25BedfordRow

This is the speech given by Professor Peter Sommer at the 25 Bedford Row symposium on the Investigative Powers Bill on 22 March 2016. Professor Sommer was a Specialist Advisor to the Joint Committee of MPs and peers that scrutinised the draft Bill. *www.pmsommer.com* *@Professor_Peter*

The purpose of pre-legislative scrutiny is, in a spirit of friendly scepticism, to ask "What could possibly go wrong?" Where are the unintended consequences, are the policy ambitions properly researched and practical, are the financial implications properly calculated, is the detailed wording clear and unambiguous?

There is very little urgency to pass this legislation. Nearly all of the powers exist already but scattered across many places and in some instances until recently not avowed. What is needed is bringing everything together into one place, to update where necessary and to provide clarity.

It may be difficult to argue in the wake of today's events in Brussels but to those who cite the number of Syrian returnees and the numbers of disrupted terrorist plots there are some alternative statistics. Deaths on UK soil from terrorism are tiny – none last year, none in 2014 one in 2013 and 52 in 2005. Against this in the last year for which we have figures there were 574 murders, 1775 road traffic deaths, 6000 fatal accidents in the home, a minimum of 30,000 dying from atmospheric pollution and 43,900 excess winter mortality deaths using definitions from the Office of National Statistics. There were 60 lightening strikes affecting humans. That tells us that using existing powers the security and intelligence agencies and law enforcement agencies are extremely effective. A future terrorist success is inevitable but it will probably be small in impact – because the greater the ambition of a plan the greater the chance of premature detection.

This is not an argument for changes in counter-terrorism policy but a warning of the dangers of rushed legislation.

The only time pressure is from the sunset clause in DRIPA but that act, made necessary by the failure of the EU Data Retention Directive only affects part four of the Bill. DRIPA went through Parliament in three days and an extension of the sunset clause could scarcely take longer.

The main aim of the legislation therefore is clarity and removal of ambiguity. There is little dispute about overall aims, though there are arguments about the extent to which mass retention as opposed to targeted collection is necessary, concerns about some bulk powers, special protections for lawyers, journalists and MPs - and the detail of authorisation and oversight mechanisms.

But the general principles of seeking balances between security and privacy, and the need to maintain the fundamental qualities of the Internet have to be turned into large numbers of individual decisions about how those balances are struck. That is why the draft Bill had 202 clauses in it and the version currently before Parliament has 233. Plus 10 schedules and a number of lengthy Codes of Practice.

That this level of detail is necessary is what we have learnt from PACE 1984 and from RIPA 2000. General principles have to be converted into precise instructions and language – and for a law that is heavily about the Internet and the digital domain, language has to reflect how the Internet works.

Decisions about balance should be for Parliament, not the Home Office, police or the agencies. But they are not giving themselves enough time. The Joint Committee reviewing the earlier, much shorter and now abandoned Data Communications Bill in 2012 took 5 months of intensive enquiries. A normal period of pre-legislative scrutiny of a Bill is 12 weeks; the Joint Committee for which I worked had 8 weeks. MPs and peers pick up all sorts of specialist knowledge as part of their routine work, especially as constituency MPs – about health, social security, education, housing. But this does not include the nitty-gritty of Internet operations and the practicalities of digital investigations. Parliamentarians need familiarity time.

It was the lack of this that resulted in so many of the Joint Committee's recommendations and conclusions taking the form: "We understand and agree with the need for this measure but more explanation and work is required". But since the committee ceased to exist when its report was published on 11 February, the question is how those issues are to be followed up.

Not by the current scrutiny committee which is mostly tasked with agreeing specific amendments and will have only 14 sessions before its final session on 5 May. The list of witnesses for the first session is worrying in that only one – from EE – can speak to the practicalities and costs of implementation. There are two to represent victims, but neither on previous showing knows anything about investigative techniques, the existing law or how CSPs work.

At the heart of practicality of implementation is the one new feature of the Bill – Internet Connection Records. The definitions keep on changing. One of the aims is to try and label some activities as "communications data" and hence be authorised by a senior designated officer as opposed to "content" which requires the signature of the Secretary of State (validated by a judge) but is also not admissible as evidence. Graham Smith of Bird & Bird, blogging as Cyberleagle (http://cyberleagle.blogspot.co.uk/) has attempted to disentangle the endless confusions of relevant communications data, secondary communications data, references to telecommunications services, telecommunications systems, telecommunications operators and complex definitions of content.

> "Content", in relation to a communication and a telecommunications operator, telecommunications service or telecommunication system, means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—
>
> (a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and
>
> (b) anything which is systems data is not content."

The police and agencies have some entirely legitimate concerns. Current definitions of Communications Data include not only records of visits to websites "up to the first backslash" but also the "from", "to" and "time" information of conventional email. Conventional email is subject to various RFC standards which specify the detail of email headers. It is trivial to write a filter which simply picks up the three "comms data" elements and then discards everything else.

The police say that they also ought to be able to have access to such information when it is transmitted by webmail. The technical problem of course is that the landing page of webmail is beyond the first backslash and the page is simply HTML; there are no convenient "flags" which can be used to separate out the comms elements; In effect the only way to filter would be via web scraping software – which would have to be written for each individual webmail service and rewritten every time a service decides to redesign its webpages. Similar problems attend the messaging services within social media apps. In any event many of the services now use encrypted HTTPS – web scraping software doesn't work on encrypted material! But the ambitions for ICRs seem to extend beyond this.

Incidentally is "data retention" the right expression for this? Data retention in ATSCA 2001 meant asking, later requiring, CSPs to hold on to data they were routinely creating in the course of their business for longer than they needed and which should have been destroyed to comply with the Data Protection Act. What is now expected is data generation and collection – creating records of activity for which the CSP has no need but law enforcement does.

All this has profound cost and value-for-money implications. Will we end up with spending large sums of money collecting data from the innocent while the bad guys use simple but effective evasive techniques? Reports around the arrest of Salah Abdeslam show the use of throw-away mobile phones and sophisticated techniques of evading electronic surveillance and the ISC reported that the two assassins of Lee Rigby seemed to be very surveillance-aware.

For a long time Home Office officials and CSPs appear to have been talking in terms of principles and generalisations; actual wordings of proposed legislation were not produced and as a result the practical difficulties of implementation not realised.

Too often the Bill's clauses reflect investigative ambitions without understanding how difficult it is to translate this into filters that can be applied, as will be necessary, at ultra high speed to the data passing through a CSP. There also seems to be little appreciation of the amount of data that will be created. Even in the simplest of Internet activities there are many background "internet connections" – DNS requests, checks with certification authorities, agreements between devices about session keys, network status checks. Moreover most people now have multiple sessions going on their computers and smartphones – tabbed browsers open to several websites, links to instant messaging and social media, news feeds, software updates. All these will need to be captured by CSPs, a storage cost, made available online to meet requests, a further cost, and then the various activities will need to be disentangled, a yet further cost. The term Internet Connection Record has no generally-recognised meaning to Internet engineers.

These problems remain and illustrate broader problems elsewhere in the Bill. They are unlikely to be resolved by the current Parliamentary process and the prospects for the Bill are confusion and disappointment. The aim of clarity is not going to be achieved – and all because of an unnecessarily fast passage through Parliament. No doubt Parliamentarians hope that somehow the techies and lawyers can get together and solve these issues – but really it is their responsibility.

I am happy to take these points further in Q&A but also any other matters which come up.

Peter Sommer

www.pmsommer.com