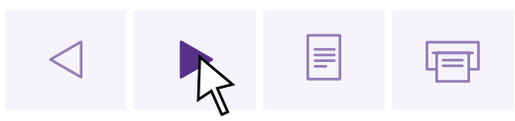
User guide

Welcome to the BT report on privacy and free expression in UK communications. In this interactive PDF you can do many things to help you easily access the information that you want, whether that's printing or going directly to another page, section or website, these are explained below:

Document Controls

Use the document controls located in the top right corner to help you navigate through this report.



Previous page | Next page | Contents page | Print

Links within this document

Throughout this report there are links to pages, other sections and web addresses for additional information.

Example

The distinction can be less easy with internet data such as a website address. Under the current Home Office code of practice, a domain name (http://sport.bt.com) is treated as communications data. But http://sport.bt.com/home-01363810438270 (i.e. anything beyond the first "/") counts as content. This matters because the law currently treats obtaining content as more intrusive than obtaining communications data.

Navigating with tabs

Use the tabs to the right to quickly go to the start of a different section. You will know which section you are in becase it will be highlighted in purple.

Privacy and free expression in UK communications

2015

Contents

Download report online:
www.bt.com/privacyandfreeexpression

Foreword

Today, communications are woven into the lives of virtually every UK citizen. Everyone expects instant connectivity – however, whenever and wherever they want. British people spend more time online than anyone else in Europe and spend more time each day using media and communications than they do sleeping.

The internet has been overwhelmingly positive and empowering, connecting people to other people and information they would not have had before. Millions are communicating, finding a voice, realising their potential.

But the internet can also be used for distasteful, or illegal activity – like sharing images of child sexual abuse or content that fuels hate, extremism or radicalisation. This raises tensions between the right to open, unrestricted communications and the need to promote safety and security. What part should companies like BT play in making those decisions?

People's communications generate vast amounts of data on our network. Our customers expect us to be guardians of that information. Yet governments expect access to it to keep society safe. How do we maintain our customers' trust when carrying out the role required by government?

Privacy and free expression have long been protected under international human rights standards. Governments must protect their citizens' human rights but also consider their responsibility to maintain a safe and stable society that – for example – protects its most vulnerable members.

BT has a long-standing commitment to respect human rights. This is why we are issuing this report: to explain how we respect the human rights which through our actions (or the actions of others) we might impact the most.

The issues are complex. People have many different views.

But fundamentally we support and respect individuals' rights to privacy and free expression, even as we accept that sometimes there need to be limitations on those rights, as international human rights standards allow. Where those limitations surface, they should be clearly delineated within strong legal frameworks. They should come with the right checks and balances.

As a company, we need of course to comply with the law, but when there is an opportunity to shape it, we take that opportunity and make clear any human rights concerns we have. That's just part of being a responsible and ethical business.

Sometimes we've led the case for change. We were the first communications provider in the world to create a system to block child sexual abuse images online (a system now used or copied around the globe). Other times we've challenged laws to make sure restrictions on free expression are clear.

But in other areas it can be more difficult: government investigatory powers are complex, wide-ranging and often difficult to work through. We want to contribute to a constructive debate about how these powers sit with people's human rights into the future.

Gavin Patterson
Chief Executive

1 Communication freedoms

- We respect human rights.
- Our main potential impacts are on rights to privacy and free expression.
- We think any limitations of these rights should be within a strong legal framework with the right checks and balances.
- If the law isn't clear, we try to find ways to help clarify or develop it.

1.1 Respecting people's rights

We were one of the original companies to sign the UN Global Compact – the world's largest corporate sustainability initiative, which sets out principles for responsible business. We're also committed to implementing the UN Guiding Principles on Business and Human Rights (UN Guiding Principles) which sets out expectations for respecting human rights.[1] These principles help us understand how our business might affect human rights, and what we need to do – and show publicly – to address that.[2]

In 2014 we decided to review how our UK operations were performing against those commitments. We looked at our potential effect on employees, customers, workers in our supply chain and communities in which we operate. (We focussed on the UK because it's where our mass-market consumer business is based.)[3]

We saw we could toughen our policy commitment with more detailed guidance. We found we could strengthen our governance with deeper engagement across the business, adopting more formal processes. To make sure we implement what we found, we have established a human rights steering group, sponsored by a member of our Operating Committee.[4] We also concluded that we could be more open about how we focus on our main potential impacts on human rights: privacy and free expression. That's why this report focuses on these two themes.

1.2 The right to privacy

We're in the business of connecting people. Businesses rely on us for connecting and communicating with customers. Millions of individuals come together with friends and family through our networks. They have access to vast amounts of information and entertainment at their fingertips. This in turn generates data on our networks. We have a duty to safeguard that data and the privacy of our customers' communications. But the UK government can compel us to give them access to data on our network, which could affect our customers' privacy.

