reveal an enormous amount of information about the individuals involved, and because of its nature it is more easily and automatically analysed and manipulated.

The implications of these three issues are significant: the current debate, as presented to the public and to politicians, is misleading and incomplete. That in turn means that experts remain sceptical about the motivations of those involved in the debate in favour of surveillance – and that it is very hard for there to be real trust between the intelligence services and the public.

It also means that the bar should be placed much higher in terms of evidence that this kind of surveillance is successful in achieving the aims of the intelligence services. Those aims need to be made clear, and the successfulness of the surveillance demonstrated, if the surveillance is to be appropriate in a democratic society. Given the impact in terms of a wide spectrum of human rights – not just individual rights to privacy – the onus is on the security services to demonstrate that success, or move away from mass surveillance as a tactic.

1 A new kind of surveillance

The kind of surveillance currently undertaken – and envisaged in legislation such as the Communications Data Bill in 2012 – is qualitatively different from that hitherto imagined. It is not like ‘old-fashioned’ wiretapping or even email interception. What also makes it new is the way that we use the internet – and in particular the way that the internet is, for most people in what might loosely be described as developed societies, used for almost every aspect of our lives. By observing our internet activities, therefore, the level of scrutiny in our private lives is vastly higher than any form of surveillance could have been in the past.

In particular, 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. In parallel with this, technological developments have changed the nature of the data that can be obtained by surveillance – most directly the increased use of mobile phones and in particular smartphones, provides new dimensions of data such as geo-location data, and allow further levels of aggregation and analysis. Other technologies such as facial recognition, in combination with the vast growth of use of digital, online photography – ‘selfie’ was the Oxford Dictionaries Word of the Year for 2013 – take this to a higher level.

This combination of factors means that the ‘new’ surveillance is both qualitatively and quantitatively different from what might be labelled ‘traditional’ surveillance or interception of communications. This means that the old debates, the old balances, need to be recast. Where traditional ‘communications’ was in some ways a subset of traditional privacy rights – as reflected in its part, for example, 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.

2 Individual right to privacy vs. collective right to security?

2.1 Privacy is not just an individual right

Privacy is often misconstrued as a purely individual right - indeed, it is sometimes characterised as an 'anti-community' right, a right to hide yourself away from society. Society, in this view, would be better if none of us had any privacy - a 'transparent society'. In practice, nothing could be further from the truth: privacy is something that has collective benefit, supporting coherent societies. Privacy isn't so much about 'hiding' things as being able to have some sort of control over your life. The more control people have, the more freely and positively they are likely to behave. Most of us realise this when we consider our own lives. We talk more freely with our friends and relations knowing (or assuming) that what we talk about won't be plastered all over noticeboards, told to all our colleagues, to the police and so forth. Privacy has a crucial social function - it's not about individuals vs. society. The opposite: societies cannot function without citizens having a reasonable expectation of privacy.

2.2 Surveillance doesn't just impact upon privacy

The idea that surveillance impacts only upon privacy is equally misconceived. Surveillance impacts upon many different aspects of our lives - and how we function in this 'democratic' society. In human rights terms, it impacts upon a wide range of those rights that we consider crucial: in particular, it impacts upon freedom of expression, freedom of association and freedom of assembly, and others.

2.2.1 Freedom of expression

The issue of freedom of expression is particularly pertinent. Privacy is often misconstrued as somehow an 'enemy' of freedom of expression – blogger Paul Staines (a.k.a. Guido Fawkes) for example, suggested that 'privacy is a euphemism for censorship'. He had a point in one particularly narrow context - the way that privacy law has been used by certain celebrities and politicians to attempt to prevent certain stories from being published - but it misses the much wider meaning and importance of privacy.

