Consultation Response: Access to Communications Data

I am writing to respond to this consultation as someone who is currently conducting research into *"Anonymity and Traceability"* at the University of Cambridge – viz: communications data is directly within my field of academic study.

This response is made as a private individual, in order to put forward a small number of specific, and rather narrow, points about communications data. However, I have a background in the ISP industry and have also contributed to or commented upon drafts of a number of organisations' responses, particularly those from the Foundation for Information Policy Research (FIPR) and Thus plc. Those responses usefully reflect the more general opinions that I hold.

I was also the "specialist advisor" to the All Party Internet Group (APIG) for their inquiry into Communications Data in January 2003 and I particularly commend that report's recommendations to you.

Types of Communication Data

It is now clear, as perhaps it was not in 1999-2000 when the RIP Act was being brought forward, that the most useful way of dividing up communications data is into three categories as follows:

a) Reverse Lookup

By "Reverse Lookup" I mean the process of translating cyberspace identifiers into "real world" identifiers. I include the telco world as part of cyberspace, so that this category includes traditional "reverse directory" searches of phone numbers.

It is quite clear that this is the majority case for access to communications data and pragmatism alone suggests that a self-authorisation scheme for investigators – with an effective oversight regime – is the only practical solution.

This type of access is – of course – privacy invasive, in that people may wish to operate pseudonymously, but if the data that is obtained is held confidentially then little damage will be done to the individual concerned.

This low level of potential damage means that I see little value in imposing extra costs or difficulties on investigators by opting for anything other than self-authorisation. Therefore I would be happy to see a RIP s22 scheme widely available to any lawfully authorised investigators – even council planning officials – who met (perhaps very seldom indeed in the planning case) the tests of necessity and proportionality.

However, my communications industry background leads me to suggest that the only way that this could possibly be made to work in practice would be the creation of inter-agency SPOCs. These would provide the day-to-day uniformity in the application of standards and Codes of Practice that would be essential.

b) Location Data

I am convinced by the argument that in a "999" "life-at-risk" situation the emergency services should be able to determine the physical location of the caller. The majority of emergency calls now come from mobiles and it is necessary to design systems that take the implications of this on board.

However, I see no reason why this location data should be accessed by giving specific powers to individual emergency services, but would recommend the creation of a suitable inter-agency organisation that could be staffed on the necessary 365 x 24 basis and would interface with the phone companies as required. Once again, the central organisation would be in a position to build up a consistent set of standards and expertise which, I predict, would not happen with, in particular, the Coastguard where individual officials might only deal with a handful of requests per year.

c) Other Communications Data

Into this category comes "everything else", particularly usage data (the contents of phone bills) and access to location data for all other purposes other than "life at risk". In particular, I envisage that access to location data for the investigation of hoax 999 calls would come into this category.

I do not believe that this type of communications data should be made available to any of the non-police organisations named in the consultation.

I come to this view partly because I consider some of the cases that were made out to be laughably weak (The Gaming Board springs to mind). The remainder of the organisations are accessing so little data that they will never build up expertise in fully understanding it. Although a group such as Trading Standards might – as an organisation – handle many requests per year, few individual officers would do so.

The way forward here is for this type of investigation to be done as a joint operation with the police – as indeed many of the organisations are already doing. This approach will improve standards all round. For just the same reason, the powers already given to the Inland Revenue under s25(1)(e) should be withdrawn.

The figures provided to support the consultation show that organisations that perform similar investigative tasks currently make radically different numbers of access requests. This is *prima facie* evidence of incompetence in using the available data, which will not be improved except by inordinate ongoing expense on training.

I do note that joint operations with the police are not universally favoured because of the reluctance of the police to assist other agencies on "unimportant" investigations. This should be addressed by centralised re-negotiation of priorities and indeed by appropriate budget allocation. In this context it should be noted that the APIG inquiry heard that the police were currently under-funding their own internal SPOCs, suggesting that on a day-to-day basis, access to communications data does not always have the importance that some ascribe to it!

The Data Categories in the RIP Act

It should be carefully noted that the division of communications data set out above is not that in RIP s21(4). However, for access to "Reverse Lookup" data to be treated specially (and indeed "Location" data) it is essential that this should be clearly defined in statute.

The current position where Reverse Lookup data is under the catchall (c) category is unacceptable. A clear definition will assist in building public confidence and prevent "case law" from damaging the balance this consultation seeks to define.

For the Record

Since consultations are often about collecting statistics as well as understanding viewpoints, for the record I wish to state that:

- I consider it very important that there be criminal sanctions for those who access communications data improperly.

- I believe that informing individuals when their communications data has been accessed (not necessarily the "reverse lookup" case, but definitely the more specialised access) will be of significant benefit to the oversight regime in ensuring that excessive access is remarked upon and looked into.

- There is a desperate need for better statistics on communications data access requests. Besides being a useful tool for the oversight regime, it should allow comparative studies on the use of access requests, leading to the identification of investigators who are unaware of the benefits or possibilities of using them.

- I believe that the law should forbid "end run" access to communications data by "legacy legislation" allowing access to "information".

- I believe that a much wider debate on privacy topics is long overdue and would welcome the Home Office engaging in such a debate.

  However, I disagree with the exact nature of the "lightning rod" analysis of last summer's events. I believe that the public were reacting not to privacy issues *per se* but to the way in which "non-policemen" have been empowered (over many years) to investigate crime. It is the widespread perception that these investigators are not as trustworthy as the (themselves cynically viewed) police service that should concern the whole of Whitehall.

Richard Clayton
66 Huntingdon Road
Cambridge, CB3 0HH

3 June 2003