Lost in the maze of surveillance laws

The ISC report on security agencies' interception techniques is a step in the right direction, but its findings are underwhelming, discuss **David McCluskey** and **Kate Parker**

David McCluskey, pictured, is a partner and Kate Parker is a paralegal at Peters and Peters
@PetersandPeters
www.petersandpeters.com

On 12 March 2015, the Intelligence and Security Committee (ISC) of parliament published its latest report: 'Privacy and security: A modern and transparent legal framework'. The report culminated an 18-month long inquiry into the surveillance and interception techniques of our intelligence and security agencies, in the wake of the Snowden revelations on GCHQ's long-standing data-sharing operation with the US National Security Agency.

The most interesting – and for some the most controversial – conclusion was that GCHQ's bulk data collection, as unearthed by Snowden, was not in breach of existing legislation. GCHQ only surveys a fraction of the data it retains, and 'is not collecting or reading everyone's emails: they do not have the legal authority, the resources, or the technical capability to do so.' Any interception must meet the three-part test enshrined in the Human Rights Act in being lawful, necessary, and proportionate to the threat at hand.

The committee drew a distinction between 'communications data' and 'communications content', the latter of which requires an official warrant by the secretary of state before interception. 'Communications data' (the who, when, and where of digital communications) can be accessed without a warrant by way of GCHQ self-authorisation.

Understandably, this process has raised public concern. Under section 22 of the Regulation of Investigatory Powers Act 2000 (RIPA), self-authorisation rests upon such vague and broad criteria as 'the interests of economic well-being' or 'for the purpose of preventing crime'. Some 58,996 authorisations were made by the agencies in 2013 alone: conveniently, there is no record of attempted authorisations which were refused.

'Communications data plus'

Perhaps this would be less disturbing if communications data were limited to the time, place, and participants in a landline call. But with the increasing sophistication of smart phone technology, the distinction between communications data and communications content (and certainly the perceived gap in intelligence value between them) is eliding. Data alone has the potential to provide 'private information about a person's habits, preferences or lifestyle choices, such as [which] website [they] visited'. The report attempts to address the widening scope of communications data by creating a new category of material which sits between data and content: the Newspeak-sounding 'communications data plus'. But the report fails to offer any further guidance on how this material would be given enhanced protection; all we are told is that it 'should attract greater safeguards'.

In failing to overhaul or sanction the existing self-authorisation process, the committee paves the way for the introduction of the Conservatives' controversial Communications Data Bill, which requires UK service providers to automatically store individuals' web and phone usage data for up to 12 months. The proposed Bill skates over the issue of the expanding remit of 'communications data', which it loosely defines as 'traffic data, use data or subscriber data'. In short, everything that the report recommends as 'communications data plus' would automatically be stored by service providers for a year under the Conservatives' law.

Of course, the government's 'greater surveillance' stance already influences the agencies' operations: non-lawyer Theresa May is, as home secretary, in charge of authorising warrants for interception of communications content. The fact that she is a politician raises obvious questions as to whether she is a sufficiently objective safeguard of citizens' privacy, and if ministerial oversight should be substituted for judicial oversight, as is the case in the US.

The relationship between the agencies and the public is a concern of the committee, and the report concludes that a greater dialogue must be established, as 'there is a legitimate public expectation of openness and transparency in today's society, and the security and intelligence agencies are not exempt from that'. However, the publicly available version of the report casts doubt on whether this is a sincerely held recommendation of the committee: many pages are redacted to the point of incomprehensibility, with asterisks substituting key evidence given by representatives of the intelligence and security community.

The report pays lip service to the questions of transparency and oversight raised by the Snowden disclosures, while implicitly supporting the agencies' position. In the words of the director general of MI5 in his evidence to the committee: 'The work we do [must be] secret from our adversaries. […] How far can we go to explain […] to the public how we work, without helping the people that we are trying to gain a covert advantage over?' What the report fails to acknowledge is the importance of public education, which stops short of such self-defeating transparency. For example, a plain-language explanation of communications data and communications content (and the differing authorisation standards that apply to each) is essential to help debunk some of the grander myths that 'all our emails are being read'.