The government has a duty to respect, protect and secure all human rights, including privacy. However, not all human rights are absolute. Under international human rights standards, governments can limit rights like privacy and free expression in order to fulfil other duties such as making sure society stays safe.

The breakneck pace of technology development, the growth of the internet and social media, the constantly evolving security threats of terrorism and cyber-attacks – these things make it difficult to find the right balance. As government tries to protect society, companies must play their part: people should be safe from threats, to enjoy their basic rights and freedoms.

Later in this report we explain the government's current powers to intercept people's communications or obtain data about those communications. We show how we do our best to respect human rights when we deal with the people exercising those investigatory powers. We detail the safeguards we have to weigh up our different obligations. And we also make a few recommendations on future developments in the law.

1 The UN Guiding Principles refer to internationally recognised human rights as expressed in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, as well as the principles set out in the Declaration on Fundamental Principles and Rights at Work: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

2 A number of industry initiatives and guidelines have been established to address the specific impacts of communications providers on the rights to privacy and free expression, most notably the Global Network Initiative and the Telecommunications Industry Dialogue.

3 The way the internet works means that communications will often pass through many networks in many countries. Outside the UK, each country will make its own decisions about the issues raised in this report.

4 http://www.btplc.com/Betterfuture/BetterFutureReport/Downloads/2015_BTBetterFuturefullreport.pdf page 10.

1.3 The right to free expression

We help people get the most they can from the power of communications. We stand up for the right to communicate openly, whenever and wherever possible, because that's what our business has always been about. The right to free expression isn't just about freedom of speech, it's also about the right to information.

We don't host (or store) much online content ourselves. We provide access to content produced by others – like shared social media content – by enabling people to transmit information across our networks.

So potentially we could limit people's rights to free expression if we block access to content online. And in rare circumstances that's what we do. We block access to child sexual abuse images. We block malware to protect our customers' communications and our network. When a court orders us to, we block material which infringes other people's rights.

Our parental control tools give customers choices over blocking certain content on devices in their homes. We believe there's a good case for people being able to make those choices themselves rather than us imposing choices on them. This was the subject of an industry debate in 2013 and 2014. Some politicians and media asserted that all adult material should be automatically blocked and that people should be forced to "opt in" in order to access it. We didn't see things quite the same way. Rather than restrict access to potentially legitimate content without consent, we argued the case for leaving the initial decision with our customers. The debate continues.

In the few situations where we host content ourselves[5] we allow people to add content and share opinions freely while protecting everyone from hateful or illegal material. Our terms and conditions are clear; customers must not upload content which is illegal, offensive, abusive, indecent, defamatory, obscene or menacing, or in breach of confidence, copyright, privacy or any other rights. If someone objects to any content, we quickly review it and remove it if we think it breaches our guidelines or is illegal. Speed is of the essence, otherwise we could be held legally responsible for making available illegal content. We've not had any requests to take down material from bt.com in the last 12 months. We've had only a handful of requests to suspend or take down material on sites we host as part of BT Community WebKit. And for MyDonate (our free online service for making charitable donations) we've taken down or modified around 20 to 30 comments made about donations in the last year.

Later in this report we explain why we take a strong stance on free expression. We believe in the right to access information online. Limitations to that right must be carefully circumscribed. Sometimes our position has meant getting clarity on the law in court (as we did when we took legal action to understand the impact of the Digital Economy Act 2010). We show where there are areas of legal uncertainty in the approach to free expression online – particularly when considering material which could be unlawful. And we make suggestions for safeguards in this area.

1.4 Our focus on free expression and privacy[6]

This report's main focus is on the rights to privacy and free expression. These aren't the only impacts on human rights we may have, but we think they're the most salient. And they're clearly connected: if people don't feel secure in their privacy, then they may self-censor their communications and the information they access online.

We believe everyone should be able to communicate openly, with their privacy protected. We also believe that sometimes it's right for online content to be blocked. Sometimes, though, it's right that government and law enforcement agencies access communications content – as long as they do it proportionately and within a strong and transparent legal framework. This will give everyone the confidence that the government is not abusing its powers. However we do recognise that the relevant laws aren't always perfect or up to date. If government (or another public body) wants to interfere with people's rights and the basis for doing that isn't clear to us, we challenge that request wherever possible.

It's a complicated scenario. Often issues are in tension with one another. The debate is moving quickly. The best way to weigh up different considerations changes quickly too. We have focussed for now on the UK because it is where we are based operationally and where we control our network. The way the internet works means that communications will often pass through many networks in many countries. Outside the UK, each country will make its own decisions about the issues raised in this report.

