2 Cedar Chase
Taplow
Maidenhead
SL6 0EU

andrew@findlay.org

Dominic Grieve QC, MP
House of Commons
London
SW1A 0AA

4th April 2012

Dear Mr Grieve,

Communications Data Monitoring

Summary

It seems that the government is again planning a massive surveillance exercise against its own citizens.

Large-scale communications data monitoring is dangerous. It is bad for society, and can have extremely serious unintended consequences for individuals. Monitoring affects everyone, not just criminals. In fact it is probably easier for criminals to avoid it than for honest citizens to do so.

In this note I hope to show you why communications data monitoring should not expand, and to persuade you to work to keep it out of the Queen's Speech.

Watching the people

Will this government follow the previous one in trying to watch and control every moment of its citizens' lives?

I wrote to you in 2009 when the previous government was planning to gather massive amounts of data about citizens' communications. At that time, your party seemed to oppose the intrusion so why is it now talking about doing exactly the same thing?

I am a consultant with 25 years experience in the networking industry, so I understand the potential value of the data that the security services want to collect. I also understand the dangers of such data.

The measures being discussed are not 'maintaining' a capability: they would massively increase the intrusion into the lives of everyone in the UK.

This is not just data about 'them': about terrorists, drug dealers, organised criminals. It is data about *us*. About you. About every member of your family. About your children's friends. About judges and MPs and Attorneys General. No amount of privilege or ex-directory orders would stop the storage and processing of this data.

The distinction between 'communications data' and 'call content' is a smokescreen. An enormous amount of information can be derived from communications data, which is why the security services want it.

Industry Trends

To understand just how dangerous these proposals are it is necessary to look at some trends in the IT industry:

- All forms of communication are converging on the Internet as a carrier.
  This includes such simple things as the link between a light-switch and the lamp that it controls.
- The mobile phone is increasingly used as the user-interface for other devices.
  This includes simple things like light-switches and thermostats as well as complex ones like TVs. Most of these applications are based on Web protocols.
- Apparently simple services are often made up of components in many locations.
  You might program your lights to come on while you are on holiday using a website owned by the light-switch manufacturer and hosted by a third party in a foreign country. You might not even be aware that the communication reaches outside your own house.
- Networked services are increasingly 'location aware', so many devices routinely report their exact location to remote servers.
  This means that your phone's light-switch application can show you the controls relating to the room that you are in. The location data really is that precise, and it will get better.
- Most of the new services use very short messages.
  In the case of the light-switch application the message may be so short that it almost disappears, with the instruction being carried entirely in a web URL. Your precise location has just become 'communications data'.

The effects of storing communications data

Using the simple example of networked light-switches and current-generation mobile phones, let us see where the storage of communications data will take us.

At *any time* in the future, this data could be used to reconstruct your day:

- When your alarm clock sounded
- How long you spent in the bathroom
- Who slept in your house last night, and in which rooms
- When you left the house
- Exactly where you went, in what car, with whom, and how fast
- Who you met during the day
- How often you checked your mail (and who the messages were to and from)
- Where you ate in the evening - and in whose company
- What TV programmes you watched
- What subjects you researched on the web
- When (and precisely where) you went to bed

It would also show other things:

- Was your house empty during the day?
- Did you remember to set the burglar alarm?
- The identity of every visitor and tradesman, and whether they had keys to enter the house in your absence
- Which online suppliers you buy from, and when you are expecting a delivery

The same amount of detail would apply to children: possibly more so, as younger people tend to be more intensive gadget-users.

Now imagine that same data being made available in real time. The precise location of every member of your family *right now* could be in the hands of a criminal. Do you want that to be possible?

We cannot trust *anyone* with a data source of this power. Consider what the police did with stop-and-search under PACE, the harassment of photographers under the same act, what local authorities have done using RIPA. People will twist the power to their own ends, and the public will suffer for it.

Even if we assume that everyone with official access to the data is honest and fundamentally good, there will be leaks. GCHQ might not leak, but we know that the police does – it has been proved in the courts and a few officers are in jail as a result. What would be the consequences of a Wikileaks-style release of a years-worth of such data on every member of the House of Commons?

Communications data is indeed valuable in investigations, but it is already too easy to obtain. The only reliable safeguards that I can see are:

1. Don't collect the data in the first place
2. If data must be collected then delete it within a few days
3. Make it require significant effort and money to access the data. The effort and cost must apply to the security services just as much as anyone else.
4. Require communications companies to notify the subject of the data within 12 months of its release. Do not permit exceptions for any reason whatever.

Terrorists are an excuse

Too many repressive acts are justified by reference to terrorists, drug dealers, and organised crime.

It is said that terrorists wish to curtail our freedoms. No terrorist has ever directly affected my freedom or that of 99.999% of the world population. It is government and police actions that curtail freedom – actions ostensibly justified by the threat of terrorism.

Society must accept that some terrorists will succeed, and that some criminals will escape justice. This is unfortunate, but the alternatives are worse. Ever-increasing surveillance of innocent citizens is producing a society that looks over its shoulder rather than moving forward. Storing communications data on the scale now being discussed will have a seriously chilling influence on legitimate activities. It will certainly hold back the development of useful networked services.

Act for an open and safe society

Please use your position in government to prevent the further surveillance of innocent citizens. The surveillance culture has become a greater danger to society than the threats it claims to be working against.

Yours sincerely

Dr Andrew Findlay BSc PhD MIET CEng

This is an open letter: I have placed a copy on the web at:
http://www.skills-1st.co.uk/papers/policy/dominic-grieve-commsdata-20120404.pdf