



**Response To:**

**'Access to Communications Data.**

**Respecting Privacy and Protecting the Public from Crime.**

**A Consultation Paper.'**

**John R T Brazier**

**Professional Projects Co Ltd**

**19 Barttelot Rd**

**Horsham**

**RH12 1DQ**



## Contents

<b>INTRODUCTION</b> .....	<b>3</b>
<b>CONCLUSION</b> .....	<b>3</b>
<b>APPROACH</b> .....	<b>3</b>
<b>COMMUNICATIONS DATA: DEFINITION</b> .....	<b>3</b>
<b>PRIVACY: RELATIVE OR ABSOLUTE?</b> .....	<b>4</b>
<b>INTRUSIVENESS</b> .....	<b>4</b>
<b>PUBLIC AUTHORITIES WITH ACCESS</b> .....	<b>5</b>
<b>CENTRAL VS DISTRIBUTED CONTROL</b> .....	<b>5</b>
<b>NOTIFICATION</b> .....	<b>6</b>
<b>SANCTIONS</b> .....	<b>6</b>
<b>CONCLUSION</b> .....	<b>6</b>



## Introduction

This document is a response to *'Access to Communications Data. Respecting Privacy and Protecting the Public From Crime. A Consultation Paper'*, published in March 2003 by the Secretary of State for the Home Department. It provides clear conclusions and makes recommendations.

## Conclusion

It is the recommendation of Professional Projects Co Ltd, and the author, that the Government should restrict the number of new public authorities with access to communications data to as few as possible. In addition, the following comments are made:

1. The definition of communications data vs content is unlikely to hold, and will need to be constantly reviewed.
2. There is at least one example of absolute privacy (client/lawyer confidentiality). Stating that all privacy is relative is inaccurate, and the debate should be so informed.
3. The controls should match the level of intrusiveness of the access request.
4. Only public authorities with life-saving or serious crime duties should be given access.
5. There should be a central agency to manage access requests.
6. People who have been monitored should be notified.
7. There should be appropriate sanctions for privacy violation due to misuse of access.

## Approach

The consultation paper covers a large number of issues, many of which will be a constant source of discussion as society periodically re-evaluates the balance between privacy and public safety. Because of the continuing nature of the debate, this paper addresses some key issues with regard to communications data, and some of the general principles by which the access to this data should be handled. It does not attempt to be exhaustive in its treatment.

This response deals with seven basic topics. It is proposed that these discussions support the conclusions given above.

## Communications Data: Definition

The consultation paper (page 7) provides what appears to be a clear set of definitions as to what is 'communications data' as compared to 'content'. For example, routing information for an electronic mail is deemed to be communications data, whilst the subject line is content.

However, this apparently clear separation will break down in practice: there is an indication of this in the definitions themselves. One URL is treated as traffic data, yet another (the result of a query) is content. Under normal conditions it will be very difficult to separate the two. Another example is when servers update each other with directory information in a distributed system: the content is data about resources and names which will become 'communications data' subsequently.



The fact is that modern communications systems have not been developed with monitoring in mind. Thus the way they operate does not match arbitrary classifications such as 'communications data' and 'content'. This will have practical implications for the gathering of such information, and one suspects that the situation will change in time as new technologies come into effect. The conclusions are that (1) there will be court cases before these definitions are fully accepted; and (2) some body will have to be brought into being to try to maintain these definitions and regularly update them.

## **Privacy: Relative or Absolute?**

In the forward by the Home Secretary on page 3, there is a statement 'In a democratic society, privacy is a right but not an absolute right'. This statement has generally gone unchallenged in these debates, yet is not entirely accurate.

There is an actual right to privacy between a client and his lawyer. Whilst there are certain limitations (such as this right cannot be abused for the furtherance of crime), the basic position of confidentiality between a client and his lawyer is regarded as 'a fundamental condition on which the administration of justice rests' (Archbold, 2002, p1238 – 1239). In this case, this absolute right to privacy is due to the general belief that this is beneficial to society.

Whilst the case of confession to a priest has not been absolutely decided in law, in practice a minister is never required to give details of a confession in a court. Similarly, doctors are not expected to give patient details (even if there is no legal privilege in such cases).