Inevitably, we make our own judgements on these issues. We try to be measured and balanced, informed by our core beliefs, and we welcome conversations with all stakeholders on how we can improve in future.

5 On bt.com, MyDonate (our online fundraising platform) and BT Community WebKit (our self-build website tool for charities and not-for-profit community groups).

6 We instructed the international law firm Linklaters LLP and Kieron Beal QC to support us in reviewing some of the legal analysis set out in this report. This report does not constitute legal advice by us or them. Neither we nor they accept any legal responsibility or liability for its contents nor should any reliance be placed on its contents. We received feedback from BSR, a global non-profit consultancy with human rights expertise, on a draft of this report.

2 Privacy and government investigatory powers

- Investigatory powers are essential to keep society safe.
- We have a legal obligation to comply with government requests for information about how people use our services and the content of their communications.
- Reform of the law governing investigatory powers is overdue.
- The draft Investigatory Powers Bill provides a foundation for open and meaningful debate.
- Any new law must be clear, with strong legal processes to hold investigatory powers in check and to make sure they're necessary and proportionate.

We have a duty to safeguard our customers' data and the privacy of their communications. You can find out more about these responsibilities in our Privacy Policy. We also have a legal obligation to comply with certain UK government requests for information from us about how people use our services and the content of their communications. For example, the government (and other public bodies) can obtain information from us about who our customers call and email. They can also sometimes require us to make the content of our customers' communications available in real-time – to find out what is being said, for example in a telephone conversation, text message or email. It's important that the way this is handled includes checks and balances and takes account of human rights, so that any information demands that are made are genuinely necessary and proportionate to the supposed threat.

The use of these powers and their impact on people's right to privacy is the subject of a healthy public and political debate. This was in part prompted by the allegations made by Edward Snowden, who leaked apparent US and UK security secrets, starting in 2013. Since then people have understandably questioned the role of communications providers in passing data to state agencies.

At the same time, the UN Guiding Principles have challenged companies to say more about how their actions impact people's human rights.

Human rights are central to the exercise of government investigatory powers. We all have a right to privacy. But international and European law allow the UK to restrict privacy rights when it's necessary and proportionate. That's because government also has a duty to protect its citizens so they can live in a safe society.

This balance between privacy and security is a big challenge in the internet age. Different stakeholders have different views: what information should be available to government and on what basis? Does government need more or different powers to reflect technological changes? Are there enough checks and balances on the use of these powers, to protect privacy rights?

And what role should communications providers play in support of these powers?

At BT, we believe government must have investigatory powers to protect society. And we support the UK government in protecting national security, fighting crime and helping individuals in "life at risk" situations. Gavin Patterson, our CEO, is on record as saying that the right to privacy should not be absolute, and must be balanced against the requirement to protect society.

But it's vital that there are proper controls over investigatory powers and how they're used. These powers can be intrusive. They should only be used when clearly lawful, necessary and proportionate. And the public must have confidence that there's a strong legal framework protecting their rights against unnecessary interference. Because privacy is even more important in an age when so much information is available about people's lives online.

The UN Guiding Principles recognise that countries have a duty to protect human rights. It's down to governments to strike the right balance between protecting individual privacy and protecting society. Our responsibility is to make sure our own actions respect human rights. And that we try to use our influence to make sure others do the same. When it comes to the government's investigatory powers we have limited discretion – we have to comply with the law.

As we show later in this report, we have strong internal oversight of what we do, and we take expert advice to inform our approach. We have actively engaged with the UK government and other bodies on the law and policy in this area. We'll keep doing this to help shape the debate about the proposed new law set out in the IPB.

We explain here our approach under the current law. However there are restrictions in particular laws, for example the Telecommunications Act 1984, the Official Secrets Act 1989 and the Regulation of Investigatory Powers Act 2000 (RIPA), which limit what we can say about these powers. There are also government policy restrictions (for example the policy to mark certain documents with a secrecy rating, and the "need to know" practice) which limit the sharing of certain information. We accept that sometimes secrecy is needed. But we're in favour of transparency whenever possible.

2.1 The current investigatory powers regime

RIPA is the main UK law governing investigatory powers. Large parts of RIPA are to be replaced by the end of 2016. On 4 November 2015, the government published the draft Investigatory Power Bill (IPB), which brings together all its powers to obtain content and communications data from communications providers. The IPB, which includes powers drawn not only from RIPA but from other relevant statutes, is due to go through a process of public consultation until early 2016. It will be considered by the Houses of Parliament, as part of a consultation review process before a Joint Committee of Parliament.

We will play a full part in the consultation. This document describes our approach to the existing legal regime, as one of its purposes is to explain how we do things prior to any legal change. Our view of how things work currently will inform our views about the best eventual shape of the IPB.

