HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 436 May 2013

Monitoring Internet Communications

Internet communications are often monitored to investigate criminal activity. Recent attempts to update UK regulation of investigatory powers have generated controversy. This POSTnote explains the use of different internet monitoring methods and discusses the impact of evolving technologies.

Overview

- Law enforcement agencies often monitor internet communications to investigate crimes.
- The rapid uptake of internet services and evolution of communications technologies present a number of technical and policy challenges for investigators.
- Various methods for avoiding detection online are used for reasons of security and privacy, or to cover up illegal activity.
- Attempts to update UK regulation of internet monitoring are ongoing and have caused controversy.
- Regulating internet monitoring requires balancing rights to privacy with public security and the need for law enforcement.

Background

Internet communications can be monitored in a range of ways for different purposes, including:

- targeted surveillance by law enforcement agencies (LEAs) of people suspected of serious crimes, which could include real-time interception of communications
- requests by LEAs to communications service providers (CSPs) for information about communications when a crime is suspected
- routine monitoring of patterns of internet activity by internet service providers (ISPs) to inform marketing or improve security.

Over the past decade, information about internet communications has been used in 95% of serious organised crime investigations and every major counter terrorist investigation in the UK.[1] This note is primarily concerned with monitoring for law enforcement purposes, so activities carried out by ISPs for business purposes will not be described in detail here.

Communications Service Providers

Surveillance and monitoring of internet communications nearly always requires the cooperation of CSPs. A CSP provides the means to communicate, including by post, telephone and over the internet. This definition includes ISPs such as BT or Virgin Media who provide their customers with the means to connect to the internet. It also includes providers of web-based or software-based communications services such as Gmail, Hotmail and Skype. Unlike ISPs, the latter do not provide the infrastructure for accessing the internet. They provide services for customers which use the network infrastructure already in place, and hence are known as ‘over the top providers’ or ‘third party providers’.

Regulation of Internet Monitoring in the UK

Monitoring of communications in the UK is governed by the 2000 Regulation of Investigatory Powers Act (RIPA) and the 2006 EU Data Retention Directive (EUDRD). RIPA distinguishes between two types of data: ‘communications data’ and ‘content’. Communications data is information about the ‘who, where, how and when’ of communications, but not the actual message being conveyed. For an email, for instance, communications data cover who sent it, when it was sent, where they sent it from, and who received it. They do not cover what is said in the email message. The actual message in the email is the content.

Content interception requires a warrant from the Secretary of State, whereas the acquisition of communications data may be authorised by designated senior figures in a number of named LEAs and other public bodies including intelligence services and the Serious Organised Crime Agency (SOCA). Under RIPA, any requests for data must be demonstrably proportionate and necessary to achieve at least one of nine permitted purposes, which include preventing or detecting

crime, maintaining national security, and protecting public health.

EUDRD requires CSPs to retain communications data for a minimum of six months, up to a maximum of 24 months. It was implemented in the UK in 2009 by a Statutory Instrument that stipulates that CSPs are required to retain communications data for 12 months, but only those generated for business purposes.

Updating Regulation

When RIPA was passed in 2000, the communications landscape was dominated by landline telephones and the postal service. Since then, internet use has increased significantly: the proportion of UK adults who regularly use the internet rose from 27% in 2000 to 82% in 2010.[2] The number of different internet communication methods available has expanded rapidly and communication methods continue to evolve. The popularity of different types of communication services can also rise and fall very quickly. This continuing evolution has had significant consequences for internet monitoring and its regulation.

In light of these changes in technology, various governments have considered how investigative capabilities can be maintained. In 2009, the Labour Government consulted on the Interception Modernisation Programme. In 2010 the coalition Government launched the Communications Capabilities Development programme to give the Home Office "the ability to continue to protect the public in the future".[3] In June 2012, the Home Office published the Draft Communications Data Bill.

The key proposed changes in the Draft Bill were:

- CSPs would be required to generate any 'necessary' communications data required by the authorities named in the Bill, in addition to what they already generate for business purposes
- where LEAs cannot obtain it directly, CSPs could be required to provide any data from third party providers that cross their networks
- CSPs would be mandated to retain communications data for a minimum of 12 months
- provision for combining databases of communications data to allow them to be filtered and searched by designated authorities.

