

From: Dr Chris Pounder
Sent: 05 December, 2002
Subject: Personal: Evidence to APIG

Dear Sir

I have worked on a professional basis in the privacy area since 1983 and I am well known in the data protection field. The attachment contains are my "top ten" recommendations in relation to communications data which I hope the Committee will consider for inclusion in its deliberations. The recommendations are not ranked in importance.

These recommendations are made in a personal capacity and do not reflect the views of my employer.

I am ready to help the Committee in further ways if this would help its deliberations.

Yours sincerely,

Chris Pounder

Recommendation 1: The Committee should examine whether public bodies who have powers to access communications data are likely to use statutory gateways which permits the onward disclosure of communications data to other bodies. If this occurs, such onward disclosure should only occur if the conditions identified in RIPA should be applied to the onward disclosure.

Reason:The provisions in RIPA dealing with communications data do not provide a local authority with a power to access to communications data from an ISP (for example) in order to assist in the collection of Council Tax. However, the police who can have powers to demand access to communications data have other discretionary powers which permit disclosure to a local authority (e.g. for the purpose of Council Tax collection via Section 29 of the Data Protection Act 1998) or via provisions in Crime and Disorder legislation. Such gateways provide a mechanism for local authorities to obtain communications data.

If such secondary disclosures of communications data are to occur, the protections established in RIPA which apply to the obtaining of communications data from a telecommunications company or ISP should; also apply to this onward disclosure. Such disclosures should also be subject to review by a Commissioner.

Recommendation 2: There are too many Commissioners, the complaints system lacks credibility, is cumbersome and overlaps – it should be replaced by one or two Commissioners – one dealing with national security issues and the other being the Information Commissioner. One solution the Committee could explore is to have a revamped Information Commissioner which can deal with RIPA and national security issues.

Reason:The Annual Reports of the Commissioner for the Interception of Communications Act 1985 records the number of cases heard by the Tribunal (which will be similar to the Tribunal established under RIPA). Between 1996 and 2002, there were over 400 cases considered by the Tribunal; none have been adjudicated in favour of the complainant. This 100% “perfection”, like 100% support for Saddam Hussein in the recent “presidential election” in Iraq, is simply not credible.

Additionally the complaints system is fragmented, overlaps and riddled with competing bodies; it should be replaced by a one or two Commissioners. For example, in relation to personal data, national security and RIPA the following public bodies could be involved in the providing protection to the public: the Information Commissioner, the Information Tribunal, the Information (National Security) Tribunal, the Security Service Commissioner, the Security Service Tribunal, the Secret Intelligence Service Commissioner, the Secret Intelligence Service Tribunal, the Interception of Communications Commissioner, the Interception of Communications Tribunal, the Surveillance Commissioner, the Surveillance Tribunal, the Investigatory Powers Commissioner for Northern Ireland, and possibly the Police Complaints Authority if an investigation extends to the police.

It is interesting to note that under the heading of “Tribunal”, paragraph 33 of HC 1244 and paragraph 65 of HC 1243 (published last month) use almost identical wording (and statistics) – even though the bodies reporting to Parliament are different. Clearly, even with their differing responsibilities, if the Interception of Communications Commissioner and the Intelligence Services Commissioner finds benefit in “joined up” Annual Report writing when describing complaints, it is reasonable to assume that these benefits should also accrue to the complainants and supervisory system itself.

Recommendation 3: All authorisation officers who allow access to communications data should keep statistics as to such authorisations so that Parliament can be informed as to the extent that communications data are accessed. If this is difficult, communications providers could also be required to keep access statistics.

Recommendation 4: The Commissioner responsible for reporting on access to communications data should have the power to require statistical returns from those who are authorised to permit access to communications data. The Commissioner should be able to describe the nature of the statistical return should be free to publish the number of requests. This is to ensure clear reporting of accesses to communications data to the Commissioner, and transparency to the public.

Reason:Recent answers to Questions tabled by Harry Cohen MP from October 2002 show that some Departments do not know (a) the number of access requests they are expected to make or (b) the number of authorisation officers or (c) both.