Legal safeguards

One reason for a lack of faith in the agencies' operations might be the absence of legal safeguards for UK nationals caught under 'external' interception warrants. That is, of course, assuming this is known in the first place. Legislation in this area is so difficult to unpack that the foreign secretary himself confused the distinction between 'internal' and 'external' communications in his recent testimony to the ISC. Worryingly, he is responsible for the executive authorisation of all GCHQ and MI6 warrants under RIPA.

There are two categories of warrant available under RIPA: section 8.1 and section 8.4 warrants. Section 8.1 warrants are used domestically to access communications content, and must specify the person or premises they are targeting. By contrast, section 8.4 warrants do not need to specify either a person or premises; instead, they are directed at 'external' communications (a communication which is either sent or received outside the UK) and only authorise interceptions which are 'necessary […] in order to do what is expressly authorised or required by the warrant'. This last 'safeguard' is entirely cyclical: interception must be authorised, and authorisation is given on the grounds that it allows the interceptor to fulfil the terms of the warrant. In reality, any 'external' communications meet the threshold for interception under section 8.4.

The report confirmed that the government treats 'external' communications as including communications sent or received over an international server. Thus I may send a Facebook message from a UK location to a friend in another UK location, but since Facebook is hosted on an overseas server, my communication is deemed 'external' and can be read by GCHQ. In their defence, the agencies rely on section 16 of RIPA, which prevents them searching communications for persons known to be in the UK (whatever 'known' might mean). However, this is a safeguard simply not worthy of the name. GCHQ could not search for my name but it could trawl the content for known frames of reference or my personal details. If the recipient was a non-UK citizen, GCHQ could search their name and thereby reveal my content indirectly. Or, GCHQ could bypass this altogether by asking overseas agencies to hand over information on UK citizens – there is currently no legal protection in place to prevent this.

Cultural complacency

The ISC report reveals a cultural complacency towards safeguarding our content: the government has admitted that 'internal' communications can be accidentally intercepted as 'external' communications, given the difficulty in untangling communication network connections. The definition of a section 8.4 warrant needs to be narrowed and subject to oversight, and UK users of international servers should be alerted to the possibility that the privacy of their communications content is not legally safeguarded. All the ISC report recommends is that the distinction between 'internal' and 'external' communications should be clarified further.

The 'key recommendation' of the report is the introduction of a new law which combines all existing legislation under which the agencies operate. At present, the legal framework governing surveillance and interception activity includes RIPA (and its accompanying codes of practice), the Data Retention and Investigatory Powers Act 2014, the Serious Crime Act 2014, the Security Service Act 1989, and the Intelligence Services Act 1994. The report concludes that the existing legislative web is 'unnecessarily complicated' and 'lack[s] transparency'. While this proposal is to be welcomed, it is a dispiriting and underwhelming conclusion to an 18-month long inquiry, and risks contributing to public disillusionment in the agencies if the ultimate outcome of the report is simply more law. In any event, the looming election is likely to mean many other policies will compete with it for government time.

While the report takes a step in the right direction by recognising the evolving categories of communications material and criticising complex and anachronistic legislation, it does not go far enough. Until the committee calls for a separation of powers between those who intercept our communications data and content and those who authorise the interception, identifies exactly how the agencies should safeguard our 'communications data plus' and 'external' communications, and commits the agencies to educating the public without compromising national security, it is easy to reach the same conclusion on the ISC as Liberty director Shami Chakrabarti: '[it is] simpl[y] [a] mouthpiece for the spooks'. **SJ**

> “
> **The government has admitted that 'internal' communications can be accidentally intercepted as 'external', given the difficulty in untangling communication network connections**