The Draft Bill caused some controversy and was referred to the Intelligence and Security Committee and a Joint Committee of the House of Lords and House of Commons for pre-legislative scrutiny. While both committees agreed that there was a need to update legislation, their reports raised concerns over many of the proposals. The Home Office announced that it would introduce a revised bill "at the earliest possible opportunity".[4] In April 2013, the Deputy Prime Minister announced his opposition to some of the key measures in the Draft Bill, while recognising that LEAs must keep up with the challenge of policing in the internet age. The Queen's Speech in May 2013 did not include the Communications Data Bill, but referred to bringing forward proposals to enable "the investigation of crime in cyberspace."

Internet Protocol and Monitoring Methods

Internet Protocol

Communication over the internet can take a variety of forms, including email, social media (such as Facebook) and internet telephony (VOIP) services such as Skype. All of the information sent over the internet is sent using internet protocol (IP): a set of global standard operating procedures. Data crossing the network is often referred to as 'traffic'. Information sent using IP is split into chunks known as 'packets', which travel across the network independently and are reassembled at their destination. Each packet contains a 'payload': the chunk of information being transported. It also has a 'header' which tells the network where to deliver the packet, and how to reconstruct the complete sequence at its destination.

Monitoring Methods

Internet Protocol Address Matching

When a person accesses the internet, they are assigned an internet protocol address (IP address) by their ISP (Box 1). An IP address enables someone to send and receive data, similar to a postal address allowing letters to be sent to a house. IP addresses can be shared between people, or can (in rare cases) be unique. ISPs sometimes keep records of which customer is using which IP address at any given time but in many cases not for very long, particularly as in most cases a customer is allocated a different IP address each time they connect. If IP address data have been retained, LEAs may request these details to find out who is associated with a particular communication.

Some website owners keep records of which IP addresses have visited the website and at what time, which may be requested by LEAs. Under RIPA, the portion of the web address up until the first forward slash is considered communications data while anything after is content. For example, if someone visits 'www.parliament.uk/POST', knowledge of the full address is content, while knowledge that they visited 'www.parliament.uk/...' is communications data.

If the data are available, it may be possible to find out the name and address of a subscriber associated with a particular IP address, allowing LEAs to physically locate the person. The 2013 Queen's Speech referred specifically to "the problem of matching internet protocol addresses" to users, with an associated brief from the Home Office stating that "the Government is looking at ways of addressing this issue with CSPs. It may involve legislation."[5]

Email and VOIP Data

CSPs may be asked to provide communications data for emails and internet telephone calls. These show who the sender and recipient were, and the time the email or call was sent and received.

Box 1. IP Address Allocation
A finite number of IP addresses are available. The global Internet Assigned Numbers Authority allocates large blocks of IP addresses to Regional Internet Registries, which in turn give blocks of IP addresses to ISPs to allocate to their customers.

IPv4 and IP Address Exhaustion
Under the most commonly used version of IP, known as IPv4, all IP addresses have 32 bits. With increasing demand for IP addresses, the remaining pool of unallocated IP addresses is nearly exhausted. One way to combat this problem is to allow multiple devices to share one IP address, using a process known as Network Address Translation (NAT). The use of NAT has implications for communications monitoring as IP addresses cannot easily be traced to a single device. This is a particular issue for mobile telecommunications, where it is common for hundreds of mobile phones to share one IP address.

IPv6
A newer version of IP known as IPv6 has been developed under which IP addresses have 128 bits, increasing the number available by a factor of a decillion (ten million billion trillion, or 10^{28}) compared with IPv4. This removes the need for NAT and would make IP address matching easier. Switching to IPv6 requires equipment upgrades, so the transition to the new protocol has been slow. Although IPv6 was introduced in 1998, by June 2012 IPv6 accounted for less than 0.21% of global internet traffic.[6]

Deep Packet Inspection
'Opening up' data packets travelling across a network to look at the payloads rather than just the headers is known as deep packet inspection (DPI). DPI may be used by ISPs to ensure quality of service, and by LEAs to intercept the content of communications when authorised by a warrant from the Secretary of State (Box 2). DPI is usually carried out by placing equipment known as 'probes' or 'black boxes' into the network to scan all the traffic passing through them. They can either re-route traffic, or copy and store data before passing the packets on to their intended destination.