What information on our networks is affected by the current regime?

RIPA allows the government (and other public bodies, including the security services and the police) to access both "communications data" and also the content of communications. The law treats communications data and content differently – although it can sometimes be difficult to tell one from the other. For telephone data, the distinction is straightforward. The number called, the date, time and duration of the call are communications data. The conversation is the content.

The distinction can be less easy with internet data such as a website address. Under the current Home Office code of practice, a domain name (http://sport.bt.com) is treated as communications data. But http://sport.bt.com/home-01363810438270 (i.e. anything beyond the first "/") counts as content. This matters because the law currently treats obtaining content as more intrusive than obtaining communications data.

Fewer public bodies are entitled to obtain content data, and they need a higher level of authorisation. However, communications data, in significant volumes, can build a detailed profile of an individual and so be very intrusive on privacy. So we think the question of whether the new law needs to adopt a different approach needs to be considered carefully.

Who can get access to communications data?

A number of public bodies have the legal right to obtain data from us. This includes intelligence and law enforcement agencies, certain government departments, local authorities and some regulators. Exactly what data they require depends on the circumstances.

But data may be disclosed only if it's necessary for one of a limited number of purposes. The most significant are the prevention of crime and the protection of national security. Data may only be disclosed if a senior officer at the relevant public body believes it's necessary and proportionate. The data might be the name and address of a person using a particular telephone number or Internet Protocol address (IP address). Or, it could be details of the calls made to or from a particular telephone number. RIPA provides the legal basis for these disclosures.

The government has now acknowledged that it has also used its powers under the Telecommunications Act 1984 for the bulk acquisition of communications data (see the table on page 14).

Where does all this information come from?

We keep some personal information, including communications data, for day-to-day business purposes like providing bills to our customers. Our reason for keeping the data, and the length of time we keep it, depends on what sort of data it is. All personal information is kept in accordance with the Data Protection Act 1998, which requires us to keep data safely and for no longer than necessary for the relevant purposes. We say more about how we do this in our Privacy Policy.[7]

The government can also require us to hold onto some types of communications data in a separate database, for up to twelve months. It can do this by serving a data retention notice under the Data Retention and Investigatory Powers Act 2014 (DRIPA), which has recently been the subject of judicial review proceedings. The Counter-Terrorism and Security Act 2015 increased the data retention powers available to government. It lets IP addresses be linked more easily to the individuals using them at the relevant time.

This is an important change, because it may require communications providers to keep information that they wouldn't otherwise need for normal business purposes. 'Summary of Public Bodies' Access to Data' (page 14) provides information about the ways in which content and communications data can be obtained.

It's currently not clear whether it's lawful for a communications provider to say that it's received a DRIPA data retention notice. No communications provider has made such information public. The IPB now contains a clause prohibiting communications providers from disclosing information about retention notices.

We believe there are good reasons for this provision such as limiting the opportunity for customers to seek out communications providers that are not subject to data retention notices.

Who has oversight of these powers?

The Interception of Communications Commissioner's Office (IOCCO) has statutory oversight for this part of the investigatory powers regime. It publishes information about how the regime is used – for example, for acquiring content and communications data. A Home Office code of practice sets out what information is retained and reported to IOCCO (by public bodies and communications providers), and this forms the basis of the statistical information which IOCCO publishes. IOCCO's March 2015 report says 517,236 communications data requests were made to all communications providers under RIPA in 2014. The vast majority came from the police or other law enforcement agencies.

Government has other powers to access communications data that in the past were not within IOCCO's remit. The Home Secretary acknowledged in her statement to Parliament on 4 November 2015 that section 94 of the Telecommunications Act 1984 has been used by successive governments to access communications data in the UK. This means the authorisations and notices reported by IOCCO don't provide a complete and accurate picture of all requests for communications data made by government.

How many times have we had to disclose communications data?

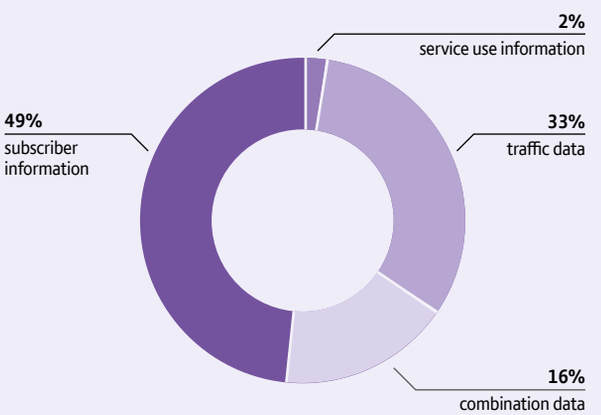
We thought carefully about whether to report on how many times we've disclosed communications data under RIPA. Communications providers operating outside the UK have reported this data (both for the countries in which they operate, as well as in some instances where they have received requests from the UK authorities). We've discussed this with IOCCO, who expressed concerns about individual communications providers reporting their own figures, since different counting mechanisms and rules could be applied. Their view is that the statistical information should only be collected and reported by the public authorities to make sure it's comparable and accurate.