The point is important. The original Regulatory of Investigatory Powers Act 2000, and the secondary legislation to which this consultation pertains, have always been couched in terms of relative privacy. Yet we have one absolute example of complete privacy, and two examples of where the courts pragmatically allow absolute privacy. Thus whilst privacy may usually be relative, it can occasionally be inviolate: and the debates on this subject should be carried out in the light of this fact. The temptation to say 'all privacy is relative' – perhaps to aid in the formulation of legislation – should be avoided.

## **Intrusiveness**

One of the issues in the consultation document is the different levels of intrusiveness inflicted for different types of access to communications data. At one level, there is a single 'reverse lookup': to whom does this phone number belong? This might be done for an emergency, and the intrusiveness is relatively low (although consideration needs to be given to the case where people have specifically asked to be ex-directory).

However, another extreme is where all a suspect's communications are tracked (but not read): what is known as 'traffic analysis'. This can be highly intrusive and can, in fact, expose a person's complete private life.



Thus whatever regime is put in place, there must be adequate controls commensurate with the estimated level of intrusion. Above a certain level (perhaps more than one or two accesses to a person's communications data in a 24 hour period) there should be specific judicial oversight of the request.

## **Public Authorities with Access**

In general, as few authorities as possible should be allowed access and, within authorities, as few departments and people as is possible. This is because the habit of data access rapidly becomes normal. The intrusion of privacy becomes forgotten in the ease of access, and a culture of privacy invasion becomes endemic. This has clearly been shown in the advertising industry, and in the phenomenon known as 'spam'.

It is recommended that any authority given access to communications data should have originally been given judicial approval. In addition, its access should be limited to what it needs (ie restrict access both by type and purpose). Only authorities which either have a life-saving function or are dealing with significant crime should be given access.

## **Central vs Distributed Control**

Certain agencies, such as the Police, generate a large number of requests. These organizations thus presumably build up an expertise in such requests, and understand what is appropriate, legal and so forth. Other agencies, however, produce very few requests (the Food Standards Agency, for example, is indicated as needing only one or two accesses per year). It is difficult to see how these agencies can ever build up an appropriate level of expertise.

Because of this, it is proposed that all requests for interception/traffic data should go through a centralised system (excepting perhaps the most trivial 'reverse lookups', as indicated above). The large users (such as the police) might actually run the agency (although there could be concerns about this) and service requests for the low-volume users.

The benefits would appear to be clear, such as:

1. the agency would provide consistent handling for all requests, following the law and CoPs;
2. there could a consistently applied categorization for different types and levels of access;
3. consistency of management in personal data collected (including its storage and destruction);
4. there should be an improved level of accuracy in processing requests (as the agency personnel should know what they are doing);
5. the provision of a consultative capability to advise other governmental agencies on the value and use of different levels of access;
6. a centralised system for statistics collection;
7. a central mechanism for audit and accountability;
8. a unified interface between this agency, the judiciary and the CPS;
9. a coherent system to advise subjects when they have been monitored;



10. a pool of expertise to deal with technological changes, so that the government and society can be advised on how legislation in this area should respond to future change;
11. a simplified mechanism for ISPs and Telcos to deal with or question requests;
12. a dedicated infrastructure to handle the technology of information gathering;
13. better management and knowledge of costs.
14. allow for increased public confidence in the system.

For all these reasons we believe the centralized approach allows for better management and consistency as compared to the distributed proposals.

## **Notification**

There seems to be no doubt that if a person has been monitored (for traffic data or actual content), then they should be told after the event. This is a key element of audit and accountability. The agency identified above could handle this.

## **Sanctions**

It is important that illegal access (and illegal requests for access) should merit clear sanctions as criminal offences. In the past agencies misusing their powers often seem to avoid any reprisals for doing so. This is clearly unfair – given the fact that ordinary subjects committing equivalent crimes who get caught are usually prosecuted – and also brings the system into disrepute.

There need to be consistent penalties for privacy violation, applicable to all members of society, including those working in Governmental agencies.

## **Conclusion**

The conclusion, based on the arguments above, is that the government should expand the list of public authorities with access to communications data to as few as possible: those dealing with life-threatening emergencies or serious crime. In addition, the mechanism should be via a centralised agency, with sanctions and notification of the monitored as part of the regime.