Technical Challenges

Evasion of Monitoring

There are several ways in which internet users can make monitoring and surveillance more difficult. These evasion methods are not illegal, and many are an essential part of modern cyber security practice (see POSTnote 389). However, they can be exploited by criminals in attempts to cover up illegal activity or avoid detection. It is not known how effective they are at frustrating law enforcement activity, as this information is classified.

Encryption
Data sent over the internet can be encrypted (encoded) to keep its meaning secret from observers (see POSTnote 270). The recipient uses a 'key' to decrypt the data. Most modern encryption uses very complex algorithms and is virtually impossible to crack. Encryption is routinely used by CSPs and applications such as internet shopping and banking. Additionally, people with sufficient technical knowledge may use their own encryption systems before the data is further encrypted by the CSP. Under RIPA, a suspect can be legally compelled to disclose a decryption key to the police or investigating authority.

Virtual Private Networks
A virtual private network (VPN) extends a private network across the internet, typically by requiring password authentication and sending traffic through an encrypted 'tunnel'. VPNs can make it appear as if a user is accessing the internet from somewhere other than their actual location. VPNs may be commercially supplied or set up by individuals. Some commercial VPN providers hold subscriber payment details and web activity logs, which may be provided to UK LEAs if the provider is within their jurisdiction or voluntarily complies with requests.

Onion Routing
Onion routing is so named because data packets sent using this method have multiple layers of encryption. The packets are sent on an unpredictable path via multiple network nodes, each of which decrypts one layer. The packet details, including their origin and destination, remain hidden from the intermediaries, so it is very difficult to determine the sender and recipient. Weaknesses do exist however, with 'entry' and 'exit' nodes particularly vulnerable to monitoring.

Alternative Communication Methods
Unregistered 'Pay As You Go' mobile phones, internet cafés and public unencrypted internet access points can be used in attempts to provide anonymity. In these cases, alternative surveillance methods such as video cameras are likely to be needed to identify the user.

Data Security

The Draft Bill called for retention of communications data in databases. Concerns have been raised that there is a risk of these data being accessed by people with malicious intent through hacking or due to human error.[7] The Home Secretary has pointed out however that ISPs routinely collect similar data and are specialised in protecting it.[8]

Maintaining Capabilities

Maintaining investigatory capabilities at the level required by the Draft Bill, while technically possible, could be costly and

Box 2. Uses of Deep Packet Inspection
DPI is used in different ways by ISPs and LEAs.

ISPs
- Security: DPI can be used to detect and prevent spam and malicious attacks on networks and services.
- Traffic regulation: some ISPs use DPI to prioritise certain types of internet traffic to run a smooth service. For example, VOIP and video streaming require a fast uninterrupted flow of data, and may be prioritised over email, where a small delay causes less disruption.

LEAs
- Content interception: DPI can be used to intercept the content of communications by revealing packet payloads.
- Third party data: one of the proposed provisions in the Draft Bill was to ask ISPs to use DPI to capture third party communications data which crosses their networks if it could not be obtained directly from third party providers. The capability to do this on a large scale does not currently exist, hence it would likely be used for targeted surveillance only.

resource intensive. For example, on the issue of using DPI to provide third party information, the ISP Association is "yet to be convinced that current [DPI equipment] can handle the volume of traffic that moves across service provider networks".[9] Retaining larger amounts of data will incur costs to CSPs. The Draft Bill stated that CSPs would be given "appropriate contributions" from the Home Office to reimburse them. In evidence to the Joint Committee, several CSP representatives stated that at present under RIPA these contributions are nearly always 100%, but would have liked this to be stipulated in the Draft Bill. The Committee expressed concern that innovation in the internet sector could be stifled by the extra time and effort spent on compliance, even if financial costs are recouped.