In the interests of greater transparency, we think it worth considering whether it might be helpful for IOCCO to provide information on trends, and further analysis of the numbers. In this context, we note that in its 2013 Annual Report, IOCCO asked for better information from public authorities on the use of these powers.

Number of authorisations and notices for communications data as reported by IOCCO

Source: Report of the IOCCO March 2015

Authorisations and notices by data type as reported by IOCCO



Source: Report of the IOCCO March 2015. "Service use information" is how a person has used a communication service; it is the sort of information that would once have been in an itemised telephone bill. "Traffic data" is attached to a communication for the purpose of transmitting it (e.g. sender, recipient, location and time of sending). "Subscriber information" is what a customer would typically provide when they sign up to a communications service (e.g. name, address). "Combination data" is a mixture of traffic data, service use and subscriber information.

7 http://home.bt.com/pages/navigation/privacypolicy.html

Who can access content data – what's said or written in a communication?

Interception powers can only be used, where necessary, for very limited purposes (for example the prevention or detection of serious crime and national security), and by very few public bodies (primarily the police and intelligence agencies). A Secretary of State must authorise a warrant, and must confirm that the warrant is necessary and proportionate.

Any person or body, including a communications provider, can be required to take all "reasonably practicable" steps to give effect to an interception warrant.

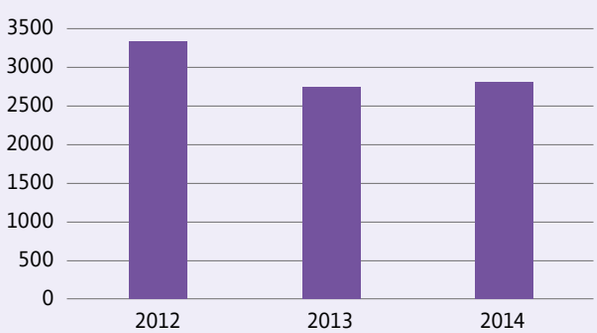
An interception warrant can be targeted at a single "person" (which includes an organisation) or premises. Or, it may be framed more broadly, without reference to a specific person or premises, and so potentially drawing in a very broad set of data. In such cases, only "external" communications can be intercepted (those sent or received outside the British Islands). The Secretary of State must also certify the descriptions of intercepted material which he or she considers it necessary to examine.

These warrants have been referred to as "bulk" warrants in the recent reports by the Parliamentary Intelligence and Security Committee and by David Anderson QC (asked by the government to review the current powers and recommend changes). The term has no legal meaning though. It simply describes any warrant that is not targeted at a single person or premises, and so potentially very broad in its scope and application.

Who has oversight of these powers?

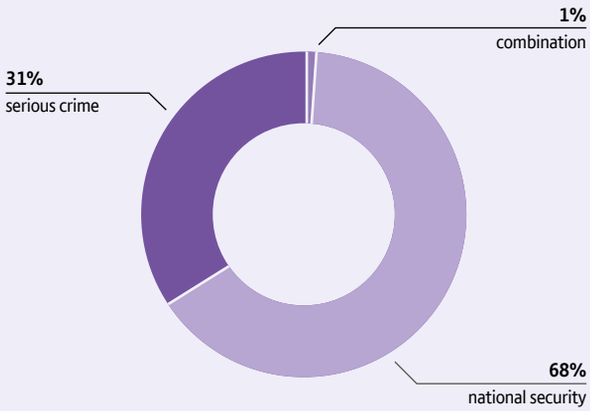
Again, IOCCO has statutory oversight. IOCCO's March 2015 report shows 2,795 interception warrants were issued in the UK in 2014. It provides information about the purposes for which these interception warrants were used.

Total Number of New Interception Warrants Issued as reported by IOCCO



Source: Report of the IOCCO March 2015

Warrants Issued by Statutory Purpose



Source: Report of the IOCCO March 2015

How many requests have we received?

It's a criminal offence under RIPA for a communications provider to disclose any information about interception warrants. We understand the need not to undermine operational effectiveness by letting criminals and terrorists know who has been targeted. So despite our support for privacy and transparency, we do therefore support this particular secrecy requirement.

In the light of this and other legal rules, sometimes communications providers follow a practice of "neither confirming nor denying" when asked a particular question (i.e. neither confirming nor denying a particular course of action).