Without privacy, speech can be chilled. The Nightjack saga, of which the committee may be aware, is one case in point. The Nightjack blogger was a police insider, providing an excellent insight into the real lives of police officers. His blog won the 2009 Orwell Award – but as a result of email hacking by a journalist working for the Times, he was unable to keep his name private, and ultimately he was forced to close his blog. His freedom of expression was stifled – because his privacy was not protected. In Mexico, at least four bloggers writing about the drugs cartels have not just been prevented from blogging - they've been sought out, located, and brutally murdered. There are many others for whom privacy is crucial - from dissenters in oppressive regimes to whistle-blowers to victims of spousal abuse. The internet has given them hitherto unparalleled opportunities to have their voices heard - internet surveillance can take that away. Even the possibility of being located or identified can be enough to silence them.

Internet surveillance not only impacts upon the ability to speak, it impacts upon the ability to receive information - the crucial second part to freedom of speech, as set out in both the European Convention on Human Rights and the Universal Declaration of Human Rights. If people know that which websites they visit will be tracked and observed, they're much more likely to avoid seeking out information that the authorities or others might deem 'inappropriate' or 'untrustworthy'. That, potentially, is a huge chilling effect. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in his report of 2013 made the link between privacy and freedom of expression as direct and crucial.

“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."

2.2.2 Freedom of association and of assembly

Freedom of association and assembly is equally at risk from surveillance. The internet offers unparalleled opportunities for groups to gather and work together - not just working online, but organising and coordinating assembly and association offline. The role the net played in the Arab Spring has probably been exaggerated - but it did play a part, and it continues to be crucial for many activists, protestors and so forth. The authorities realise this, and also that through surveillance they can counter it. A headline from a few months ago in the UK, "Whitehall chiefs scan Twitter to head off badger protests" should have rung the alarm bells - is 'heading off' a protest an appropriate use of surveillance? It is certainly a practical one - and with the addition of things like geo-location data the opportunities for surveillance to block association and assembly both offline and online is one that needs serious consideration. The authorities in the Ukraine recently demonstrated this through the use of surveillance of mobile phone geolocation data in order to identify people who might be protesting – and then sending threatening text messages warning those in the location that they were now on a list: a clear attempt to chill their protests. Once more, this is very much not about individual privacy – it is about collective and community rights.

3 Controls are required at the gathering stage

The essential approach in the current form of internet surveillance, as currently practiced and as set out in the Communications Data Bill in 2012, is to gather all data, then to put 'controls' over access to that data. That approach is fundamentally flawed – and appears to be based upon false assumptions.

3.1 Data vulnerability

Most importantly, it is a fallacy to assume that data can ever be truly securely held. There are many ways in which data can be vulnerable, both from a theoretical perspective and in practice. Technological weaknesses – vulnerability to 'hackers' etc – may be the most 'newsworthy' in a time when hacker groups like 'anonymous' have been gathering publicity, but they are far from the most significant. Human error, human malice, collusion and corruption, and commercial pressures (both to reduce costs and to 'monetise' data) may be more significant – and the ways that all these vulnerabilities can combine makes the risk even more significant.

In practice, those groups, companies and individuals that might be most expected to be able to look after personal data have been subject to significant data losses. The HMRC loss of child benefit data discs, the MOD losses of armed forces personnel and pension data in laptops, and the numerous and seemingly regular data losses in the NHS highlight problems within those parts of the public sector which hold the most sensitive personal data. Swiss banks' losses of account data to hacks and data theft demonstrate that even those with the highest reputation and need for secrecy – as well as the greatest financial resources – are vulnerable. The high profile hacks of Apple, Facebook, Twitter, Sony and others show that even those that have access to the highest level of technological expertise can have their security breached. These are just a few examples, and whilst in each case different issues lay behind the breach the underlying issue is the same: where data exists, it is vulnerable.

3.2 Function Creep

Perhaps even more important than the vulnerabilities discussed above is the risk of 'function creep' – that when a system is built for one purpose, that purpose will shift and grow, beyond the original intention of the designers and commissioners of the system. It is a familiar pattern, particularly in relation to legislation and technology intended to deal with serious crime, terrorism and so forth. CCTV cameras that are built to prevent crime are then used to deal with dog fouling or to check whether children live in the catchment area for a particular school. Legislation designed to counter terrorism has been used to deal with people such as anti-arms trade protestors – and even to stop train-spotters photographing trains.

