

COMMUNICATIONS DATA – HOME OFFICE FACTSHEET

What is communications data?

Communications data is the “who, when and where” of a communication. It can include a mobile telephone number, or an e-mail address or data showing the location of a mobile telephone. It’s important to note that communications data is **not the content** of a communication e.g. what was said in a telephone call or written in an e-mail.

What is it used for?

Communications data plays a critical role in investigating and prosecuting serious crimes such as child sex abuse, kidnap, murder and drug related crime, as well as in public protection – such as locating missing persons. Communications data also prevents terrorist activities – it has for example played a significant role in all major Security Service operations over the last decade. The law enforcement, security and intelligence agencies (as well as the emergency services) all rely heavily on communications data. Without it they could not do their job.

When has it been used?

In the last six months alone, communications data has been key in securing convictions in the Rhys Jones and Hannah Foster murder cases as well as in the suicide terror attack on Glasgow Airport and in the case of Philip Thompson, the ‘librarian’ who ran an international paedophile website.

What happens at the moment?

Communication Service Providers (CSPs) (for example mobile phone operators and Internet Service Providers) keep communications data for business purposes such as billing. Law enforcement, security and intelligence agencies can then access this data when it is necessary and proportionate to do so. It is worth noting that 98% of all applications for access to communications data are made by these agencies.

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA) provides the legal framework for the acquisition of communications data. Communications data can only be accessed if it is necessary and proportionate and required for a specified purpose agreed by Parliament. It must be properly authorised by a senior officer in a public authority designated by Parliament. Restrictions also apply to the purposes for which individual public authorities may acquire communications data and the types of communications data they may acquire.

For example local authorities are not entitled to acquire traffic information – such as location information for a mobile phone.

What is changing?

New and exciting forms of internet based communications such as social networking sites and online multiplayer games are being introduced and adopted by consumers. Nearly 137 billion instant messages were for example sent in the UK in 2007. Whilst in terms of more ‘traditional’ forms of communications there are now more mobile phones than people in the UK with nearly 60 billion text messages sent in 2007 – a 36% increase since 2006. Whilst these new forms of communications undoubtedly bring many benefits, their effect on the way we can use communications data will be profound. If we do not make changes now, the law enforcement, security and intelligence agencies will no longer be able to use this data in the future.

What happens next?

The cross-government Interception Modernisation Programme (led by the Home Office) has been looking at how we can maintain our access to communications data in the face of this rapidly changing technology. The Programme has been working closely with the UK’s law enforcement, security and intelligence agencies to research and identify possible options that will maintain the UK’s communications data capabilities. On 27 April a consultation was launched to invite the public’s views on the need to maintain these capabilities and on possible options for achieving this.

Consultation on communications data

The consultation, *Protecting the Public in a Changing Communications Environment*, began on 27 April 2009 and will run for twelve weeks. It sets out the importance of communications data in protecting the public. It then discusses the emerging problems caused by the advances in new technologies, the impact of any potential capability gaps, and describes possible solutions. Throughout the document the importance of safeguards to protect individuals’ right to privacy is emphasised. The safeguards surrounding communications data are also one of the main topics of the RIPA consultation on Consolidating Orders and Codes of Practice, which commenced on 16 April.

What are the requirements?

The fundamental requirement is for a system which, as far as possible, maintains our crucial communications data capability and, as is currently the case, balances the requirements of security and privacy in a way which commands public confidence. The two major consequences of technological change will need to be addressed. We need to ensure the collection and storage of communications data from services accessed over UK communications networks, but which is not already retained by the service providers for their business purposes. We also need to find a way to overcome the fragmentation of communications data that occurs in the modern world. We need to prevent it taking longer to find and piece together the data needed to identify and build up a picture of a suspect, or to establish the location of a missing person.

What options does the consultation document set out?

The consultation includes a range of options. The Government believes it would be failing in its duty to protect the public if it allowed the capability of public authorities to use communications data to degrade and made no effort to address it. Doing nothing is therefore not an option. A single store of communications data from CSPs would be the most effective technical solution and would go furthest towards maintaining the current capability, however, **a single store will not be pursued due to the privacy implications**. The consultation will therefore set out a range of 'middle way' options based on the model for collecting and retaining data that exists today. These will require CSPs to collect and store communications data and to support the effective acquisition of communications data by public authorities.

Which approach does the Government recommend?

The Government will recommend taking the steps outlined in the middle way options which aim to strike the right balance between privacy and security. These would require legislation to ensure that all data that public authorities need to protect the public is collected and retained by CSPs, and that the retained data is further processed by CSPs to enable specific requests by public authorities to be processed quickly and comprehensively. **This would require additional legislation.** Any legislative provisions brought forward following this consultation will be accompanied by a fully developed and robust Impact Assessment measuring the impact on the public, private and third sectors. The consultation contains no proposals for changing the legislation governing lawful interception.

Safeguards and civil liberties

The Government is clear that it must act in the face of technological changes which would otherwise lead to a reduction in the capability of public authorities to use communications data. We expect our police, security and emergency services to work effectively to keep us safe and to bring criminals to justice. But we also expect our right to privacy to be respected. Whatever option the Government adopts, it will be critical to ensure that the regulatory and oversight arrangements remain effective. The consultation document sets out the current policy and legal safeguards that will remain and the measures that would be required to safeguard the recommended approach to maintaining the communications data capability. The consultation invites a response on the sufficiency of future options for safeguards.

What will the cost of the recommended solution be?

The range of options would offer different levels of benefits to the public authorities, such as the law enforcement and intelligence agencies. Initial estimates of the implementation costs of the range of options discussed above are up to £2bn.

What will the cost to industry be?

As provided for in the Regulation of Investigatory Powers Act 2000, the Government is required to make reasonable contributions to CSPs towards the costs incurred by them in complying with the Act's communications data requirements. The Government is therefore actively seeking the views of industry on the proposals through consultation to help meet Better Regulation commitments to minimise the costs and impact on the private sector.

It is judged that the costs of modernising capabilities are more than justified by the costs of failure to implement. Terrorist incidents have, in the past resulted in huge financial costs to the economy and the Government. The IRA bombs in the London Docklands in 1996 are thought to have cost insurers £170m, while the Manchester bomb later that year led to £411m being paid out in insurance claims. It is also impossible to put a price on the human cost of these or other incidents.