

Co-funded by the Prevention of and Fight against Crime Programme of the European Union

*Towards a Polish Cybercrime Centre of Excellence*

**Comparative Research Project – Country Report United Kingdom**

**Dr Subhajit Basu**

**University of Leeds**

1. *How providers of publicly available telecommunication technologies are classified in the legal System of your country? (UK)*
2. What are the regulations concerning data retention by IAPs (i.e. providers of publicly available electronic communications services or of public communications networks) and ISPs (i.e. providers of information society services)?
3. Are there traffic data related to technologies such as Facebook, blogs or other information society services covered by your (UK) national legislation?
4. What data are kept by ISP, IAP?
5. What are the legal regulations enabling law enforcement and judicial authorities to obtain data from IAP, ISP with particular reference to social networking sites?
6. What are the legal requirements for an access of traffic data, stored content (e.g. e-­‐mail message) and subscriber’s data by LE/judicial authorities from ISPs?
7. Are there any laws, policies or arrangements for the remuneration of costs incurred by ISPs when providing LEAs with requested data?
8. What are the legal regulations concerning taking down and blocking illegal content on the Internet before start of criminal proceedings and during criminal proceedings (powers of law enforcement and powers and obligation of service providers), what problems of taking down and blocking could be indicated?
9. Were there any research projects concerning cooperation between LEA and ISP/IAP in fighting cybercrime in your (UK) country? If yes, please specify and shortly describe the results. What are the main problems of cooperation?
10. What problems of cooperation between LE / judicial authorities with ISP/IAP can be indicated on the base of judicial decisions/judgments?
11. What is the effectiveness of investigation and prosecution of illegal content crimes and child abuse on the internet in your country according to available statistical data and research?
12. Is there any new legislation prepared or proposed concerning the above mentioned issues? If so, please indicate what the intended changes are and what reasons for them?
13. **How providers of publicly available telecommunication technologies are classified in the legal System of your country? (UK)**

The Communications Act chapter 21 2003 creates the regulatory framework electronic communications. It recognises two types of electronic communication providers; providers of electronic communications networks (PERNs) and providers of electronic communication services (PECSs). Electronic communications network (ECN) is defined as a transmission system for the conveyance of signals by electrical, magnetic or electro-magnetic energy. ECN include networks used to carry broadband internet traffic and to provide end users with internet access.[[1]](#footnote-1) An electronic communication service (ECS) is a service which has as its principal feature, the conveyance of messages by means of electronic communications network excluding content services.[[2]](#footnote-2) ESC involves the conveyance of signals and includes internet access services provided by ISPs.[[3]](#footnote-3) A content service is any service which consists of (a) the provision of material with a view to its being comprised in signals conveyed by means of an electronic communications network; and/or (b) the exercise of editorial control over the contents of signals conveyed by means of such a network.[[4]](#footnote-4)

Under the law, public electronic communications network” means an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public. Public electronic communications service” means any electronic communications service that is provided so as to be available for use by members of the public.[[5]](#footnote-5)

The General Conditions of Entitlement made pursuant to section 48(1) of the Communications Act set out the conditions and obligations of communication providers.[[6]](#footnote-6) For the purpose of determining the applicable conditions and imposing obligations on service providers, the Conditions distinguish between three main types of network or service providers. These are;

1. Providers of Electronic Communications service or networks
2. Providers of Public Electronic Communications Services or Networks
3. Providers of Publicly Available Telephone Services or Public Telephone networks

Providers of Electronic Communications service or networks broadly applies to providers of all communication services and includes public or private networks, mobile and fixed networks, voice telephony and data and the internet. It also includes own-network providers and resellers but excludes providers of terminal equipment such as phones.

The General conditions define Public Communications Network as an Electronic Communications Network used wholly or mainly for the provision of Public Electronic Communications Services which support the transfer of information between Network Termination Points. Public electronic communications services or networks is a narrower group of communication providers who provide services or networks available to members of the public. They therefore exclude private networks and services run on private networks and other services not offered to the general public.

Publicly available telephone service means a service made available to the public for originating and receiving, directly or indirectly, national or international calls through the use of numbers in the national or international telephone plans. The service therefore covers only providers of network or services which enable members of the public to make and receive public switched telephone network (PSTN) phone calls. It includes providers of indirect access and resellers of PSTN services.

The Regulation of Investigatory Powers (RIPA) uses the terms telecommunications systems and telecommunications services The law defines “telecommunications service” as any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and “telecommunication system” as any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. “Public telecommunication system” under the RIPA means any part of a telecommunication system located in the United Kingdom by means of which any public telecommunications service is provided. Public telecommunications service” means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom.[[7]](#footnote-7)

It is important to note that both the Communications Act and the RIPA use general terms such as ECS, ECN or public telecommunications systems or services and omitted to specify in details or give examples of the services or networks. However, the General Conditions of Entitlement give some indications of networks or services which may fall into different categories.

1. **What are the regulations concerning data retention by IAPs (i.e. providers of publicly available electronic communications services or of public communications networks) and ISPs (i.e. providers of information society services)?**

The following laws regulate data retention in the UK.