It is not an offence to deny that assistance was required, in cases where it wasn't. But to do so would mean that a failure to deny in any other case would be taken as confirmation of involvement – so undermining the purpose of the secrecy rules.

Are there any other government powers to access people's information?

The government has a range of other investigatory powers. For example, it has a very broad discretion to issue directions under section 94 of the Telecommunications Act 1984, if necessary in the interests of national security. When publishing the IPB, the government acknowledged that this power has been used for the bulk acquisition of communications data.

Another example is the Intelligence Services Act 1994, under which the intelligence agencies can interfere with electronic equipment such as computers. This is termed "equipment interference" or "computer network exploitation" and requires a warrant issued by the Secretary of State. Conduct of this type was first acknowledged by the government early in 2015. Secrecy restrictions apply to the use of these powers, both of which, with some changes, have been brought within the ambit of the IPB.

2.2 The part we play

At BT, we understand and support the need for government to use investigatory powers to protect national security, fight serious crime and to protect people in "life at risk" situations. Communications providers clearly have a part to play in this. It's also important that our customers can trust us to do the right thing with their personal information.

We play no part in the authorisation of requests. We don't know why a request has been made, or the grounds for deciding that it is necessary and proportionate. Generally, we believe that this is the right approach – it's for our democratically elected government and its agencies to decide what is needed for law enforcement or national security reasons. However we do think that we should have the opportunity to give our view on technical and practical issues relating to use of the powers.

If we're required to assist, for example, with a warrant relating to an individual or to provide the communications data for a particular account, our role is primarily to check that the request is made in a lawful way, and that we comply with it accurately and on time. The requesting public body is responsible for making sure that any request is compliant with human rights laws. Sometimes, we might ask for clarity about the scale and scope of a requirement on us.

What are our internal governance arrangements?

Since 1984, a committee comprising members of our main Board and other senior people has been responsible for governance and oversight of the assistance that we are asked to provide to government in relation to RIPA and related matters. This includes requests for interception and communications data. Its membership currently includes the Group CEO, the BT Chairman, senior technical, security and legal experts, together with a non-executive BT Director and an independent member with specialist knowledge. The oversight of this committee gives us a solid basis for considering how best to balance our legal obligations against privacy and humans rights considerations.

We also have operational teams that deal solely with the practical aspects of our obligations under the investigatory powers regime. These are supplemented by senior people with the responsibility for monitoring BT's legal obligations under RIPA, and for making sure that we take account of human rights considerations.

Underpinning all this, we have systems and processes to check that requirements on us are properly made under the law; to ensure that the action we take is lawful; and to audit what we do on a regular basis. Following the Snowden revelations, we sought an independent view on some of our processes and some issues of legal interpretation, from Linklaters LLP, a leading law firm, and from Kieron Beal QC.

If we have any concerns about something we're being asked to do, we carry out our own legal review – and get an expert opinion where necessary – before raising our concerns with the requesting authority.

We've done this on a number of occasions for both legal and operational reasons. And sometimes we've spoken directly with the government to voice our concerns or seek assurances. (The law – which is intended to stop criminals and terrorists knowing too much about the drive against them – means we can't go into any more detail about these exchanges.)

We also speak regularly to government about investigatory powers, giving our opinions on the underlying regime and how it could be improved. In the last two years, we've had meetings with government and government officials, some at a very senior level, to discuss things like RIPA, DRIPA and section 94 of the Telecommunications Act 1984. In 2014, at our Chairman and Chief Executive's request, we met with the then Interception of Communications Commissioner, Sir Anthony May, to talk through the scope and interpretation of some RIPA provisions. And we meet regularly with IOCCO officials to discuss a broad range of topics.

Whenever we can, we use our influence to improve the law, in line with our commitment to respect human rights. We will keep on doing this – throughout the IPB consultation process and beyond.

It's vital that our customers feel they can trust us. They need to be confident that the authorisation and oversight regime is robust and working well. We'll challenge the government on something we're uncomfortable with, whether that's a particular request or particular law.

2.3 Where next for the investigatory powers regime?

In 2015, before the IPB was published, there were a number of reports on the investigatory powers regime. On top of that, the UK Prime Minister asked Sir Nigel Sheinwald to talk to some internet companies, the US and other governments to find a better way for countries to access and share data for the fight against crime and terrorism. These conversations led to the Sheinwald report on international data sharing (delivered to government in June 2015).

These reports shaped the government's thinking in how it developed the IPB.

What was in these reports?
The three reports (summarised below) all agreed that investigatory powers law was fragmented and outdated. They all called for reform. In particular they called for greater transparency and oversight of the powers. But they also disagreed on some big things – like the authorisation of warrants.

