Summary of ISPA Speech – Sir Anthony May

Wednesday 28th May 2014

This is a summary of a talk given by the Interception of Communications Commissioner to the Internet Service Providers Association (ISPA) on 28th May 2014. ISPA is the UKs trade association for Internet services whose members include Internet Service Providers (ISPs) and the majority of UK based telecommunications companies and mobile networks.

I welcome the opportunity to speak at this ISPA meeting after the recent publication of my first annual report on 8th April 2014. The members of ISPA are a vital part of the strategic relationships enabling the lawful interception of communications and the acquisition of communications data. This is because collaboration between law enforcement agencies and the industry is vital for both effective operations and also oversight by my office. With this in mind, I was able during my first year in office to visit a number of CSPs, most of whom are represented here today. I was most grateful for the information and instruction that these visits provided.

My Annual Report is available through the IOCCO website (www.iocco-uk.info). My report provides a detailed account of the statutory oversight which I and those in my office undertake. The report is different in shape and content from the reports of previous years. In particular it aims to be more open and therefore less secretive. There is no Confidential Annex with material withheld from full publication.

The report describes the legislation under the relevant parts of the Regulation of Investigatory Powers Act (RIPA 2000) and the detailed and thorough oversight and investigations which we have undertaken. It demonstrates that I and all those in our office are entirely independent of the Government and of all the public authorities whom we oversee. I personally composed a large part of the entire report and the rest was drafted by our Chief Inspector, Joanna Cavan, on my behalf. No one suggested or told us what we should write. Our oversight and the report are the product of full and unrestricted access, required to be provided to me by statute, of all information, however sensitive, that I require. This means that, even if I cannot publish all the detail, you and the public can be assured that

I have concluded that the operations which I oversee are conducted lawfully, except to any limited extent that I note otherwise in the body of the report. That applies importantly for your purposes to the downstream use by the public authorities of the intercepted material and communications data which you provide.

The report describes the findings from the 101 communications data and lawful interception inspections that my office conducted in 2013. During those inspections over 350 recommendations were made to ensure compliance or to improve systems and procedures.

The report addresses publically expressed legitimate concerns about intrusion into people's privacy. Some such intrusion is unavoidable if conduct of the kind which RIPA 2000 legitimises is to be undertaken at all. There has to be a proper balance justifying the intrusion for one or more of the statutory reasons of necessity. This balance goes under the flag heading of proportionality. It is here crucial to appreciate that the whole structure of RIPA 2000 Part I derives from and implements the provisions of Article 8 of the European Convention on Human Rights (ECHR). RIPA 2000 Part I is human rights compliant, provided of course that its provisions and those in the Codes of Practice are properly adhered to. It is my job and that of our Inspectors to see that they are, and to have corrected any particular respect in which they may not be.

The second half of 2013 featured media disclosures said to derive from the activities of Edward Snowden. These have carried forward into 2014. In addition to our normal oversight, I personally did a great deal of investigative work arising from these media reports in so far as they related to RIPA 2000 Part I activities. The product of this may be found in Section 6 of my Report under the heading "Questions of Concern". I formulated these questions with specific reference to a significant volume of media comment. Two main questions concerned:

(a) the contemporary structural integrity of RIPA 2000 Part I in the developing internet age, and;

(b) whether the public authorities had misused RIPA 2000 Part I to engage in random mass intrusion into the privacy of innocent individuals.

As to (a), I concluded that developing technology has not outgrown the legislation. Difficult legislation though it may be, its application to the internet was as well understood in Parliament in the year 2000 as it is today. The legislation is technology neutral.

As to (b), the public authorities do not engage in random mass intrusion into the privacy of innocent individuals, and it would be comprehensively unlawful if they did. I am able to say this from very thorough investigation into the sensitive detail of how the relevant systems operate.

My report also gives details of the full investigation which we required and carried out into the Retention, Storage and Deletion of intercepted material throughout all the 9 interception agencies who can be warranted to undertake the interception of communications.

The acquisition of communications data has also become of greater public interest and concern. It is in volume and, I think, importance the greater part of our business. We now have in addition to the Chief Inspector, 8 full time and independent Inspectors. We now inspect the larger police forces and law enforcement agencies annually. The annual report goes into this in great detail, but it is perhaps worth highlighting two aspects.