* The Electronic Communications Data Retention (EC Directive) Regulations (the Data Retention Regulations) 2009.
* The Data Retention Data Retention and Investigatory Powers Act (DRIPA) c.27 2014
* The Regulation of Investigatory Powers Act (RIPA) 2000
* The Data protection Act 1998

**Mandatory data retention under the Data Retention Act 2009**

The Data retention Act implemented the EU Directive 2006/24/EC on Data Retention.[[8]](#footnote-8) The Regulations 2009 require public communications providers to retain communication data specified in the law for a period of 12 months from the date of the communication in question.[[9]](#footnote-9) “Public communications provider” means—

(i) a provider of a public electronic communications network, or

(ii) a provider of a public electronic communications service.[[10]](#footnote-10)

“Public electronic communications network” and “public electronic communications service” have the meanings assigned in section 151 of the Communications Act 2003.[[11]](#footnote-11)

As providers of public communications services, the law requires ISPs to retain data including the details of internet telephony and emails as well as traffic and location data.[[12]](#footnote-12) The content of communication is exempted.[[13]](#footnote-13) Appropriate technical and organisational safeguard measures must be applied to retained data to ensure they are accessed by specially authorised persons only. Data retained in accordance with law must also be destroyed at the end of the retention period.[[14]](#footnote-14)

It is important to state that the EU Directive 2006/24/EC on Data Retention which the UK Data Retention Regulations implement has been declared invalid by the Court of Justice of the European Union (CJEU) for disproportionately infringing on the individual privacy rights of EU citizens.[[15]](#footnote-15) As a result of the invalidation, the DRIPA 2014 was passed to replace the UK Regulations.

**Data Retention Notices under the DRIPA 2014 and RIPA 2000**

DRIPA was a fast-tracked legislation passed in 2014. Government argued that it was an emergency legislation needed to ensure that law enforcement and intelligence agencies could maintain their ability to access telecommunication data needed to investigate criminal activities and protect the public.[[16]](#footnote-16) Section 1 of the DRIPA empowers the Secretary of state to issue a retention notice requiring a public telecommunications operator to retain relevant communication data if the Secretary of state considers the requirement necessary and proportionate for one of the purposes falling within paragraphs (a) to (h) of section 22(2) of the RIPA. Communication data has the meaning assigned under section 21(4) of the RIPA and includes traffic data, use data and subscriber data. The content of the communication is excluded. [[17]](#footnote-17)

The circumstances under which a retention notice is deemed necessary as stated in section 22(2) RIPA are, if in the interests of national security, for the purpose *“in circumstances appearing to the Secretary of State to be relevant to the interests of national security”[[18]](#footnote-18)* for preventing or detecting crime or of preventing disorder, or if it is in the interests of the economic well-being of the United Kingdom, *“so far as those interests are also relevant to the interests of national security”*[[19]](#footnote-19) Other grounds for issuing the notice are if it is the interests of public safety; for the purpose of protecting public health, for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, for the purpose, in an emergency, of preventing death or injury or of mitigating any injury or damage to a person’s physical or mental health. The Secretary of State may also by an order issue a notice for any other purpose not covered by the provisions of the law.[[20]](#footnote-20)

Although the laws on data retention make no specific reference to ISPs, or providers of information society services (ISS), the DRIPA applies generally to public telecommunications operator defined as a person who-

1. Controls or provides a public telecommunication system, or
2. Provides a public telecommunications services;[[21]](#footnote-21)

Public telecommunications systems and services have the meanings given by section 2(1) of the RIPA and covers ISS as defined by art 2(a) of the EU Directive 2000/31/EC.[[22]](#footnote-22)

**Retention of personal data under Data Protection Act 1998**

Retention of personal data is regulated by the Data Protection Act (DPA) 1998. The Act provides that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.[[23]](#footnote-23) In effect, the Act did not also set out specific minimum or maximum periods for retention of personal data. However, further guidance on retention of personal data is provided by the Information Commissioner’s Office (ICO).[[24]](#footnote-24) According to the ICO, considerations which may affect the length of personal data retention include current and future value of the information, the costs, risks and liabilities associated with retaining the information, and the ease or difficulty of making sure the information remains accurate and up to date. The appropriate retention period will therefore depend on what the information is used for, the surrounding circumstances, any legal or regulatory requirements to retain the data and agreed practices in the relevant industry.[[25]](#footnote-25)

1. **Are there traffic data related to technologies such as Facebook, blogs or other information society services covered by your (UK) national legislation?**

**Traffic data generally**

The Regulation of Investigatory Powers Act (RIPA) 2000 defines certain communication as traffic data. Traffic data is data comprised in or attached to a communication for the purpose of transmitting the communication and which in relation to any communication;

* Identifies or appears to identify a person, equipment, or the location to and from which the communication is transmitted,
* Identifies or selects or appears to identify or select the equipment by means of which the communication is transmitted,
* Comprises signals that activate whether wholly or partially, the equipment used for the transmission of any communication.
* Identifies data as data comprised in or attached to a communication.[[26]](#footnote-26)

Traffic data therefore includes information relating to the time, method and the device or equipment used in the process of communication. It also includes subscriber information such as names, addresses and direct debit details of subscribers. Service use information such as itemised records of calls and internet connection are classified as traffic data. [[27]](#footnote-27) Traffic data however excludes the content of the communication.[[28]](#footnote-28)

The RIPA contains general categories of traffic data without associating them with specific technologies. However, web-browsing information such as host machines, servers, domain name, and IP addresses which may be traffic data associated with Facebook and other social networking services, would be covered by section 21(6) of the RIPA.

