Date: Tuesday, 14 July 2009
Name: Dephormation.org.uk
Contact: Pete
Address:

'Protecting the Public in a Changing Communications Environment'

Question 1 - 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?

1

Dealing with the points in the question in turn;

Current Safeguards and Oversight Arrangements

There is precious little evidence to suggest that current safeguards and oversight arrangements are at all effective.

Few (if any) complaints made to the Investigatory Powers Tribunal have ever been upheld. The predecessor, the Interception of Communications Tribunal, did not uphold a single complaint in its 13 years of existence.

Concerning the conduct of covert trials by BT/Phorm of illegal interception, no Police force was prepared to investigate RIPA offences, the Interception Commission claimed they were not empowered to act, and the Information Commissioner claimed to be generally powerless to prosecute despite malicious DPA/PECR transgressions.

The ICO further stated that they were 'not technical experts', and incapable of comprehending the information technology they were being asked to regulate.

So, inverting the question; what compelling evidence is there that present safeguards are effective to protect the public given the complete failure of Police/Information Commissioners Office/Interception Commissioners to act on substantial complaints about widespread illegal interception by BT? None.

Use of Communications Data by Law Enforcement, Security, and Intelligence Agencies

Communications data is obviously essential for intelligence gathering, but it is also essential to respect the privacy/security/integrity of the communications of the vast majority of innocent people who are not and never will be engaged in serious crime, terrorism, or pose a risk to the public.

The question then arises what is the communication information that is necessary to capture, and who is it necessary to target?

Communications Data

When a person is suspected of a serious criminal offence, the capture and decoding of communication content should be *comprehensive*. There are a plethora of communication techniques which sophisticated (and even unsophisticated) criminals might employ, and those methods can only be determined by detailed analysis of data.

Proportionality

In a democratic free society a simple principle must be retained; interception should only be used to monitor communications of the minority of people who are suspected of serious criminal offences (and absolutely no one else). When a person is not suspected of a crime, the volume of data collected should be **nil**. A warrant must be required for such surveillance to take place, with effective safeguards.

Recommendations

1. **To ensure confidence in the sufficiency of present safeguards, the role of the Interception of Communications Commissioners should be reviewed. If no complaint is ever upheld, there is no need to maintain such an expensive facility for complaint. More likely, the Commissioners are failing in their role to 'protect people in the United Kingdom from any unlawful or unnecessary intrusion in their privacy'.**
2. **The role of the Police service enforcing RIPA must be reconsidered. If the Police will not investigate or prosecute following complaints of interception offences, no one can have confidence that the safeguards are sufficient. Perhaps a wholly independent enforcement body is required?**
3. **The office of the Information Commissioner must be overhauled. Presently, they employ no technical IT/telecommunications expertise, and claim their resources are constrained. The ICO have been remarkably unwilling to investigate, let alone prosecute, reported offences against DPA/PECR. Consequently, no one can have confidence that the safeguards are sufficient if the regulator lacks the technical skills, resources, powers, and initiative to enforce the law.**
4. **Given the European Infringement proceedings presently in progress (64/08/INSO), it would seem European Commissioners share the view that UK safeguards are presently insufficient.**

   "Following an analysis of the answers received the Commission has concerns that there are structural problems in the way the UK has implemented EU rules ensuring the confidentiality of communications. Under UK law, which is enforced by the UK police, it is an offence to unlawfully intercept communications. However, the scope of this offence is limited to 'intentional' interception only. Moreover, according to this law, interception is also considered to be lawful when the interceptor has 'reasonable grounds for believing' that consent to interception has been given. The Commission is also concerned that the UK does not have an independent national supervisory authority dealing with such interceptions."
5. **Observation, the European Data Retention directive focuses exclusively on internet email and internet telephony [Article 5.1(a)(2) & 5.1(b)(2) & 5.1(d)(2)] but fails to capture TCP/UDP connections to destination IP addresses, thereby failing to capture essential communications data relating to services other than email and internet telephony.**
6. **Communications data should only be captured from the tiny minority of persons suspected of serious criminal offences; consequently requesting voluntary retention or compulsory retention of communications data relating to the majority of innocent persons is wholly disproportionate. A warrant for such intrusive surveillance should be a minimum requirement.**
7. **Where suspicion of a serious criminal offence arises, and a warrant obtained, the data captured must be comprehensive if the methods and/or content of communication are to be accurately determined and/or decoded.**
8. **On no account should any data captured for state security purposes be repurposed to facilitate a commercial service. This will comprehensively undermine trust and confidence in the privacy/security/integrity of the UK telecommunication network, and UK Security Services.**