Volume of Data

Building a complete picture of one person's communications requires multiple communications channels and devices to be monitored. The volume of data available is therefore very large, requiring significant resources to process and store it. The resources required are likely to increase, as the growth of 'smart technology' sees increasing numbers of devices connect to each other and the internet (see POSTnote 423). Conversely since per minute internet billing is now much less common and many connections are 'always on', data on periods of usage are now often not available – hence the requirement in the Draft Bill for additional data generation. LEAs have stated that they are now missing significant chunks of information, partly due to these changes in technology.[10] However, some privacy groups argue that the increase in the overall volume of communications means that LEAs now have access to more and richer information than before.[11]

Communications Protocols

Different internet communication services use different sets of operating procedures, known as communications protocols. Knowledge of each of these protocols would be required for monitoring equipment to separate the communications data from the content, and the filtering software must be updated every time a protocol is introduced or modified. Protocols change frequently as methods and services for communication proliferate, which can make keeping 'black boxes' up to date difficult and costly. As a result, some stakeholders consider that a communications 'arms race' is developing between LEAs and criminals.

Regulatory Challenges

Privacy

Regulating monitoring of internet communications requires a balance to be struck between citizens' right to privacy and law enforcement. Concerns that the proposals in the Draft Bill would disproportionately impinge on privacy were raised by organisations including NGOs such as Big Brother Watch and Open Rights Group,[12] and trade organisations including the London Internet Exchange and the ISP Association.

The Draft Bill included a provision for retained data to be filtered by running search queries, to facilitate enquiries using data from multiple sources. The Joint Committee's report pointed out that this tool could be used for profiling, although queries of this nature would be subject to an enhanced authorisation process similar to that for communications data requests under RIPA. The Committee also noted however that the filter could minimise "collateral intrusion" by allowing more targeted requests.[13]

Overseas CSPs

Many CSPs, including Hotmail, Twitter and Facebook, provide services in the UK, but are owned by foreign companies and store all their data outside the UK. This means that they are not under UK jurisdiction. In practice, the majority of overseas CSPs currently comply with requests for information on a voluntary basis, while retaining the right to refuse. Requests for information from another country may also be made via a Mutual Legal Assistance Treaty if one exists between the two countries. This introduces a time delay however as the request must go through diplomatic channels.

Separating Communications Data from Content

For telephone calls and emails, the distinction between communications data and content is clear. However, for other forms of communication it can be harder to draw the line. For example, operators of online games or 'virtual worlds' such as Second Life have expressed confusion over how the definitions apply to them.[14] The distinction between communications data and content acknowledges that interception of the latter is considered more intrusive. However, communications data can be just as revealing in some cases. For example, knowledge that someone has visited 'www.debthelp.co.uk' allows inferences to be made.

Future Technologies

Future changes in internet and computing technology could make some current monitoring or evasion methods obsolete. The Home Office attempted to deal with this issue by including provisions in the Draft Bill whereby the Secretary of State can order CSPs to retain any categories of data in addition to those currently available. While the Joint Committee recognised that the Home Office was likely to require retention of other data types in future, it recommended that these additional powers be subject to Parliamentary scrutiny before becoming law.

Endnotes

1 HM Government, 2010. *The Strategic Defence and Security Review*
2 International Telecommunication Union 2013
3 Gov.uk, updated 26th March 2013. *Protecting the UK Against Terrorism:* http://bit.ly/12eX0Dn
4 James Brokenshire MP, HC Deb, 27 February 2013, c482W
5 The Queen's Speech 2013, Background Briefing Notes
6 Scott Iekel-Johnson, 2012. *World IPv6 Launch: Taking a longer view:* http://bit.ly/16nEmWJ
7 Joint Committee on the Draft Communications Data Bill, Oral Evidence p205
8 Ibid p406
9 Joint Committee on the Draft Communications Data Bill, Report p32
10 Joint Committee on Draft Communications Data Bill, Written Evidence p234
11 Ibid, p77 and Oral Evidence p37-39
12 Open Rights Group, 2013. *Digital Surveillance*: http://bit.ly/16alH4U
13 Joint Committee on the Draft Communications Data Bill, Report p37
14 Joint Committee on the Draft Communications Data Bill, Oral Evidence p132

POST is an office of both Houses of Parliament, charged with providing independent and balanced analysis of policy issues that have a basis in science and technology. POST is grateful to Hannah James for researching this briefing, to EPSRC for funding her parliamentary fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Martin Griffiths.