The Foundation for Information Policy Research and the Open Rights Group

Consultation response on

Regulation of Investigatory Powers Act 2000 Consolidating Orders and Codes of Practice

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

The Open Rights Group (ORG) is a grassroots technology organisation which exists to protect civil liberties wherever they are threatened by the poor implementation and regulation of digital technology.

FIPR was actively involved in lobbying parliament during the passage of this Act, and subsequently as regulations have been promulgated. ORG members were also involved. We have since observed it in operation. We believe that many of FIPR's original criticisms have been borne out in practice. We hope that the next Government will replace RIP with a regulatory structure along the following lines.

1. The police should be permitted to use intercepted content in evidence, as they are in most civilised countries.
2. In consequence, wiretap warrants should no longer be issued by ministers but by High Court judges.
3. The use of traffic data should also require a judicial warrant, but at the level of a magistrate. Since this type of request is uncommon, this will not be a significant burden over and above existing requests for search warrants.
4. The overwhelming majority of all RIP requests are for reverse directory lookup, where the owner of a phone number or IP address is identified. These should continue to be available to the current wide range of public bodies on their own authorisation.
5. Local authorities do not make many RIP requests of any kind, and so their staff are usually not familiar with the procedures, the possibilities, and the appropriate tests for proportionality and necessity. Prior to the introduction of RIP all requests were made through a central portal (in Northamptonshire). This scheme should be resurrected for reverse directory lookups. Moreover, if a council official, such as a Trading Standards Officer, has a need for traffic data, he should work through his local police force. Once again, this will avoid requests being performed by people for whom this is a once-in-a-lifetime occurrence.

6. Alongside these changes to the authorisation regime, the controls against abuse need to be dramatically improved. At present the Interception Commissioner has no practical way of detecting abusive access to traffic data or reverse directory lookup. Recent events show that we need a way to detect a journalist who hires a private detective, who then bribes or social-engineers an official into slipping in an extra request about a celebrity. (There are many other possible abuse cases.)
7. We propose primary and secondary controls. The primary control should be the notification by the Communications Service Provider (CSP) of the data subject who is the target of each act of interception, traffic data disclosure or reverse directory lookup. Notification should occur when the data subject is charged, or when the investigation is closed, or after a default period of time – say 90 days. Investigators should be able to request a notification delay from the judge who issued the warrant, or, in the case of reverse directory lookup, from a magistrate. The sworn statements used to support warrants should also be made available to the data subject (with public interest immunity exceptions for secret intelligence) to enable judicial review proceedings to be taken.
8. The secondary control we propose is that all applications for warrants should be reported to the Interception Commissioner by the judge who receives them, together with all judicial decisions on whether to grant them and/or delay notification. All requests for reverse directory lookup should be reported to the Interception Commissioner by the CSP that receives them. The system on which these data are stored should be classified at least SECRET. It should support routines for abuse detection and anomaly detection. It should not contain the results of the requests – merely who made what request, against whom, when, the CSP, the judge if any, and all judicial decisions. The Commissioner should be the data controller of this system and should not be permitted to subcontract its operation to a police force, intelligence agency or other regulated entity.
9. Finally, both warrants and reverse directory lookups should be supported by sworn evidence, which will be made available to data subjects in due course (subject to public interest immunity certificates to cater for secret intelligence matters) so as to enable judicial review proceedings to be taken when appropriate.

This will adopt best practice from elsewhere and give Britain a regulatory regime that is fit for purpose in the 21st century rather than the present mess. It will facilitate legitimate investigation while controlling rogue investigators; inspire public confidence; and avoid creating unnecessary tension between law enforcement agencies and the technical community whose support is essential for robust policing.

Professor Ross Anderson FRS FREng
Foundation for Information Policy Research
Cambridge, July 2009

Jim Killock
Open Rights Group
London, July 2009