Skills 1st Limited
2 Cedar Chase
Taplow
Bucks
SL6 0EU

Tel: +44 (0)1628 782565
email: office@skills-1st.co.uk

30. April 2009

Nigel Burrowes
Communications Data Consultation
Room P.5.37
Home Office
2 Marsham Street
London SW1P 4DF

Dear Sir,

Communications Data Consultation

I write in response to the consultation paper *Protecting the Public in a changing Communications Environment,* Cm7586, dated April 2009.

I am an Information Technology consultant with more than 20 years experience. In a previous job I was in charge of a large enterprise network, so I know the value of communications data in investigations. I now specialise in directory services and e-mail systems so I am well aware of the privacy and data-protection implications of databases.

The consultation paper asks four questions which I will address in turn.

> *Q1 On the basis of this evidence and subject to current safeguards and oversight arrangements, do you agree that communications data is vital for law enforcement, security and intelligence agencies and emergency services in tackling serious crime, preventing terrorism and protecting the public?*

Answer: **no**. This question muddles two concepts: the desirability of data access and the adequacy of safeguards. While I agree that some level of access is desirable, I do not find the current safeguards adequate.

> *Q2 Is it right for Government to maintain this capability by responding to the new communications environment?*

My answer to the literal question on its own would be “yes”, but in the context of the rest of the paper I feel that the only safe answer is **no**. The reason for this is that the proposed regulations would not simply maintain an existing capability: they would vastly expand it into realms that no democracy could sustain.

The consultation paper assumes that communications data has always been available to public authorities and that this is an unalloyed public good. This is simply not true. There was no routinely-collected communications data at all until the advent of computer-controlled telephone exchanges in the 1980s, and even then it only covered telephone calls between subscribers on those exchanges. At that time people made far less telephone calls than they do now, and their use of the telephone was only attributable to them while using their own home instrument.

Communications data now includes mobile telephone data, which has the potential to disclose the physical location of the subject at all times when the phone is turned on, whether it is in use or not. The flow of letters through the post was not routinely recorded in the past, but modern sorting technology offers the possibility of doing that. E-mail and similar technologies have shifted a lot of communication from the untraceable face-to-face and postal modes into the realm of traceable communications data, again vastly increasing the amount of detailed personal information that would be kept about each and every one of us.

The paper is careful to make the distinction between communications data (which will be recorded) and content (which will not, or at least is supposed to require an interception warrant). I do not find this very reassuring. The trend in communication modes is towards a large number of small messages rather than a few large ones. Many of these messages are carried on protocols such as HTTP, where the “communications data” (URL in this case) often carries a significant amount of “content”. Anyone with access to the communications data records would be able to reconstruct much of the content of a discussion.

Looking to the future, there will be a vast increase in the use and scope of mobile technologies. Many of these are converging on the use of a mobile-phone-like handset as the primary human interface. Couple that with the increasing use of home automation, remote light switches etc, and it is clear that “communications data” will soon reveal the most intimate details of everyone's day-to-day lives. Just using the mobile-phone and home-automation example, a snooper could easily discover:

- Where I live
- Who else lives there
- Who visited, and on what occasions
- Who slept with who, and on what occasions
- What room each person was in at any time
- Exactly when each person went to the lavatory
- Exactly when lights and appliances were turned on and off, and by whom
- What books magazines and newspapers each person read, and where they were at the time

Retaining this data is not “maintenance” of a capability: it is a very severe expansion and a significant erosion of privacy.

It might be argued that such trivial local messages would not pass through public communications networks, but that is a false assumption. The trend is towards the use of multiple networks and distributed service provision. I have already witnessed visitors to my own house exchanging phone numbers using two different mobile networks, the Internet, and several intermediate service providers.

> *Q3 Do you support the Government’s approach to maintaining our capabilities? Which of the solutions should it adopt?*

Answer: **no**. Of all the options the only one that I feel at all comfortable with is “do nothing”.

The “middle way” favoured by the consultation paper is a thinly-disguised outsourced version of a massive state-owned database. It requires communications providers to analyse everyone's traffic at all times, to store session data, and to index it comprehensively. I can see that investigators would love to have such a tool, but the potential for misuse is truly terrifying.

Q4 Do you believe that the safeguards outlined are sufficient for communications data in the future?

Answer: **no**. There are no safeguards that could be applied to such a store of highly-personal information that would prevent future governments from misusing it. If such a store were to be created it is certain that it would be misused. Its very existence would lead to a controlled society in which people are afraid to express any opinion or read any non-government-issued text in case it were later held against them – whether in a court of law or not.

I consider even the existing situation to be unsafe. The Regulation of Investigatory Powers Act allows police and other public officials to obtain communications data from service providers on the signature of a senior officer in their own organisation. The Investigatory Powers Tribunal is not an effective protection, as the Act makes it a criminal offence for the fact of the data disclosure to be itself disclosed to the subject. If a citizen does not know that their data has been disclosed, how can they make a complaint?

The only safeguard that seems to have any strength is to make the gathering and correlation of data *hard work*. Regrettably this must apply to honest policemen investigating serious crime just as much as it does to a potentially-repressive arm of government.

Further, I would make a requirement that the organisation disclosing data relating to an individual must inform them of the disclosure within a reasonable time, stating what data were disclosed, who to, and for what reason. Obviously there should be a delay in this process to allow legitimate use of the data in investigations, but the delay should be short enough to ensure that mis-uses of the data can effectively be brought to account.

Gathering detailed data on the day-to-day lives of honest citizens does not make us safer. Official statements tend to justify this erosion of liberty using the currently-fashionable bugaboos: Terrorism, Paedophiles, and Drug Dealers. The damage done to society by such evil people pales into insignificance beside the effect of a database such as the one described in this paper.

The implementation costs of the proposals are given as £2 billion. There would undoubtedly be continuing maintenance costs as well. I find it hard to believe that the proposed database could provide an economic benefit sufficient to justify itself on financial grounds even if it were morally acceptable.

I strongly recommend reading *Schneier on Security* (Wiley). It is a collection of essays by Bruce Schneier, who is a leading thinker in the IT security industry. In particular, the short article titled *The Value of Privacy* is particularly relevant: it was originally published in *Wired* and is available online at
http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886

In summary, I am very worried by the trend evident in this consultation paper, and I am strongly opposed to further expansion of government access to personal data.

Yours faithfully

Dr Andrew Findlay BSc PhD MIET CEng

This is an open letter. It is published on the web at:
http://www.skills-1st.co.uk/papers/policy/commsdata-200904.pdf