**4. *What data are kept by ISP, IAP?***

It is difficult to know precisely what data ISP keep. However, as a matter of industry practice, service providers retain large quantities of communication data for internal business reasons. For example, they keep records of telephone numbers to allow itemised billing, they hold names, addresses and bank details in order to bill customers, and they monitor and retain information about traffic passing across their networks to help improve the services they offer. Service providers may also enter into agreements with governments to retain certain types of data. [[29]](#footnote-29)

Apart from voluntary retention regimes, laws may also require mandatory data retention. The legal frameworks for data retention under UK laws have been discussed above.

1. **What are the legal regulations enabling law enforcement and judicial authorities to obtain data from IAP, ISP with particular reference to social networking sites?**

The principal legislation relating to lawful acquisition or obtaining of data by law enforcement authorities in the UK is the Regulation of Investigatory Powers Act (RIPA) 2000. Section 1 of the RIPA provides that it is generally unlawful to obtain to or intercept communication in the UK.[[30]](#footnote-30)However, the RIPA also provides for circumstances under which, and the procedure to be followed, to obtain communication data from providers of public telecommunication services. Such communication may be intercepted or obtained through interception warrants issued under the hand of the secretary of State or by imposition of obligations notice also issued by the secretary of State.

**Interception of communication with warrants**

Section 5 of the RIPA empowers the Secretary of State to issue warrants to law enforcement or intelligence agencies which they may serve on providers of public telecommunications services.[[31]](#footnote-31) A warrant may only be issued if the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct and if it is necessary on grounds specified in the law. A warrant is justified if it is issued in the following circumstances;

* in the interests of national security
* for the purpose of preventing or detecting serious crime
* for the purpose of safeguarding the economic well-being of the United Kingdom
* for the purpose of giving effect to the provisions of any international mutual assistance agreement in circumstances which appears to the Secretary of State to justify the issue of a warrant for the purpose of preventing or detecting crime in the UK.[[32]](#footnote-32)

An interception warrant shall only be issued under the hand of the Secretary of State or under the hand of a qualifying senior official if the case falls under section 7(2) of the RIPA.[[33]](#footnote-33) Warrants may also be issued on an application by, or on behalf of persons specified in section 6(1) RIPA. The warrant must name or describe either one person or a set of premises to which it relates, and must describe the communications required to be intercepted.[[34]](#footnote-34) When served with an interception warrant, it is the duty of a provider of a public telecommunications service to take all reasonably practicable steps for giving effect to the warrant.[[35]](#footnote-35) Failure to comply with the duty is an offence punishable with imprisonment or a fine.[[36]](#footnote-36)

**Imposition of obligations notice**

Section 12 of the RIPA empowers the Secretary of State to impose obligations on public telecommunication services to ensure they are and remain able to provide interception capability in order to give effect to interception warrants. The obligations may be imposed on providers of public postal services or public telecommunications services or those who are proposing to do so.[[37]](#footnote-37)

In the exercise of his powers, the Secretary of State issues a notice requiring the person who is to be subject to the obligations to take all such steps as may be specified or described in the notice. The steps specified must be necessary and the service provider must have the practical capacity to comply.[[38]](#footnote-38) Failure to comply with the obligations is a breach of statutory duty and may be enforced by civil proceedings by the Secretary of State for an injunction or for specific performance of a statutory duty.[[39]](#footnote-39)

Exempted providers are those whose services are limited to not more 10,000 persons or those who provide, or propose to provide, a public telecommunications service in relation to the provision of banking, insurance, investment or other financial services[[40]](#footnote-40) Again, the RIPA did not specify particular technologies but applies to all providers of public telecommunication services generally. Nevertheless, it appears debatable whether there is need for RIPA authorisations to obtain access to social networking sites. Commenting on the use of such sites for investigations and intelligence, the UK Chief Surveillance Commissioner noted as follows;

This [social network] is now a deeply embedded means of communication between people and one that public authorities can exploit for investigative purposes. I am reasonably satisfied that there is now a heightened awareness of the use of the tactic and the advisable authorisations under RIPA that should be considered. Although there remains a significant debate as to how anything made publicly available in this medium can be considered private….[[41]](#footnote-41)

1. **What are the legal requirements for an access of traffic data, stored content (e.g. e-mail message) and subscriber’s data by LE/judicial authorities from ISPs?**

 **Traffic data and subscriber data**

Traffic and subscriber data are forms of communication data under the RIPA.[[42]](#footnote-42) Part I of chapter II of the RIPA contains provisions regulating access to communication data as follows;

*Grant of Authorization and Issue of Notice*

Section 22 RIPA enables designated individuals to grant authorisation or issue notices for access to communication data held by providers of public telecommunication services including ISPs.[[43]](#footnote-43) Designated persons for the purpose of the grant of authorisation or notice are individuals holding offices, ranks or positions with relevant public authorities and prescribed as designated persons by an order made by the Secretary of state.[[44]](#footnote-44)

Authorisation is granted if the designated person believes that method of obtaining the data is proportionate to what is sought to be achieved by obtaining the data.[[45]](#footnote-45) In particular, authorisation is granted only if it is necessary for purposes stated in the RIPA. That is, it is in the interest of national security, for preventing or detecting crime, the protection of the economic well-being of the United Kingdom and it is in the interests of public safety. Other grounds for granting authorisation include on grounds of protecting public health, assessing or collecting any tax, and in an emergency, as well as for preventing death or injury.[[46]](#footnote-46)

