The Law Society

EVIDENCE FOR INVESTIGATORY POWERS REVIEW

Introduction

The Law Society of England and Wales is the professional body representing more than 145,000 solicitors in England and Wales. It works globally to support and represent its members, promoting the highest professional standards and the rule of law.

1. Overview

We are grateful for the opportunity to provide evidence to the first stage of the current review of communications data and interception powers in the UK. Such a review is long overdue and it is regrettable that the price of holding it was the passage of the Data Retention and Investigatory Powers Act 2014 (DRIPA), which also mandated it.

We hope that the review marks the start of a journey that will end with Parliament simplifying and clarifying a complex and confusing legal framework. Surveillance law should strike a better balance between security and privacy – one that is better understood and one that commands greater public assent.

We have grouped our comments around the scope of the review as set out in DRIPA s.7(2) and in the published terms of reference.

We would however like to make some general opening observations.

- The ability to mine communications data is now so great that much information about individuals' activities and lives can be gleaned simply from their traffic; and consequently the distinction between data and content is no longer so important in the determination of legislative interference and safeguards;

- The legislation is in a mess and contradictory - the fact that it is neither accessible nor intelligible is an affront to the rule of law and the requirement in ECHR Art 8(2) that interference be "in accordance with the law" - as to which see Halford and Malone. The law has not kept pace with technological developments and needs overhaul.

- We need to develop a coherent set of principles to determine what should be the limits of permitted surveillance and how such surveillance should be policed.

2. Current and future threats and the capabilities to combat them

The public have been given differing accounts of the surveillance capabilities of the UK government. On the one hand, the Snowden revelations suggest that GCHQ and

its allies have exceptional technical intercept capability; on the other, the Home Office argues that there is a 'capability gap'.

According to reports based on documents provided by Snowden, GCHQ and the NSA have exceptional technical capabilities.

In June 2013, the Guardian reported that GCHQ personnel had attached intercept probes to the transatlantic fibre-optic cables running into Europe through Britain. These cables carry data including data generated by phone calls, email messages, social media and web browsing. According to the article 'For the 2 billion users of the world wide web, Tempora represents a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world'.

There have also been allegations that GCHQ acted illegally by accessing communications content via the NSA's PRISM programme (a programme through which the US Government obtains intelligence material from Internet Service Providers (ISPs)). Parliament's Intelligence and Security Committee (ISC) concluded that GCHQ had not circumvented or attempted to circumvent UK law, but this is further evidence of capability.

The ISC has accepted Home Office assertions of a so-called a 'capability gap'. This is the gap between what communications data the agencies need access to and what communications service providers (CSPs) currently retain for "internal business reasons" (*Access to communications data by the intelligence and security Agencies*, February 2013). Data are lost between service infrastructure providers like BT and application service providers like Facebook; single communications are fragmented between numerous service providers and overseas CSPs "cannot be obliged to provide [relevant data] to … UK authorities'.

The ISC concluded that the shortfall between the data required by the Agencies and that which the CSPs – both domestic and overseas – hold for their internal business reasons is significant and, without any action, will continue to grow.

It is unclear whether the Agencies have the exceptional capabilities suggested by numerous reports based on the Snowden revelations or have a significant gap in these capabilities as stated by the Home Office and others. A great fear is that they simply have a significant legal gap in their exceptional technical capabilities (and practice). Unfortunately the public just does not know.

It is essential that the review establishes the true facts about capability and that a way is found to provide credible information to inform public debate.

3. Safeguards to protect privacy

> It is well-known that in English law there is no right to privacy, and accordingly there is no right of action for a breach of a person's privacy. The facts of the present case are a graphic illustration of the desirability of Parliament considering whether and in what circumstances statutory provision can be made to protect the privacy of individuals.
>
> Glidewell LJ *Kaye v.Robertson* [1991] FSR 62

Since *Kaye v Robertson* the Human Rights Act 1998 has changed English law. However, the ECJ's attempt to safeguard the right to privacy[1] by striking down Directive 2006/24 was defeated in the UK with the passage of DRIPA.

