Access to Communications Data

Ian G Batten

$Id: ripa.tex,v 1.2 2003/06/05 11:06:53 igb Exp $

Contents

1 Introduction

The Home Office has requested responses from interested observers over the issue of access to Communications Data by law enforcement. Somewhat to the surprise of the public, the scope of "law enforcement" is wider than the police, and the government encountered some resistance to their original proposals. Rather than attempting to cover the entire issue, for which my responses would almost certainly mirror that of many other people who broadly do not trust government with private data, I would like to make some focussed points to attempt to improve the process.

I should make it clear that I agree that law enforcement is entitled to gather information in the pursuit of criminal investigations. My position is that this should be tightly regulated, with a clear process to avoid 'scope creep' extending both the bodies which have access to the data and the purposes for which the data is used.

My proposals are:

- That individuals about whom data is requested, who are not subsequently charged with offences, should be notified of that request at an appropriate time (Section 3);
- That there should be a lay oversight body, able to sample requests and assess their necessity and proportionality (Section 4);
- That the process by which data is requested, obtained, stored, analysed and disposed of should be the subject of a publicly available quality manual, assessed and certified against ISO 9001 or a similar, appropriate quality system (Section 5);
- That there should be penalties, both criminal and disciplinary, against officials who misuse their powers, and that these sanctions should apply to all responsible people within the scope of the process (Section 6);
- That there should be a credible, visible regulatory process covering interception, rather than the current system which provides no sanction, criticism or oversight (Section 7);
- That the bodies able directly to request access to data should be the shortest list possible, consistent with effective law enforcement (Section 8).

2 About The Author

I am Head of Information Technology at a £150 million turnover telecommunications manufacturing concern. I have managed electronic mail systems and Internet connections for my several employers since 1986. I hold a BSc. (Hons) in Software Engineering from The University of Birmingham. My mail address is `igb@batten.eu.org`.

3 Subject Notification

People have an expectation of privacy. If they are confident that invasions of that privacy will be notified to them then they can take the absence of such notifications as confirmatory that their privacy is not, in fact, being invaded. Additionally, knowledge that notifications will be given to affected individuals will prevent officials from misusing their powers to investigate matters outside their remit.

The notifications should be made once the person whose privacy has been compromised is eliminated from the investigation and shown to have no connection to the subjects of the investigation. If it is not possible to determine this point accurately then the latest it may be made is following any trial or decision not to proceed to trial.

The notification would state:

- The information that was requested;
- The purpose for which it was requested;
- The name of the organisation which requested it.

Exceptionally, there would be a process by which such notifications would be withheld. However, this process would require senior intervention and the numbers of notifications withheld would be published annually.

Notifications should be an opt-out process: people would receive notifications unless they explicitly opted not to. There would need to be further discussion in respect of the notification of minors.

The means of notification would require careful consideration, to avoid themselves causing potential difficulty for subjects. It is quite possible that the notification may itself indicate patterns of access which the subject would rather keep secret from their friends or family.

4 Lay Oversight

Law enforcement does not have a happy record with regard to transparency. There is a widely-held view that oversight in the field of security and law enforcement is a toothless dog that never barks. The appointment of a lay oversight body, drawn from outside the security, law enforcement and judicial community, would provide additional confidence that powers were not being abused, because a report stating that all is well would have more credibility. This body would:

- Sample requests chosen at random — but covering all bodies which are empowered to make requests — for correct procedure, proportionality and necessity;
- Recommend disciplinary or criminal investigation in relation to requests that they feel are improper;
- Discuss matters of policy and provide a sounding board for developments;
- Issue an annual report describing their work.

The people involved in this lay oversight body would probably require clearance involving at least Positive, if not Developed, Vetting. This may reduce the pool of people who would be prepared to undertake such screening, and yet who could reasonably be described as ‘lay’. This would be a topic for further discussion if the proposal were accepted, but I do not believe the problems — which can be attacked with non-disclosure agreements, removal of personal details from requests being examined and other measures — are insurmountable.

5 The Use of a Quality System

The processes by which data is requested, obtained, stored, analysed and disposed of are critical to public confidence. Obtaining certification under ISO9001 would provide some public confidence that the processes were strong; annual audit reports by the certificating body would show that they were being adhered to.

Moreover, the discipline involved in operating within a quality framework — including (but not limited to) correct record keeping, clearly defined training requirements and strong definitions of rôles and responsibilities — would improve the efficiency and effectiveness of the organisations making requests.

Again, the auditors would require clearance: this situation is no different to that existing within defence sector concerns which hold ISO9001 certification and auditors with appropriate clearance are available.

6 Penalties

Many people were offended by the fact that the Regulation of Interception Powers Act places far more emphasis on sanctions against citizens subject to its powers than it does on sanctions against officials who wield its powers. There should be clearly defined criminal penalties against people who misuse the powers vested in them.

The offences should be defined to include:

- Signing a request which is later found to be improper, when a reasonable application of the skills expected of the post-holder would have made them refuse to sign;
- Acting upon a request which has not been been correctly signed if should be apparent to a reasonable person that the signatures on it are defective;
- Failing to keep secure the results of a request for data, or retaining the data beyond the lifetime of the investigation.

7 Regulation

The current system of oversight of the interception regime has no credibility, and is widely seen as a rubber stamp on the actions of government. A regulator should be appointed from outside the magic circle of the security services and the judiciary, who will take a questioning and skeptical view of the claims of law enforcement.

The regulator should be empowered and required to:

- Investigate allegations or suspicions of malpractice, with the power to compel testimony from officials;
- Issue an annual report, covering the numbers, purposes and outcomes of data requests, broken down by requesting body;
- Ensure that the process by which requests are made is robust, and that it is being followed.

8 Authorised Bodies

The issue of the original SI caused surprise because of the breadth of bodies who required access. The detailed cases provided by the Home Office subsequently did not make terribly convincing reading, and it is questionable if some of the para-legal bodies have the experience or processes to handle confidential data.

Therefore, the list of bodies which can make data access requests should be limited to only those that can show each of the following:

- That they have a regular, proportionate requirement to access data;
- That they request data sufficiently regularly that they will develop a body of experience of best practice;
- That they have robust processes to ensure the requests are necessary and proportionate;
- That they are in a position to handle the resulting data securely and properly.

It is a matter for discussion what bodies which do not meet these criteria, but which nonetheless have legitimate requirements, should do. A central clearing house would find it difficult to scrutinise requests, and would rapidly degenerate into a rubber stamp operation. Judicial oversight may be an excessive drain on resources.

I would advocate ‘pairing’ bodies with legitimate needs with an appropriate other body which meets the above criteria. The incremental load would be small, but it would be hoped that the certified body would develop an understanding of their ‘paired’ body’s requirements such that they could provide effective scrutiny.

9 Conclusion

I hope that these proposals can, in some way, improve the quality of the data access regime. Mistrust between government and the governed is not healthy, but sometimes government must accept that its *bona fides* are not taken as an article of faith by the population at large. It is better to shine a light on areas of suspicion and prove them to be clean, than it is to blindly assert that there is nothing to be worried about.