However, one recent answers reveal that the Metropolitan Police issued 155,000 requests for communications data last year; it follows that the total number of requests for communications data, across the public sector as a whole, will number millions.

Note that a single demand for access could involve communications data which relate to a number of individuals. If you read RIPA provisions carefully, they use the word “person” – and person could thus be a legal person. So a request which states “give me communications data which relate to Organisation X” counts as one request but involves extensive access to communications data which relate to all those who called Organisation X.

In any event, the Committee should demand some basic statistics on the use of these powers.

Recommendation 5: The Committee should consider the impact of predictive use of communications data and whether there should be limitations on predictive use.

Reason:There are arguments that predictive use should be limited to terrorism and cases of serious crime as the public could distrust the authorities if communications data are trawled to explore who might be connected with minor misdemeanours. The Committee should come to a judgement as to when predictive uses are possible.

“Predictive use” is a problem because it involves processing communications data in order to find those who match patterns of suspicious behaviour; this is different to the situation where the authorities already have grounds for suspicion and are seeking access to data to pursue proof. Additionally, because someone matches a profile does not necessarily mean that they are guilty, and if this is the case, such individuals could come under very close scrutiny.

Recommendation 6: In cases where the Commissioner responsible for reporting on access to communications data comes across an inappropriate use of access powers, then he should have the power to oblige the public authorities involved to contact the individuals concerned and to apologise, and where appropriate to alert them to available remedies. This is especially the case when predictive use of communications data results in an individual’s life coming under close scrutiny based on assumptions which are proved to be false. Communications providers should be able to seek the advice of the Commissioner if they have reason to believe that a request for access from a public body is excessive.

Recommendation 7: Deliberate breach of the provisions of a Code of Practice could result in an individual and/or the public body concerned being prosecuted. This is to ensure that the provisions of the Code are taken seriously.

Recommendation 8: Codes of Practice in relation to communications data should be statutory and produced in an independent manner.

Reason:The main problem with Codes of Practice is a structural one, as the Secretary of State producing the Code of Practice is also largely responsible for some of the public bodies which wants to interfere with private life – consequently, there is always an in-built bias in favour of interference. This structural deficiency is common to **ALL** Codes of Practice produced by **any** Secretary of State

This is one reason why Lindop Committee on Data Protection (Cmnd 7341, 1979) recommended that Codes of Practice should be produced by the Data Protection Authority for the approval of the Secretary of State. Although this was rejected by the Conservative Government in the early 1980’s Lindop’s approach might be worthy of reconsideration by the Committee. Lindop also suggested that the Data Protection Authority should be able to deal with national security issues, through the appointment of a figure who had been vetted by these agencies.

I am confident that Parliamentary time will not be diverted into looking at the minutiae of the Codes. For example, the Code could be drafted by the Information Commissioner and subject to the input from the Secretary of State. If this process did not produce consensus on the text of Code, then two SI's making reference to the two drafts could be presented to Parliament, and debated at the same time. Parliament could debate and then vote upon which one it preferred.

Recommendation 9: There should be an annual debate on privacy matters.

Recommendation 10: Personal data which include communications data held for policing purpose should be subject to consistent set of data protection rules.

Reason:The Security Service Acts do not define national security however the Security Service have a role in assisting the police in cases of serious crime. The Home Secretary has issued a Certificate (placed in the House of Commons Library) which equates the role of the Service as safeguarding national security,

This has a knock on effect for personal data processed for policing purposes, for when the police process personal data, the data are subject to Section 29 of the Data Protection Act 1998 (DPA), whilst if the Security Service process the same personal data, the Certificate claims that such data are subject to Section 28. Thus the same set of personal data can be subject to different data protection rules depending on which organisation holds the personal data.

In practical terms, the national security exemption in the DPA is very broad. Thus, to take an extreme example, if the police were to process personal data which were of risk of breaching the Data Protection Act, the mere act of passing such personal data to the Security Service could remove the risk of a breach.

Dr. Chris Pounder (December 2002)