First, in addition to undertaking a full individual audit of around 10%, randomly selected, of the total volume of communications data applications, the Inspectors conduct query based thematic searches of the systems to look at specific areas in more detail and test them for compliance. An example would be to search to look at the form of all the approvals given by individual Designated Persons (DPs). This would result in 100% of the DPs considerations being examined over the search period and could show, for example, that a particular DP produces formulaic justifications, suggesting that inadequate consideration is given to the questions of necessity and proportionality.

Second, our office now regularly asks for and gratefully receives data from the other end of the process, that is to say from you - the CSPs, or the larger volume ones at least. This enables us to check that what you have provided properly correlates with what the police forces say they have asked for. It is a very valuable part of the audit process for which, as I say, we are grateful. One of our Inspectors is working on this and our oversight would be significantly enhanced if we could receive data more frequently from a larger number of CSPs.

Just as I have reported a number of interception questions of concern, there are some communications data questions of concern. Let me mention four.

(a) **Errors.** This may conveniently be brought under communications data, although errors can occur with interception as well. The communications data Code of Practice specifically deals with error reporting (which the Interception Code of Practice does not); and a communications data error is intrinsically (if quixotically) more likely to result in serious consequences for individuals. This is because communications data can generate enforcement action directly in a way that interception material usually does not because of the restrictions and safeguards on its use. For example, resolving an IP address incorrectly could result in police conducting a search warrant at the wrong address and accusing innocent individuals of crimes they did not commit.

Errors can have many causes and they can happen with CSPs as well as with public authorities. Errors can occur, for instance, if there is mistaken transposition of digits in a non-automated system or, at the other end of the scale, if there are systemic programming bugs. Thankfully, the number of errors is quite small in relation to the volume, but every error is regrettable and a tiny minority can have disastrous consequences. One of our Inspectors is in charge of investigating errors and you will, I am sure, continue to be cooperative to ensure that errors are duly reported, that human error is avoided so far as possible, and that systems are fully tested and monitored to avoid the glitches that occasionally occur.

(b) **Statistics.** The Communications Data Code of Practice requirements for the provision of statistics are inadequate for our and the public's purposes. This is dealt with in my report and I will not repeat the detail. But please be aware, as I know most of you are, that responding to requests for your statistics may result in apparent distortions if, as may legitimately be the case, what you count is not the same as what the Code of Practice requires the public authorities count. A request to my office for elucidation might help in an individual case.

(c) Data Retention Directive. I am well aware that the recent European Court decision has caused widespread concern. I am not centrally involved in resolving the issues that have arisen, which, as you know, are with the Home Office for urgent consideration. My role is to audit what happens under RIPA 2000, and not centrally to advise about other future legislation. Nor importantly am I anyone's legal advisor. Suffice to say that I do not read the Court's judgement as precluding all possible

domestic legislative requirements for the retention of data from being Human Rights compliant. Speaking very generally – and I am not going to go beyond this – it is evident that existing UK legislation does carefully regulate the use to which retained data may be put, and to that extent, provides many, but not all, of the elements and safeguards which the European Court says is lacking in the European Directive.

(d) **514,608 Communications Data Authorisations and Notices.** As my report indicates, there were 514,608 communications data authorisations and notices in 2013, the large majority of them from police forces and law enforcement agencies. I am publically committed to investigating whether this very large number may not be the product of institutional overuse. Our Inspectors are engaged at looking into this and I shall personally join a selection of their inspections for that purpose. I emphasise that I have not pre-judged the outcome of this investigation, which may well demonstrate that a number of this order is justified. What we shall look at is the use of communications data in police operations as a whole since you cannot make the necessary judgement from a series of disconnected individual authorisations. If there is overuse, it would occur if proportionality is habitually subordinated to perceived necessity. So we shall look at the strength of the necessity through a series of operations.

I hope that this has given you all a good overview of the work we conduct and, in particular, some of the inquiries we are in the process of undertaking. I would like to thank all of you for coming to listen today and I look forward to your continued cooperation with my statutory oversight function. I would also like to extend my thanks to ISPA for organising this event and to Bird & Bird for hosting.