



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

House of Lords Select Committee on the Constitution

Inquiry into 'The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State'

Additional evidence Submitted by the Information Commissioner

1. The Information Commissioner is aware that the Committee is currently in the process of concluding its inquiry and so is grateful for the opportunity to provide additional written evidence. This evidence relates to the Regulation of Investigatory Powers Act 2000 (RIPA). It is intended to draw the Committee's attention to problems with the definition of "interception" in that Act and the lack of any body with powers to provide advice and promote good practice similar to those powers provided to the Information Commissioner in to the Data Protection Act 1998 (DPA).

The Regulation of Investigatory Powers Act 2000

2. Section 1(1) of RIPA makes it an offence to "intentionally and without lawful authority" intercept any communication in the course of its transmission by means of a postal service or a public communications system. There are several means by which one can obtain lawful authority to intercept a communication. One of these is where both the sender and recipient of the communication have consented to the interception.
3. Section 2 of RIPA provides some definition of when an interception of communication occurs. The interception must occur in the "course of transmission" of the communication and must modify or interfere with the system or its operation; must monitor the transmissions made by use of the system; or monitor transmissions made by wireless telegraphy to or from apparatus comprised in the system. Interceptions of communications do not include references to the interception of communications broadcast for general reception.
4. This approach to the meaning of "interception" is relatively easy to apply in the context of traditional telephony. However, this concept and the concept of both the "sender" and "recipient" consenting is less easy to apply to internet based communications, particular when dealing with transmission of information between a website and an individual's personal computer. On the one hand this can, in some circumstances, leave those developing internet based services exposed to the risk of criminal prosecution even if these services pose little or no threat to privacy. On the other hand the development of some otherwise acceptable services may be curtailed because the developers are not prepared to take the risk of committing the criminal offence of interception.

Targeted online advertising

5. An example has arisen in relation to the development of targeted online advertising (TOLA). A company called Phorm has developed a system where, with the cooperation of an individual's ISP they can profile the addresses and certain content of websites visited by users and then use that information to match that user against predefined broad advertising categories. The ICO is aware that other products are being developed which could operate in a similar way. Indeed some such as Gmail, which scans the content of subscribers' email, are already in operation.
6. Exponents of TOLA state that the user profiling occurs with the knowledge and agreement of customer and within the technological infrastructure of the ISP and that the advertising and profiling can take place in such a way that there is no need to know the identity of the individual users.
7. The problem is that there is confusion over whether the operation of individual TOLA systems constitute an "interception of a communication" under RIPA and, if it does, can companies imply the consent of the website the individual visits to justify the interception?
8. Effectively, this means that if an organisation develops a product where its operation might be seen as an interception of a communication, they have nowhere to turn for advice.

The Data Protection Act 1998

9. The Information Commissioner's interest stems from the connection between RIPA and the DPA. The first data protection principle states that processing of personal information must be fair and lawful. Any processing of personal information which is in contravention of the provisions of section 1(1) of RIPA would also be a breach of the first principle. Understandably organisations approach the ICO for advice. However, it is inappropriate and arguably beyond his powers for the Information Commissioner to advise on the nuances of RIPA. He does not have particular expertise in this area. Furthermore, this advice could expose those seeking it to criminal prosecution, given that the Information Commissioner is not the prosecuting authority for offences under RIPA.
10. Section 57 of RIPA creates the role of Interception of Communications Commissioner, but his role is limited to overseeing the persons who issue warrants, and the procedures of those who are acting under warrant or who are assisting those acting under warrant. RIPA places no duty on the Interception of Communications Commissioner to provide advice to those who want to ensure they are acting in a manner which is in compliance with RIPA, nor is he resourced to provide such advice.
11. The Home Office has issued general guidance on the operation of RIPA in relation to targeted online advertising, but this general statement did not address the specific concerns about the operation of individual TOLA systems, or the technical issues around whether the specific actions of such systems would constitute an interception of communications.

12. In contrast, when the ICO is approached for advice as to the application and applicability of data protection law, the ICO is empowered to provide such advice under section 51 of the Data Protection Act 1998. Indeed, the ICO is under a specific obligation to promote the following of good practice which includes but is not confined to compliance with the requirements of data protection law. The problem is that whilst the DPA and RIPA together form part of the framework of regulation that limits excessive surveillance and provides safeguards for individuals it is only in relation to the DPA that there is an organisation charged with promoting compliance with the legislation and with providing authoritative advice to those who need it.