It is noteworthy that Lord Neuberger, the president of the Supreme Court, ended a recent speech with the following observations that are relevant to this review:

"First, I would suggest that, at least in many cases, the right to privacy is not, in fact, really a separate right, but, in truth, it is an aspect of freedom of expression. If I want to do or say something which I am only prepared to do or say privately, then it is an interference with my freedom of expression, if I cannot do it or say it because it will be reported by a newspaper…

The other point arises from the consequences of the astonishing developments in IT: the ease with which information can be transmitted and received across the world, the ease with which words and scenes can be clandestinely recorded, and the ease with which information can be misrepresented or doctored. These developments may make it inevitable that the law on privacy, indeed, the law relating to communications generally, may have to be reconsidered. It undermines the rule of law if laws are unenforceable." [2]

The question of 'safeguards to protect privacy' cannot easily be detached from the question of what we mean by 'privacy' and how this should be addressed in English law.

Clearer basic legal principles – a reconsidered law on privacy and communications – would provide a better context within which Parliament could legislate, and public authorities could operate, in matters of surveillance.

4. Changing & global nature of technology

Internet access continues to widen in the UK with users increasingly engaging in social networking on global platforms like Facebook, selling goods and services, internet banking, making health appointments or using travel related services. According to the latest figures from the Office of National Statistics (August 2014) in 2014 38 million adults in Great Britain accessed the Internet everyday, 21 million more than in 2006; access via a mobile phone grew between 2010 to 2014 from 24% to 58%; and 22 million households (84%) had Internet access. In 2014 over half of all adults (54%) used social networking and this figure rises to 91% for the 16-24 age group.

According to OFCOM, the proportion of adults who personally own/use a mobile phone in the UK was 93% in Q1 2014.

These figures are significant in a number of ways. They indicate the scope of the privacy impact arising from internet-based surveillance. They demonstrate the pace and scale of technology-related change that can, and has, taken place - most dramatically by the global growth of Facebook from 1m users at the end of 2004 to

[1] See Article 7 of the Charter of Fundamental Rights of the European Union ("the Charter") and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

[2] *The Third and Fourth Estates: Judges, Journalists and Open Justice* at the Hong Kong Foreign Correspondents' Club.

1.11bn users by March 2013. Finally, they confirm the huge importance of overseas service providers like Facebook in thinking about UK citizens' communications data.

Other developments including cloud computing, the Internet of Things (IoT), the growth of big data sets and big data analytics are increasing the amount of data available and the potential to analyse it. This trend is beginning to eliminate any meaningful distinction between communications data and content. This has already been acknowledged by the Home Office in the context of web browsing. In Oral Evidence to the ISC (16 October 2012) they conceded that "*the distinction between data and content, you can argue, is muddied in the Internet world*".

Developments in technology are increasingly generating such vast quantities of analysable data that either a 'capability gap' must eventually be allowed to exist or government will commit itself to ever increasing expenditure in pursuit of near total surveillance of the population. The best way to address this may be to establish clearer basic legal principles and to reflect these within a more considered legislative framework.

5. The legislative framework

Over ten years ago, in January 2003 an All Party Parliamentary Group (APIG) published a report of its inquiry into communications data. Amongst other matters it expressed concern about a lack of clarity in the definition of "communications data", a conflict between various statutes, and delay by the Home Office in publishing a code of practice.

APIG's analysis of the conflict between the Anti-Terrorism, Crime and Security Act 2001 (ATCSA), the Regulation of Investigatory Powers Act 2000 (RIPA), the Data Protection Act 1998 (DPA) and the Human Rights Act 1998 (HRA) recommended that the Home Office should drop its plans to introduce a voluntary scheme for data retention under ATCSA. The Home Office did not follow APIG's advice.