A designated person may also issue a notice to a telecommunications operator requiring him to disclose certain communication data in his possession or if it is not in his possession, to obtain such data. Compliance with the notice by the operator is a statutory duty and may be enforced by an order of injunction or specific performance.[[47]](#footnote-47)

Sections 23 and 24 of the RIPA set out the procedure to be followed for grant of authorisation or issue of notices. The sections provide that the authorisation or notice must be in writing or in manner that produces evidence that authorisation is granted or the notice is given. They must describe the conduct and communication data to which the authorisation or notice relates. They must specify the matters under section 22(2) (the interest of national security etc.) by reference to which an authorisation is granted or a notice given. They must also specify the rank or position of the person granting the authorisation or giving the notice.

**Content data**

Although content is excluded from communication data under UK law, content data is not itself defined. This could raise practical difficulties. According to a report issued by the Intelligence and Security Committee, changes in technology have blurred the clear distinctions between data and content particularly in the context of the internet. The Report concluded that it is difficult to reach “…a definitive conclusion as to which elements of internet communications and traffic should be deemed to be data and which parts content.”[[48]](#footnote-48)

Nevertheless, access to content is also regulated by part I of chapter I of the RIPA. Under the provisions of section 5 of the RIPA, access to content data may be obtained by an interception warrant issued under the hand of the Secretary of State*.*

1. **Are there any laws, policies or arrangements for the remuneration of costs incurred by ISPs when providing LEAs with requested data?**

ISPs and other providers of telecommunication services are entitled to fair contributions towards the cost of providing access to or obtaining data by law enforcement in the UK. Under section 14 RIPA, the Secretary of State has a duty to ensure that providers of telecommunication services receive fair contributions towards the costs incurred or likely to be incurred in consequence of an interception warrant or an order imposing obligations under section 12 of the RIPA. The Secretary of State must ensure that arrangements for such payments are in force and may comply with the provisions by making arrangements for payment to be made out of the money provided by parliament.[[49]](#footnote-49)

1. **What are the legal regulations concerning taking down and blocking illegal content on the Internet before start of criminal proceedings and during criminal proceedings (powers of law enforcement and powers and obligation of service providers), what problems of taking down and blocking could be indicated?**

**Illegal content generally**

The following contents are illegal under UK laws:

* Child sexual abuse images including non-photographic and pseudo- prohibited by the Protection of Children Act (POCA) 1978 as amended by the Criminal Justice and Public Order Act 1994, the Criminal Justice and Immigration Act 2008 and the Coroners and Justice Act 2009
* obscene and hateful speech and extreme pornographic images – prohibited by the Obscene Publications Act 1959 and Criminal Justice and Immigration Act 2008
* Content infringing copyright – regulated by the Copyright, Design and Patent Act 1998 and the Digital Economy Act 2010
* Some adult pornography - the Audiovisual Media Services Regulations 2014 prohibits video works in respect of which the British Board of Film Classification (BBFC) has or would have refused to issue a classification certificate. It also places restrictions on certain adult pornographic content produced or sold in the UK.
* Content which encourages or incites terrorist acts – prohibited by Terrorism Act 2006

Legal regulations for blocking or taking down illegal content are as follows;

1. *Filtering of illegal Content – child sexual abuse content*

Blocking access to child sexual abuse images is carried out through a notice and takedown system operated by the Internet Watch Forum (IWF). The IWF is a self-regulatory body established in 1996 and is funded by the EU and the online industry including ISPs. It serves as a hotline for the public to report offending pornographic content and operates a notice and takedown system in collaboration with ISPs to swiftly block access to child sexual abuse content in the UK. The IWF shares intelligence with law enforcement which may then take further action including investigations and prosecution.[[50]](#footnote-50)

1. *Blocking by Law enforcement- terrorist related content*

Section 3 of the Terrorism Act 2006 gives law enforcement the power to demand, the removal from public availability content deemed to be inciting or encouraging terrorism. The law requires a law enforcement officer to serve a notice on the service provider declaring that in his opinion, the relevant content is unlawfully terrorist-related. If the content is not removed within two working days without reasonable excuse, the service provider is deemed to have endorsed the content and senior officers of the organisation may be liable to criminal prosecution.

*(c) Court ordered blocking - Content infringing intellectual property rights*

1. The Copyright, Design and Patent Act 1998

Section 97A of the Copyright, Design and Patent Act 1998 empowers the courts to grant an injunction against service providers with respect to website content infringing copyright. Section 97(A) implements Article 8(3) of European Parliament and Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (“the Information Society Directive”). It provides, **E+W+S+N.I.**

“The High Court (in Scotland, the Court of Session) shall have power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright.”[[51]](#footnote-51)

The main condition for grant of injunction is that the service provider must have actual knowledge of the fact of the infringement. In determining whether the provider has actual knowledge, the court is required to take into account certain relevant matters. These includes whether the service provider has received a notice through a means of contact made available in accordance with section 6(1)(c) of the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013).[[52]](#footnote-52) Section 6(1) of the E-commerce Regulations requires service providers to make available to the recipient of the service and any relevant enforcement authority, the details of the service provider, including his electronic mail address, to make it possible to contact him rapidly and communicate with him in a direct and effective manner.