In relation to internet surveillance this is a very significant risk: the ways that it could be inappropriately used are vast and multi-faceted. What is built to deal with terrorism, child pornography and organised crime can creep towards less serious crimes, then anti-social behaviour, then the organisation of protests and so forth – there is evidence that this is already taken place. Further to that, there are many commercial lobbies that might push for access to this surveillance data – those attempting to combat breaches of copyright, for example, would like to monitor for suspected examples of 'piracy'. In each individual case, the use might seem reasonable – but the function of the original surveillance, the justification for its initial imposition, and the balance between benefits and risks, can be lost. An invasion of privacy deemed proportionate for the prevention of terrorism might well be wholly disproportionate for the prevention of copyright infringement, for example.

There can be creep in terms of the types of data gathered. The split between 'meta data' and 'content' is already one that is contentious, and as time and usage develops is likely to become more so, making the restrictions as to what is 'content' likely to shrink. There can be creep in terms of the uses to which the data can be put: from the prevention of terrorism downwards. There can be creep in terms of the authorities able to access and use the data: from those engaged in the prevention of the most serious crime to local authorities and others. All these different dimensions represent important risks: all have happened in the recent past to legislation (e.g. RIPA) and systems (e.g. the London Congestion charge CCTV system).

Prevention of function creep is inherently difficult. As with data vulnerability, the only way to guard against it is not to gather the data in the first place. That means that controls need to be placed at the data gathering stage, not at the data access stage.

4 The role of metadata

Rather than being less important, or less intrusive, than 'content', the gathering of meta data in the new kinds of surveillance of the internet may well be more intrusive and more significant. Meta data is the primary form of data used in profiling of people as performed by commercial operators for functions such as behavioural advertising. It is easier to analyse and aggregate, easier for patterns to be determined, and much richer in its implications than content. It is also harder to 'fake': content can be concealed by the use of code words and so forth – meta data by its nature is more likely to be 'true'.

In relation to trust, it is important that those who are engaged in surveillance acknowledge this: and those that scrutinise the intelligence services understand this. It was notable in the open session of the Intelligence and Security Committee at the end of 2013 that none of those questioning the heads of MI5, MI6 and GCHQ made the point, or questioned the use of statements to the effect that they were not reading our emails or listening to our phone calls. Those statements may be true, but they are beside the point: it is the gathering of metadata that matters more. It can reveal automatically – without the need of expert human intervention – great details. As Professor Ed Felten put it in his testimony to the Senate Judiciary Committee hearing on the Continued Oversight of the Foreign Intelligence Surveillance Act:

"Metadata can expose an extraordinary amount about our habits and activities. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath, or makes a large number of calls on Christmas Day; our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations."

Professor Felten was talking about telephony metadata – metadata from internet browsing, emails, social network activity and so forth can be even more revealing.

5 Conclusion

The subject of internet surveillance is of critical importance. Debate is crucial if public support for the programmes of the intelligence service is to be found – and that debate must be informed, appropriate and on the right terms It isn't a question of individual privacy, a kind of luxury in today's dangerous world, being balanced against the deadly serious issue of security. If expressed in those misleading terms it is easy to see which direction the balance will go. Privacy matters far more than that - and it matters not just to individuals but to society as a whole. It underpins many of our most fundamental and hard-won freedoms - the civil rights that have been something we, as members of liberal and democratic societies, have been most proud.

Similarly, the question of where the controls are built needs to be opened up for debate – at present the assumption seems to be made that gathering is acceptable even without controls. As noted above, that opens up a wide range of risks, risks that should be acknowledged and assessed in relation to the appropriateness of surveillance.

Finally, those involved in the debate should be more open and honest about the role of meta-data: the bland reassurances that 'we are not reading your emails or listening to your phone calls' should always be qualified with the acknowledgment that this does not really offer much protection to privacy at all.

Dr Paul Bernal
Lecturer in Information Technology, Intellectual Property and Media Law
UEA Law School
University of East Anglia
Norwich NR4 7TJ
Email: paul.bernal@uea.ac.uk