The only official, public-domain information on Sir Nigel Sheinwald's work is a two-page summary of his report. In it he advocates improving government-to-government cooperation, reforming the existing UK / US Mutual Legal Assistance Treaty and building a new international framework for those countries with similar high standards of oversight, transparency and privacy protection.

Privacy and Security: A Modern and Transparent Legal Framework – The Intelligence and Security Committee

The Intelligence and Security Committee (ISC) is a Parliamentary Committee. It has access to the government agencies which use the laws on investigatory powers. Its March 2015 report criticised the current law as outdated, complex and opaque. It recommended:

- A single, new, more transparent law backed up with better oversight.
- New definitions for "communications data", "communications data plus" and "content-derived information", with differences reflecting varying levels of intrusiveness.
- Reforming section 94 Telecommunications Act 1984 to clarify when it could be used and why.
- Reforming the Investigatory Powers Tribunal (IPT) which hears claims against government's use of the regime (often in secret) – to include a right of appeal.
- Government ministers (not judges) should continue to approve warrants for intrusive data requests.

The report also acknowledged that the government uses "bulk interception". However, the ISC was happy that only a very small percentage of internet traffic was actually collected and an even smaller proportion looked at. On this basis, it said bulk interception is a valuable capability that should remain available to the intelligence agencies.

2015 ▶

January | February | March | April | May | June

A Question of Trust – Report of the Investigatory Powers Review – David Anderson QC, Independent Reviewer of Terrorism Legislation

The government asked David Anderson QC to review the current law and recommend changes. He looked at terrorist threats to the UK; the capabilities we'd need to tackle them; safeguards to protect privacy; the challenges of changing technologies; and transparency and oversight. His review identified five key principles for the new law:

- Minimise no-go areas for law enforcement – meaning data shouldn't be beyond the reach of government simply because of the way it is sent or stored over the internet (for example, if it's encrypted or sent over the dark net).
- Investigatory powers should be limited powers – to protect privacy.
- Rights compliant – meaning people must know what the intrusive powers are and how they can be used.
- Clear and transparent rules – because "obscure laws corrode democracy".
- A unified approach – meaning one regime for intelligence communities and law enforcement.

In line with those key principles, his review made a lot of recommendations, including:

- Replacing the relevant parts of RIPA, DRIPA and other related laws with a single new law, "drafted from scratch".
- Replacing the three existing oversight bodies (or regulators) with a new Independent Surveillance and Intelligence Commission (ISIC).
- Making sure all warrants are issued only by Judicial Commissioners (within ISIC), who must hold, or have held, high judicial office.
- Keeping the data retention laws but bringing them into line with EU law and human rights.
- Limiting specific interception warrants to a single person, or premises (as now) or operation (new category).
- Introducing a new "combined warrant" for interception / intrusive surveillance / property interference.
- Allowing lawful "bulk" interception, with the right safeguards, under EU law.
- Introducing a new type of warrant for "bulk" communications data.
- Adding backstop powers to the new law – along the lines of section 94 Telecommunications Act 1984.
- Reviewing the distinction between content and communications data.
- Keeping the requirement for IP address resolution. But government should show why it needs communications providers to keep internet connection records (weblogs) – which is likely to be justified if there's good reason, and "third party data" (like data from Facebook or Google) – for which it's harder to show a good reason to keep.

On 4 November 2015, the government published the IPB, which brings together all its powers to obtain content and communications data from communications providers. The IPB, which includes powers drawn not only from RIPA but from other relevant statutes, is due to go through a process of public consultation until early 2016. It will be considered by the Houses of Parliament, as part of a consultation review process before a Joint Committee of Parliament.

In drafting the IPB, the government has also taken into account other views, including ours. There are also a number of important legal cases that may have an impact on the government's proposals. Some of these cases are over, some are still pending. Some may have a direct impact, some indirect. But they are all potentially significant:

