Mike Hennessy
Commons Clerk of the Joint Committee on Human Rights
Committee Office
House of Commons
7 Millbank
London
SW1P 3JA

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

10 August 2012

Submission to the Joint Committee on Human Rights

Re: Draft Communications Data Bill

The Draft Communications Data Bill raises significant human rights issues – most directly in relation to Article 8 of the Convention, but also potentially in relation to Articles 9, 10, 11 and 14. These issues are raised not by the detail of the bill but by its fundamental approach. Addressing them would, in my opinion, require such a significant re-drafting of the bill that the better approach would be to withdraw the bill in its entirety and rethink the way that security and surveillance on the Internet is addressed.

I am making this submission 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, and set out a possible rights-based approach to internet privacy. The Draft Communications Data Bill 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.

1 The fundamental approach of the bill

As set out in Part 1 of the draft bill, the approach adopted is that *all* communications data should be captured and made available to the police and other relevant public authorities. The regulatory regime set out in Part 2 concerns accessing the data, not gathering it: gathering is intended to be automatic and universal. Communications data is defined in Part 3 Clause 28 very broadly, via the categories of 'traffic data', 'use data' and 'subscriber data', each of which is defined in such a way as to attempt to ensure that all internet and other communications activity is covered, with the sole exception of the 'content' of a communication.

The all-encompassing nature of these definitions is necessary if the broad aims of the bill are to be supported: if the definitions do not cover any particular form of internet activity (whether existent or under development), then the assumption would be that those who the bill would intend to 'catch' would use that form. That the 'content' of communications is not captured (though it is important in relation to more conventional forms of communication such as telephone calls, letters and even emails) is of far less significance in relation to internet activity, as shall be set out below.

2 The nature of 'Communications Data'

As noted above, the definition of 'communications data' is deliberately broad in the bill. This submission will focus on one particular form of data – internet browsing data – to demonstrate some of the crucial issues that arise. Article 8 of the Convention states that:

"Everyone has the right to respect for his private and family life, his home and his correspondence'

On the surface, it might appear that 'communications data' relates to the 'correspondence' part of this clause – and indeed communications like telephone calls, emails, text messages, tweets and so forth do fit into this category – but internet browsing data has a much broader impact upon the 'private life' part of the clause. A person's browsing can reveal far more intimate, important and personal information about them than might be immediately obvious. It would tell 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 and so forth. This kind of data can reveal habits, preferences and tastes – and can uncover, to a reasonable probability religious persuasion, sexual preferences, political leanings etc.

What is more, 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, most directly by those involved in the behavioural advertising industry. Significant amounts of money and effort are being spent in this direction by those in the internet industry – it is a key part of the business models of Google, Facebook and others. It is already advanced – but we can expect the profiling and predictive capabilities to develop further

What this means is that by gathering, automatically and for all people, 'communications data', we would be gathering the most personal and intimate information about everyone. When considering this bill, that must be clearly understood. This is not about gathering a small amount of technical data that might help in combating terrorism or other crime – it is about universal surveillance and ultimately profiling. That 'content' data is not gathered is of far less significance – and that focussing on it is an old fashioned argument, based on a world of pen and paper that is to a great extent one of the past.

3 Articles 9, 10, 11 and 14

The kind of profiling discussed above is what brings Articles 9, 10, 11 and 14 into play: it is possible to determine (to a reasonable probability) individuals' religions and philosophies, their languages used and even their ethnic origins, and then use that information to monitor them both online and offline. When communications (and in particular the internet) are used to organise meetings, to communicate as groups, to assemble both offline and online, this can become significant. Meetings can be monitored or even prevented from occurring, groups can be targeted and so forth. It can enable discrimination – and even potentially automate it. Oppressive regimes throughout the world have recognised and indeed used this ability – recently, for example, the former regime in Tunisia hacked into both Facebook and Twitter to attempt to monitor the activities of potential rebels.

It is of course this kind of profiling that can make internet monitoring potentially useful in counterterrorism – but making it universal rather will impact directly on the rights of the innocent, rights that according to Articles 8, 9, 10, 11 and 14 should be respected.

4 The vulnerability of data

The approach taken by the bill is to gather all data, then to put 'controls' over access to that data. That approach is flawed for a number of reasons.

Firstly, 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 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 to human intervention. The high profile hacks of Sony's online gaming systems 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.

What is more, designing and building systems to implement legislation like the Communications Data Bill exacerbates the problem. The bill is not prescriptive as to the methods that would be used to gather and store the data, but whatever method is used would present a 'target' for potential hackers and others: where there are data stores, they can be hacked, where there are 'black boxes' to feed real-time data to the authorities, those black boxes can be compromised and the feeds intercepted. Concentrating data in this way increases vulnerability – and creating what are colloquially known as 'back doors' for trusted public authorities to use can also allow those who are not trusted – of whatever kind – to find a route of access.

Once others have access to data – or to data monitoring – the rights of those being monitored are even further compromised, particularly given the nature of the internet. Information, once released, can spread without control.

5 Function Creep

As important as 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 the Communications Data Bill this is a very significant risk – if a universal surveillance infrastructure is put into place, 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 might creep towards less serious crimes, then anti-social behaviour, then the organisation of protests and so forth. 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, and the justification for its initial imposition, can be lost.

Prevention of function creep through legislation is inherently difficult. Though it is important to be appropriately prescriptive and definitive in terms of the functions for which the legislation and any systems put in place to bring the legislation, function creep can and does occur through the development of different interpretations of legislation, amendments to legislation and so forth. The only real way to guard against function creep is not to build the systems in the first place: a key reason to reject this proposed legislation in its entirety rather than to look for ways to refine or restrict it.

6 Conclusions

The premise of the Communications Data Bill is fundamentally flawed. By the very design, innocent people's data will be gathered (and hence become vulnerable) and their activities will be monitored. Universal data gathering or monitoring is almost certain to be disproportionate at best, highly counterproductive at worst.

Even without considering the issues discussed above, there is a potentially even bigger flaw with the bill: on the surface, it appears very unlikely to be effective. The people that it might wish to catch are the least likely to be caught – those who are expert with the technology will be able to find ways around the surveillance, or ways to 'piggy back' on other people's connections and draw more innocent people into the net. As David Davis put it, only the incompetent and the innocent will get caught.

The entire project needs a thorough rethink. Warrants (or similar processes) should be put in place before the gathering of the data or the monitoring of the activity, not before the accessing of data that has already been gathered, or the 'viewing' of a feed that is already in place. A more intelligent, targeted rather than universal approach should be developed. No evidence has been made public to support the suggestion that a universal approach like this would be effective – it should not be sufficient to just suggest that it is 'needed' without that evidence.

That brings a bigger question into the spotlight, one that the Joint Committee on Human Rights might think is the most important of all. What kind of a society do we want to build – one where everyone's most intimate activities are monitored at all times just in case they might be doing something wrong? That, ultimately, is what the Draft Communications Bill would build. The proposals run counter to some of the basic principles of a liberal, democratic society – a society where there should be a presumption of innocence rather than of suspicion, and where privacy is the norm rather than the exception.

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