Question 2 - Is it right for Government to maintain this capability by responding to the new communications environment?

It is obviously necessary to respond to the present communication environment.

However, the safeguards must remain robust.

Recommendations

1. **The present measures place excessive value on web, voice, and email traffic (potentially ignoring a myriad of other communication protocols and methods).**

2. **Where suspicion of a serious criminal offence arises, and a warrant obtained, the data captured must be comprehensive if the methods and/or content of communication are to be accurately determined and/or decoded.**
3. **Communications data should only be captured from the tiny minority of persons suspected of serious criminal offences; consequently requesting voluntary retention or compulsory retention of communications data relating to the majority of innocent persons is wholly disproportionate. A warrant for such intrusive surveillance should be a minimum requirement.**

3

Question 3 - Do you support the Government's approach to maintaining our capabilities? Which of the solutions should it adopt?

I strongly reject the idea of a centralised communications database. Further, if this constitutes 'maintaining current capability' then I consider the Government is presently acting illegally.

I strongly reject the idea of communication data retention by communication companies for reasons other than suspicion of serious criminal offences, and in that case only with a warrant.

Where persons are suspected of serious criminal offences, I fully support the retention of *all* communication data (because no other method would enable comprehensive identification of the sources and destinations of communications originated or terminated by that user).

Recommendations

1. **The Government should not create a centralised communications database**
2. **Communications data should only be captured from the tiny minority of persons suspected of serious criminal offences; consequently requesting voluntary retention or compulsory retention of communications data relating to the majority of innocent persons is wholly disproportionate. A warrant for such intrusive surveillance should be a minimum requirement.**
3. **Where suspicion of a serious criminal offence arises, the data captured must be comprehensive if the methods and/or content of communication are to be accurately determined and/or decoded.**

Question 4 - Do you believe that the safeguards outlined are sufficient for communications data in the future?

In a word, no. Emphatically not.

It is quite clear that the Interception Commissioners are not effectively regulating the use of interception; no complaint has ever been upheld.

The failure of the Police to enforce the Regulation of Investigatory Powers Act against BT/Phorm (despite the illegal interception of the private communications of 200,000 ordinary people and the businesses that served them) demonstrated that there is no safeguard offered by that act.

The Police were, however, willing to enforce RIPA against Stanford & Liddell, Goodman & Mulcaire, and in Operation Barbatus, suggesting that enforcement is rather selective and heavily dependent on the public profile of the victim.

The failure of the Information Commissioner to apply the Data Protection Act, or the Privacy in Electronic Communications Regulations, and the lack of effective penalties therein illustrates clearly that present safeguards are not adequately enforced, and are utterly ineffective as deterrents.

Recommendations

1. **The safeguards presently outlined are presently ineffective and therefore clearly insufficient protection for communications data now and in the future.**

2. **The robust protection afforded by the Telegraph Act 1864 Section 20 must be reinstated, and suitably updated (this measure was regrettably repealed by Statutory Instrument 2001/1149). A suggested modern update might state;**

> **"Any person having official duties connected with a communication service provider, or acting on behalf of a communication service provider, who shall, contrary to his duty, disclose or in any way make known or intercept**
>
> **I. the contents**
> **II. or any part of the contents**
> **III. or the location or identity of the sender or recipient**
>
> **of any electronic datagram or message intrusted to the communication service provider for the purpose of transmission, shall be guilty of an offence, and shall upon conviction be subject to imprisonment for a term not exceeding twelve calendar months"**