The court must also take into account the extent to which any notice includes—

(i)the full name and address of the sender of the notice;

(ii)details of the infringement in question.[[53]](#footnote-53)

The above provisions have been applied in a number of cases to make orders requiring ISPs to block, or at least impede access to websites containing content which infringes copyright.[[54]](#footnote-54) Although, the remedy of injunction in section 97(A) is limited to copyright infringement, the courts have also extended its provisions to cover cases where content infringes registered trademarks.[[55]](#footnote-55)

1. The Digital Economy Act 2010

Sections 17 and 18 of the Digital Economy Act (DEA) 2010 enables the Secretary of State to make regulations to empower courts to grant injunction which requires ISPs and other service providers to block access to a website involved in infringing copyright. Under section 17 of the DEA, the courts may grant a “blocking injunction” in respect of locations on the internet used for or in connection with activity that infringes copyright. Blocking injunction “means an injunction that requires a service provider to prevent its service being used to gain access to the location.”[[56]](#footnote-56)

The regulations may be made subject to the Secretary of State being satisfied that the infringing copyright activity has serious adverse effects on businesses or consumers, that the regulations is a proportionate way to address that effect and that making the regulations will not prejudice national security and the detection of crimes.[[57]](#footnote-57) The Act contains further provisions relating to the conditions for the grant of injunction by the courts including the factors which the court must take into account in granting the injunction.[[58]](#footnote-58)

It is important to note that after the provisions of section 17 and 18 DEA has been the subject of judicial review and review by the Ofcom,[[59]](#footnote-59) the government announced on 3 August 2011 that it did not intend to bring the provisions into force.

**Problems implicated by site blocking**

Problems implicated by site blocking include;

1. Over-blocking – this relates to where blocking technologies employed also block access to legal content or legal websites.[[60]](#footnote-60)
2. Cost- costs of implementing the blocking orders as well as associated costs of over-blocking and costs of legal challenge which may arise from such over-blocking raise the costs for ISPs.
3. Censorship- Site blocking could have adverse effects on privacy and freedom of speech and lead to allegations of censorship.
4. Ineffectiveness of blocking technologies – Blocking technologies can be circumvented by site operators and users. For example, operators who may change the location of the infringing website.[[61]](#footnote-61)
5. Due process in court ordered blocking – Injunctions are largely pre-emptive orders and this may raise concerns about due process.

9. **Were there any research projects concerning cooperation between LEA and ISP/IAP in fighting cybercrime in your (UK) country? If yes, please specify and shortly describe the results. What are the main problems of cooperation?**

 No research project in this area was identified. However, commentaries from stakeholders suggest that the main areas of cooperation include intelligence sharing between law enforcement and ISPs, provision and facilitation of training programs for law enforcement officers by ISPs and funding of cybersecurity through the national cybersecurity program.[[62]](#footnote-62)

10. **What problems of cooperation between LE / judicial authorities with ISP/IAP can be indicated on the base of judicial decisions/judgments?**

The cases decided under section 97(A) of the Copyright, Design and Patent Act 1998 highlight some of the problems which may arise as a result of cooperation between law enforcement/judicial authorities and ISPs. These include;

* Disclosure of technical and/or commercial information that is sensitive or proprietary. As noted in Cartier International AG v British Sky Broadcasting Limited, cooperation with law enforcement or compliance with court orders may involve the disclosure of technical and proprietary information the details of which ISPs prefer to keep secret. [[63]](#footnote-63)
* Conflict of interests - Conflicts may arise between ISP’s duty to protect users’ personal information and requirement to disclose the information to law enforcement.
* Cost - Investment in filtering and blocking technologies to meet either voluntary or mandatory cooperation requirements has cost implications for ISPs.[[64]](#footnote-64)
* Access and quality of service -Cooperation can impact on access and quality of service particularly if sites and services were wrongly categorised. For example, over-blocking may occur.[[65]](#footnote-65)
* Cyber-attacks- ISPS may be subject to cyber-attacks such as distributed denial of service attacks following implementation of court orders.[[66]](#footnote-66)

 11. **What is the effectiveness of investigation and prosecution of illegal content crimes and child abuse on the internet in your country according to available statistical data and research?**

**Online Child sexual abuse**

Available evidence (not figures or estimates) indicate that there have been a number of successful investigations and prosecution of child sexual abuse cases in the UK. These include high profile investigations codenamed “operation span”, “Operation Retriever” and “Operation Bullfinch”. These cases are however not specific to internet child abuse and are still considered marginal successes against the number of potential cases in which investigation or prosecution is needed. According to the Crown Prosecution Service (CPS), while there has been an increase in the number of sexual abuse cases brought to the court as well as in the conviction rate for offenders, fundamental questions persists “…about the way in which we investigate and prosecute sexual offences, particularly those involving children.”[[67]](#footnote-67)

Specific to online child abuse, the National Crime Agency stated that in 2014, 50,000 people in the UK have accessed child abuse images, but because it is unrealistic to bring them all to justice, the police focus only on those who posed the most risk. The Agency also noted that out of 20,000 to 30,000 potential offenders, only 660 arrests were made.[[68]](#footnote-68) Since according to the Home Office, all crimes should be investigated, these statistics indicate both the scale of the problem and the relative ineffectiveness of investigative and prosecutorial capacities in online child abuse cases.