The clarity of the legislative framework has not improved since 2003 and this may, in part, be due to the reactive nature of the legislative programme. RIPA was necessary in order to provide the UK with a lawful basis for interception of and access to communications (including communications data) in the light of *Halford v. United Kingdom* [1997] ECHR 32 and the HRA. ATCSA was a response to 9/ll. The Data Retention Directive (2006/24/EC) – heavily promoted by the UK government – was a response to the Madrid (2004) and London (2005) bombings. And various aborted or abandoned legislative proposals like the draft Data Communications Bill (2012) have been associated with various aborted or abandoned government surveillance projects including ID cards, the Citizen Information Project and the Interception Modernisation Programme.

DRIPA itself was, of course, another 'emergency' response – this time to the European Court of Justice (ECJ) judgment of 8 April 2014 in joined cases C-293/12 Digital Rights Ireland and C-594/12 Seitlinger (Digital Rights case) which declared the Data Retention Directive (2006/24/EC) invalid. Given that the ECJ struck down the Directive for being disproportionate under the EU Charter of Fundamental Rights and that the Charter rights are similar to those under article 8 of the European Convention, changing the legislative basis (from the Directive to DRIPA) does not alter these facts. It is a form of forum-shopping that is contrary to the rule of law.

It is possible to detect subtle links between atrocity, reaction, the global and changing nature of technology, capability and the inadequacies of the legislative framework (and process) by noting just one aspect of DRIPA. The government has argued that whilst RIPA was intended to apply to overseas CSPs offering services to UK customers irrespective of where those companies were based, DRIPA was necessary "to make that clear on the face of the legislation" (para 15, DRIPA explanatory notes).

One aspect of surveillance legislation that has been of long-standing concern to the Law Society is the absence of explicit protection in RIPA for legal professional privilege (LPP).

In relation to targeted surveillance, guidance which provides for additional oversight where privileged material might be the subject of interception has been published in the Interception of Communications Code of Practice (issued under s71 of RIPA). The code is directed at those public authorities who may seek warrants under RIPA and the provisions of the code may be taken into account by any court or tribunal and by the Interception of Communications Commissioner.

In relation to mass surveillance (communications data) it would appear that the question of legal privilege does not arise since privilege would apply to the content of a communication. However, the absence of any exception under the Data Retention Directive for persons whose communications were subject to 'professional secrecy' was a matter on which the ECJ commented in the Digital Rights case noting that the Directive "does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy." Given the ability to mine communications data to form a picture, laws requiring data retention and permitting its interrogation by public authorities should have an explicit exception for the fact of communications with legal advisers. That is to say, in an age of mass surveillance traditional common law principles of LPP need to be supplemented by broader protections.

The legislative framework for surveillance is complex and, in part, confused. It has often been the product of inadequate public consultation and debate or Parliamentary scrutiny. Its piecemeal development has often been in response to external threats, judicial decisions or technological uncertainty. It needs systematic review and revision.

6. Conclusion

The adequacy of government's surveillance capabilities are unclear. Greater clarity to inform public debate is essential particularly in relation to achieving some degree of assent to large-scale mass surveillance. Technological developments that are already in train mean that some self-imposed, legally enforceable limits on government surveillance will be essential if the UK is not to become a total-surveillance society (it has already been described by many, including a former Information Commissioner as a 'surveillance society').

Basic principles of English law could be developed, as the president of the Supreme Court mooted they might need to be, which would begin to address the new digital world into which we are moving. These principles should inform a less hasty, better informed legislative programme to deliver a more balanced legislative framework. Arguably this programme should be taken out of the hands of the Home Office and given to a public body with some degree of independence from the government of the day.

All this points to one other matter addressed by the current reviews terms of reference: openness and oversight. In 2013 public authorities made over half a million requests for communications data - a figure the Interception of Communications Commissioner said ‘has the feel of being too many’. Alongside the sheer scale of global data flows, the vast expenditure on government surveillance capabilities, the ever expanding reach of technology and overarching surveillance laws which the ECJ has found to be in breach of basic human rights, can it be right that the Interception of Communications Commissioner's Office (IOCCO) is currently staffed by two senior appointees, nine inspectors and two secretarial staff?

Oversight of UK surveillance, including the development of proposals for a balanced framework for surveillance, needs to be conducted by a well-staffed, well-resourced and independent public body with the technical and legal expertise that it needs.