



Home Office

All Party Internet Group public inquiry into the retention of and access to communications data for law enforcement purposes

Note by the Home Office

Communications data provides a valuable investigative tool in the prevention and detection of crime and the protection of the public. For the emergency services, access to communications data can – quite literally – save lives. The Home Office welcomes the opportunity to brief the All Party Internet Group on the issues of access to communications data, preservation of communications data and retention of communications data.

2. Perhaps the most important point to make clear at the outset of this paper is that the issues of access to, and retention and preservation of communications data concern information “about communications” not information “in communications”. It is about routing and packaging, about senders and recipients, about timings and sizes but not about contents.

3. In a phone call, communications data comprises who called who, when and for how long – but not what was said. For an e-mail: who mailed who, when – but not what the message contained, and for a letter or parcel: the addressee and the when and where it was posted – but not what is inside.

How is communications data used for law enforcement purposes?

4. Everyone generates communications data – law-abiding citizens going about their lives and by criminals who use communications technologies to plan, organise and conduct their criminal activities and to seek to evade detection. Just as criminals exploit communications technologies for their purposes, law enforcement agencies and public authorities with law enforcement functions use the traces these technologies generate to help them to prevent and detect crime and to protect the public.

5. Communications data is used, either as intelligence or evidence, in a range of criminal investigations. Examples include using:

- mobile phone location data to help locate a group of kidnappers and their victims, or the location of an illegal drugs store, to trace the movements of a murder victim, or in an emergency to locate a person lost and in distress;
- internet service provider dial-up logs to match dynamically allocated IP addresses with telephone lines and identify locations from which material has been uploaded to the Internet (whether paedophile material, web sites soliciting unauthorised financial services or advertising pirate radio stations, or from which harassing or threatening (stalking) e-mail has been sent);
- itemised telephone call records between brokers and clients to support insider trading charges, between organisers of people smuggling or between dealers and vendors recycling food unfit for human consumption;
- itemised phone records showing whether a person's phone was in use at the time of an accident; and
- subscriber records showing to whom a phone number, a phone line or an e-mail account belongs.

Access to Communications Data

6. The Government acknowledges that public authorities' access to communications data – even undertaken where necessary and proportionate to what is sought to be achieved by obtaining that access to the data – represents an intrusion into privacy. To be justified any such intrusion must satisfy the principles of lawfulness, necessity and proportionality derived from the European Convention on Human Rights.

7. The Government believes that Part I Chapter II of the Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutorily based framework to regulate access to communications data by public authorities with functions to prevent and detect crime and to protect the public. The legislation explains what "communications data" means, sets out statutory purposes for which access to communications data may be necessary and describes the ways in which data may be obtained (by authorisation someone within a public authority or serving a notice upon a service provider). The exercise of the provisions will be overseen by the Interception of Communications Commissioner and there is access to the Investigatory Powers Tribunal for those who believe data about them has been improperly accessed.

8. Within RIPA there is a list of public authorities (police, customs, the National Criminal Intelligence Service, the National Crime Squad, the intelligence agencies and the Inland Revenue) that Parliament has agreed should be public authorities for the purposes of Part I Chapter II. However, as soon as RIPA completed its passage through Parliament, other public authorities indicated their wish to be considered as a relevant public authority within the meaning of RIPA Part I Chapter II.

9. These “other” authorities – like those listed in RIPA – presently access communications data using general information gathering powers, or seek disclosure from service providers under an exemption to the Data Protection Act (DPA). However service providers are increasingly concerned about their ability (or inability) to judge properly the necessity and proportionality of any requests for them to exercise the exemption for disclosure under the DPA. Some public authorities are increasingly concerned that the exercise of general information gathering powers may be argued to be not in compliance with human rights legislation.

10. In June 2002 the Government laid the “Regulation of Investigatory Powers (Communications Data: Additional Public Authorities) Order 2002” before Parliament for affirmative resolution. It listed in very general terms public authorities to be added to the list in RIPA as relevant public authorities for the purpose of accessing communications data. This Order would have been followed shortly afterwards by the “Regulation of Investigatory Powers (Communications Data: Prescription of Offices, Ranks and Positions) Order 2002” that would have explained which officials in executive agencies or with specific functions would be able to authorise access to what communications data for what purposes.

11. In the face of Parliamentary and public concern about the apparent scope of the first Order the Home Secretary withdrew it on 18 June. Consequently the second Order was not laid before Parliament (although the Schedule to the draft second Order was available to Members of Parliament as an attachment to an explanatory memorandum about the first Order). The Home Secretary announced

“I recognise there is widespread concern about the current proposals to regulate how public bodies can access phone and internet records.

“It’s clear that whilst we want to provide greater security, clarity and regulation to activities that already go on, our plans have been understood as having the opposite effect. Bob Ainsworth and I have therefore decided that it makes sense to withdraw the current proposals to allow calmer and lengthy public discussion before we bring forward new plans in this field.”¹

The Government is preparing a consultation paper for publication early in the New Year.

¹<http://www.nds.coi.gov.uk/coi/coipress.nsf/7709c1f0104c752080256bf400338394/c0bde2541eaa9d4280256bf3005afdb0?OpenDocument>

Preservation of Communications Data

12. Preservation of communications data relates to the practicality of identifying (and preserving pending disclosure) of specific communications data that are or may be retained by a service provider for lawful disclosure to a public authority. The provisions within RIPA Part I Chapter II provide for reasonably practicable preservation of data.

Retention of Communications Data

13. The length of time for which service providers retain communication data for their business purposes is gradually decreasing with technological advances and changing business models. For example, itemised billing is largely redundant for subscription-based services and prepaid services. In addition, there are economic and commercial pressures to minimise the cost of data retention across the industry.

14. Part 11 of the Anti-Terrorism, Crime and Security Act (ATCS) provides for retention of communications data based on a voluntary code of practice for the purposes of safeguarding national security or preventing or detecting crime related directly or indirectly to national security. This purpose of retention is narrower than the purposes for which data can be accessed under RIPA.

15. The Office of the Information Commissioner (OIC) has publicly expressed concerns that the ATCS restricts the purposes for which data can be retained but does not address access to that data. The consequences of the difference between the purpose for retention and the purposes for access were clearly explained by Ministers during the passage of the ATCS Bill, when it was indicated that access would not be restricted to retained data.

16. The OIC and Industry are concerned about the apparent disparity between the purpose for data retention under ATCS and the wider purposes for which communications data can be accessed under RIPA and other legislation. The view has been expressed that access to ATCS retained data for a purpose other than one related to national security is arguably unlawful on human rights grounds. However, Parliament concluded that retention of communications data not needed for business purposes is proportionate when national security considerations are at stake and consistent with Article 8(2) of the European Convention on Human Rights. In addition the Government considers that the acquisition of that communications data under RIPA is lawful when such acquisition is necessary and proportionate to what is sought to be achieved by accessing that data.

17. The Government will not proceed with a voluntary code of practice unless it is clear that it is drafted in such a way as to enable service providers who adopt it to comply with data protection and human rights legislation. The Government is continuing to continue to consult the Industry and the OIC on these issues.