**Other Content Related Offences – Intellectual property rights infringement**

Under Section 107 of the Copyright, Design and Patent Act 1998, communication of copyright works to the public and commercial distribution of copyright works are offences. The Digital Economy Act (DEA) 2010 also made provisions enabling right owners to investigate and prosecute individual infringers. Section 3 of the DEA enables a copyright owner to make a copyright infringement report (CIR) to an ISP if it appears to the owner that a subscriber to an internet access service has infringed or allowed another to infringe the owner’s copyright. The report is subject to the condition that the “initial obligations code” under sections 124C and 124D of the Communications Act 2003 allows the copyright owner to do so. An ISP who has received a CIR must notify the concerned subscriber within a month if the initial obligations code requires it. The notification must specify that it (the notification) was sent due to receipt of a CIR and set out the details of the alleged infringement. The notification in general or particular cases may also include a statement that the right owner may apply to court to learn the subscriber’s identity and may bring proceedings against the subscriber for copyright infringement.

Ofcom’s Draft Initial Obligations Code proposed that where a subscriber receives three notifications within a year, (referred to as “three strikes” or graduated response) he should be included on the Copyright Infringement List (CIL)[[69]](#footnote-69). As a consequence of being included on the list, the subscriber may be taken to court for copyright infringement. However, the process of identifying infringers by linking named individuals to IP addresses is fraught with factual and technical difficulties. It is therefore unclear whether criminal prosecutions could follow from the application of the relevant sections of the DEA.

Generally, statistics are not available to indicate the rate of criminal convictions for online infringement. According to a 2012 Ofcom report however, although infringement of copyright content is widespread among internet users in the UK, “The ways in which consumers access and share copyright material online change regularly, and infringement levels in particular are notoriously difficult to measure.”[[70]](#footnote-70) Also, a voluntary initiative by industry to combat online infringement projected that 2.5 million letters would be sent to alleged infringers within the first year of implementation.[[71]](#footnote-71) These developments are indicative of the attendant difficulties of investigating and prosecuting individuals for infringement of copyright online.

More crucially, the DEA is considered controversial and has been criticised as “legislation rushed through without sufficient scrutiny.”[[72]](#footnote-72) As a result, government has now shelved the enforcement regime under the law in favour of the voluntary framework proposed by industry. The framework involved the Creative Content UK Scheme formed by UK’s largest ISPs and content creators. Although a date has not being set for its commencement, the programme would involve sending up to four letters to subscribers to advise them when an infringement is happening on their account. The letters would give further advice on how to prevent infringement and point the alleged infringer towards the legal ways to access copyright content. No consequences are attached if recipients of the letters choose to ignore the advice and warnings.

 **12.** **Is there any new legislation prepared or proposed concerning the above mentioned issues? If so, please indicate what the intended changes are and what reasons for them?**

Current proposals for legislation in the UK focus on extending the powers of law enforcement and other relevant authorities with respect to access to communication data. Recent proposals are as follows;

**Draft Communications Bill 2012**

The Draft Communication Bill would replace chapter II of Part I RIPA. Although like the RIPA, the draft Bill would exclude the contents of communication, it would extend the powers of government to access more communication data. Clause 1 of the Bill allows the Secretary of State by order to ensure that communication data is available from telecommunications operators to public authorities. In particular, the law would cover the following communication data;

* Subscriber data relating to IP addresses,
* Data identifying which services or websites are used online, and
* Data from communication service providers based abroad who provide webmail and social networks to users in the UK.

It would therefore include messages sent on social media, webmail, voice calls over the internet and gaming as well as emails and phone calls. These categories of data are deemed to be currently unavailable to law enforcement in the UK. The new powers were necessary to ensure that relevant authorities keep pace with technological changes.[[73]](#footnote-73)However, the bill, which is also referred to as the “snooper’s charter”, has been widely criticised for being too invasive and appears to have been abandoned.[[74]](#footnote-74)

**Review of RIPA**

The Home secretary announced in July 2014 that she has commissioned a review of the RIPA. The review would be carried out by the independent reviewer of terrorism legislation and followed conclusions of a report by the Home Office Select Committee that the RIPA was not fit for purpose. The aim of the review is to consider, in the light of diverse emerging threats faced by the UK, and the need to uphold civil liberties, the capabilities and powers required by law enforcement and intelligence and the regulatory frameworks within which such capacities should be exercised. In particular, the objectives of the review will include the assessment of the interception powers with respect to communication data under the RIPA. The review is expected to report on whether the UK needs new legislation along the lines of the proposed Communications Data Bill.[[75]](#footnote-75)

**Counter-terrorism and Security Bill 2014-2015**

Clause 17 of the Counter-terrorism bill proposes to amend section 2(1) of DRIPA 2014. The amendment will enable the Secretary of State to require telecommunications operators to retain an additional category of communications data. Specifically, such data that will allow relevant authorities to identify the person or device using a particular IP address at any given time.[[76]](#footnote-76)

The justification for the amendment as stated by the Home Office, is to ensure that that intelligence and law enforcement agencies have access to communication data which may be required in investigations involving national security and organised crimes.[[77]](#footnote-77)

1. Ofcom FAQs by ISPs and about New Regulatory Framework available http://www.ofcom.org.uk/static/archive/oftel/publications/eu\_directives/2003/ispfaq0303.htm accessed 19/01//2015. [↑](#footnote-ref-1)
2. Communications Act 2003 s 32(1),(2). [↑](#footnote-ref-2)
3. Ofcom FAQs by ISPs and about New Regulatory Framework available http://www.ofcom.org.uk/static/archive/oftel/publications/eu\_directives/2003/ispfaq0303 [↑](#footnote-ref-3)
4. Communications Act 2003 s 32(7). [↑](#footnote-ref-4)
5. Communications Act 2003 s 151. [↑](#footnote-ref-5)
6. See Consolidated Version of General Conditions as at September 2014 (including annotations) Schedule of the Notification under section 48(1)of the Communications Act 2003). [↑](#footnote-ref-6)
7. See generally RIPA s. 2(1). [↑](#footnote-ref-7)
8. See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. [↑](#footnote-ref-8)
9. Data Retention Regulations ss 4, 5. [↑](#footnote-ref-9)
10. Data Retention Regulations s 2. [↑](#footnote-ref-10)
11. See Communications Act 2003 s 151; see also previous notes above. [↑](#footnote-ref-11)
12. See Data Retention Regulations pt.3 Sch. [↑](#footnote-ref-12)
13. Data Retention Regulations s 4(5). [↑](#footnote-ref-13)
14. Data Retention Regulations s 8. [↑](#footnote-ref-14)
15. See *Digital Rights Ireland* case (*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [C-293/12](https://www.lexisnexis.com/uk/legal/search/enhRunRemoteLink.do?A=0.013796884882983584&service=citation&langcountry=GB&backKey=20_T21249588357&linkInfo=F%23GB%23C%23sel1%252012%25page%25293%25year%252012%25&ersKey=23_T21249588343), [[2014] All ER (D) 66 (Apr)](https://www.lexisnexis.com/uk/legal/search/enhRunRemoteLink.do?A=0.37889374732479275&service=citation&langcountry=GB&backKey=20_T21249588357&linkInfo=F%23GB%23ALLERD%23vol%2504%25sel1%252014%25page%2566%25year%252014%25sel2%2504%25&ersKey=23_T21249588343" \t "_parent)). [↑](#footnote-ref-15)
16. See Philip Ward and Alexander Horne, ‘Interception of Communications’ (House of Commons Library Standard Note SN/HA/6322 of15th January 2015, 10-11. [↑](#footnote-ref-16)
17. RIPA s 21(4)(a)-(c). [↑](#footnote-ref-17)
18. RIPA section 22(2) as amended by DRIP ss 3(1)&(2). [↑](#footnote-ref-18)
19. RIPA s 22 as amended by DRIP Act s 3(4). [↑](#footnote-ref-19)
20. RIPA s 22(2) paragraphs (a) to (h). [↑](#footnote-ref-20)
21. DRIPA s 2(1). [↑](#footnote-ref-21)
22. See EU Directive 2000/31/EC. on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (the Directive on electronic commerce) as amended by Directive 98/48/EC. [↑](#footnote-ref-22)
23. This is the fifth data protection principle, see DPA pt.1 sch. 1 [↑](#footnote-ref-23)
24. See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/.... accessed 15/01/2015. [↑](#footnote-ref-24)
25. See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-5-retention/.... accessed 15/01/2015. [↑](#footnote-ref-25)
26. RIPA s 21(4)-(6). [↑](#footnote-ref-26)
27. See RIPA s 21(6)(a)-(d). [↑](#footnote-ref-27)
28. RIPA s 21(4)(b). [↑](#footnote-ref-28)
29. See e.g. Explanatory Notes to the Data Retention and Investigatory Powers Bill http://www.publications.parliament.uk/pa/bills/lbill/2014-2015/0037/en/15037en.htm accessed 18/01/2015. [↑](#footnote-ref-29)
30. RIPA s 1(1)(a)-(b). [↑](#footnote-ref-30)
31. RIPA 5(1) (a) –(d). [↑](#footnote-ref-31)
32. See RIPA s 5(3) (a)-(c). [↑](#footnote-ref-32)
33. See RIPA s 7(1),(2). [↑](#footnote-ref-33)
34. RIPA s 8(1),(2). [↑](#footnote-ref-34)
35. RIPA s11(4),(5). [↑](#footnote-ref-35)
36. RIPA s 11(7)(a),(b). [↑](#footnote-ref-36)
37. RIPA 12(1). [↑](#footnote-ref-37)
38. RIPA 12(2),(3). [↑](#footnote-ref-38)
39. RIPA 12(7). [↑](#footnote-ref-39)
40. See RIPA (Maintenance of Interception Capability Order) 2002. [↑](#footnote-ref-40)
41. Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers for 2013-2014 HC 345-SG/2014/93 [5.30]. [↑](#footnote-ref-41)
42. RIPA s 21(4). [↑](#footnote-ref-42)
43. RIPA s 22 (1) -(4). [↑](#footnote-ref-43)
44. RIPA s 25(1),(2). [↑](#footnote-ref-44)
45. RIPA 22(5). [↑](#footnote-ref-45)
46. RIPA s 22(2). [↑](#footnote-ref-46)
47. RIPA 22(4)-(8). [↑](#footnote-ref-47)
48. See Intelligence and Security Committee, ‘Access to Communications Data by the Intelligence and Security Agencies (Cm 8514) Feb 2013, 5. [↑](#footnote-ref-48)
49. RIPA s 14(1)-(3). [↑](#footnote-ref-49)
50. See https://www.iwf.org.uk/about-iwf accessed 28/01/2015. [↑](#footnote-ref-50)
51. Copyright, Design and Patent Act 1998, s 97A(1). [↑](#footnote-ref-51)
52. Copyright, Design and Patent Act 1998 s 97A(2)(b). [↑](#footnote-ref-52)
53. Copyright, Design and Patent Act 1998 s 97A(2)(b). [↑](#footnote-ref-53)
54. See e.g.Twentieth Century Fox Film Corporation v British Telecommunications plc [2011] EWHC 1981 (ch) ; see also Twentieth Century Fox Film Corporation v British Telecommunications plc (No 2) [2011] EWHC 2714;Dramatico Entertainment Ltd and other companies v British Sky Broadcasting Ltd and other companies - [2012] All ER (D) 30 (May); Football Association Premier League Ltd v British Sky Broadcasting Ltd and other companies - [2013] All ER (D) 189 (Jul); and Paramount Home Entertainment International Ltd and others v British Sky Broadcasting Ltd and others - [2013] All ER (D) 151 (Nov). [↑](#footnote-ref-54)
55. seeCartier International AG and others v British Sky Broadcasting and others [2014] EWHC 3354 (Ch). [↑](#footnote-ref-55)
56. Digital Economy Act 2010 s 17(2). [↑](#footnote-ref-56)
57. Digital Economy Act s 17(3). [↑](#footnote-ref-57)
58. Digital Economy Act s 17(4),(5), (6). [↑](#footnote-ref-58)
59. See British Telecommunications v Secretary of State for Business, Innovation & Skills [2011] EWHC 1021 (Admin); see also OFCOM, “Site Blocking” to Reduce Online Copyright Infringement A Review of Sections 17 and 18 of the Digital Economy Act 7 May 2010, 50. [↑](#footnote-ref-59)
60. See e.g. Cartier International AG and others v British Sky Broadcasting and others [2014] EWHC 3354 (Ch). [↑](#footnote-ref-60)
61. See Twentieth Century Fox Film Corporation v British Telecommunications plc [2011] EWHC 1981 (ch). [↑](#footnote-ref-61)
62. See https://www.gov.uk/government/speeches/keynote-speech-for-the-internet-service-providers-association-ispa-annual-conference accessed 27/01/2015. [↑](#footnote-ref-62)
63. (2014) EWHC 3354 [para 38]. [↑](#footnote-ref-63)
64. see Cartier International AG v British Sky Broadcasting Limited (2014) EWHC 3354 [para 26, 38-51], see also Twentieth Century Fox Film Corporation v British Telecommunications plc [2011] EWHC 1981 (ch) [para 73]; see also Twentieth Century Fox Film Corporation v British Telecommunications plc (No 2) [2011] EWHC 2714 [para 6]. [↑](#footnote-ref-64)
65. Cartier International AG v British Sky Broadcasting Limited (2014) EWHC 3354 [para 36, 66- 77], [↑](#footnote-ref-65)
66. See Cartier International AG v British Sky Broadcasting Limited (2014) EWHC 3354 [para 68] [↑](#footnote-ref-66)
67. See Keith Starmer QC, Director of Public Prosecutions, ‘The Criminal Justice Response to Child Sexual Abuse: Time for a National Consensus’ available http://www.cps.gov.uk/news/articles/the\_criminal\_justice\_response\_to\_child\_sexual\_abuse\_-\_time\_for\_a\_national\_consensus/ accessed 29/01//2015 [↑](#footnote-ref-67)
68. http://www.bbc.co.uk/news/uk-2969268527/01/2015. [↑](#footnote-ref-68)
69. See Ofcom, Online Infringement of Copyright and the Digital Economy Act 2010 Notice of Ofcom’s proposal to make by order a code for regulating the initial obligations Interim statement and notice of a proposal to make an order published June 26 2012 [paras 6.1-6.39]. [↑](#footnote-ref-69)
70. See Ofcom, OCI Tracker Benchmark study Q3 2012 Nov 2012, 1 available http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/Intro.pdf accessed 28/01/2014. [↑](#footnote-ref-70)
71. See http://www.bbc.co.uk/news/technology-27330150 accessed 27/01/2015. [↑](#footnote-ref-71)
72. See https://www.openrightsgroup.org/issues/deact*I)* accessed 27/01/2015. [↑](#footnote-ref-72)
73. See House of Lords House of Commons Joint Committee on Draft Communications Data Bill Session 2012-2013 [[HL paper 79 HC 479] 2012, 16. [↑](#footnote-ref-73)
74. See House of Lords House of Commons Joint Committee on Draft Communications Data Bill Session 2012-2013 [[HL paper 79 HC 479] 2012, 3. [↑](#footnote-ref-74)
75. See Review of Communication Data and Interception Powers Terms of Reference https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/330749/Review\_of\_Communications\_Data\_and\_Interception\_Powers\_Terms\_of\_Reference.pdf accessed 31/01/2015. [↑](#footnote-ref-75)
76. Counter Terrorism and Security bill European Convention on Human Rights Memorandum by the Home Office [para 23]. https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/378948/Introduction\_-\_JCHR\_memo\_-\_Parly\_Team.pdf accessed 23/01/2015. [↑](#footnote-ref-76)
77. Counter Terrorism and Security bill European Convention on Human Rights Memorandum by the Home Office [para 25]. [↑](#footnote-ref-77)