- The Data Retention Directive – In April 2014 the Court of Justice of the European Union (CJEU) declared this invalid in the Digital Rights Ireland case because it didn't comply with the principle of proportionality. its interference with the right to privacy was not limited to what was strictly necessary.
- DRIPA – In July 2014, DRIPA was passed to make sure the government (and other public bodies) kept a legal right to make communications providers hold onto communications data. It's due to expire at the end of 2016. The UK High Court said that parts of DRIPA aren't compatible with Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the European Union's Charter of Fundamental Rights. The Court of Appeal disagreed with the High Court, has now referred this case to the CJEU and will seek further clarity on the Digital Rights Ireland case.
- Bulk interception – in September 2013 Big Brother Watch asked the European Court of Human Rights (ECtHR) to review whether the UK's surveillance laws were compatible with the European Convention on Human Rights. This claim was then put on hold because of a similar challenge at the IPT, brought by Liberty, Amnesty International, and Privacy International.
- The IPT found in December 2014 that the UK's bulk interception regime did not contravene Convention rights. Liberty, Privacy International and Amnesty International effectively appealed this decision by filing a claim at the ECtHR in April 2015.
- The IPT also issued two further decisions in 2015 which related to the December 2014 judgment. In February it found that the lack of transparency around the security services' policies and procedures breached Article 8 (although the breach had since been fixed). In June, it concluded that the lawfully intercepted communications of Amnesty International and the South African Legal Resources Centre had not been handled in line with GCHQ internal procedures.
- In an unrelated case, the IPT also found in June 2015 that legally privileged documents belonging to a Libyan dissident had been unlawfully intercepted.
- Two other challenges were filed at the ECtHR in September 2014 and are waiting to be heard. In one, the Bureau of Investigative Journalism questioned whether UK law adequately protects the communications of journalists. In the other, Privacy International asked for the disclosure of documents relating to surveillance arrangements between the US, United Kingdom, Canada, Australia, and New Zealand.
- Safe Harbor – in October 2015, the CJEU made an important decision on data protection in the Schrems case. It said that the Safe Harbor scheme (under which personal data can be transferred from the EU to registered bodies in the US) doesn't adequately protect data. One reason was that the scheme may not be able to stop the US intelligence authorities accessing the transferred data on a large scale. And this isn't compatible with the right to privacy in the EU Charter of Fundamental Rights.

July | August | September | October | November | December

A Democratic Licence to Operate – Report of the Independent Surveillance Review Royal United Services Institute

RUSI is an independent think-tank on international defence and security. Its report:

- Called for a new and more transparent law.
- Recommended that the definitions of content and communications data should be reviewed.
- Said that bulk communications data collection should be under a warrant.
- Said that there should be more judicial involvement in the issue of warrants.
- Supported the need for a new Mutual Legal Assistance Treaty to allow the better exchange of information between countries for crime and terrorism prevention.

What do we think the new regime should look like?

In our response to the Anderson Review, we summarised our position like this: "We consider that it is appropriate to maintain a regime that permits access to content and communications data, provided that the circumstances are suitably circumscribed, and provided that all necessary checks and balances are in place to ensure the lawful and proportionate operation of that regime, particularly from a human rights perspective."[8]

This is still our view. It will underpin everything we say during the formal consultation on the IPB and its passage through Parliament when it is introduced in 2016. We agree with David Anderson QC that: "the road to a better system must be paved with trust".

With the publication of the IPB, for the first time, one document sets out the totality of the investigatory powers government thinks are necessary. Reform is overdue, and the IPB provides a foundation for open and meaningful debate. It's not going to be possible to please everyone in all aspects of these powers, but there's a tremendous opportunity now to build a much better new regime. We'll respond formally to the government consultation, but we've set out our initial opinion below.

The government's powers

All the powers in the IPB should protect the rights established in the European Convention on Human Rights (as implemented in the UK by the Human Rights Act 1998) and the European Union's Charter of Fundamental Rights. Bulk powers on interception, communications data and equipment interference – which are potentially extremely privacy–intrusive – should only be used in very rare circumstances, when all other capabilities have been considered.

Bulk interception is controversial. A UK court has said that the current rules are lawful and comply with human rights. David Anderson QC believes that government has shown it needs these powers for both content and communications data. Some privacy campaigners believe that bulk interception is too great an infringement of privacy in a free society. Our view is that government should be able to use bulk powers provided the pending legal cases uphold their validity, and that strong oversight means that they're only used when it's necessary and proportionate.

It would help to assess exactly what is and what isn't proportionate if there were more clarity on the word "bulk".

It could potentially be broken into separate categories – rather than used as a catch-all term for all warrants not falling into other categories.

The scope of any new power along the lines of section 94 of the Telecommunications Act 1984 should be more limited than it is now. It should also expressly give a right of appeal and be stringently overseen. The relevant clause in the IPB (national security notices) is a big improvement.

We think the position on powers to compel communications providers to keep third party data is unclear. Government has said publicly that it has dropped the idea, but it still seems to be permitted under the IPB. So far, no one has made a compelling case that these powers are necessary and proportionate.

Even though the new proposals making communications providers keep internet connection records aren't as extensive as those in the draft Communications Data Bill 2012, they still need carefully evaluating in terms of their proportionality feasibility and cost.

Subject to the right checks and balances, we see a strong case for communications providers being compelled to provide help as law enforcement and security agencies pursue suspected criminals, terrorists and threats from overseas. We recognise the IPB has removed some discretionary elements. But others are still there – notably on disclosing communications data. We intend to discuss this with government.

Content versus communications data

This is a tricky issue. Any new legal definitions must balance covering a broad range of factual circumstances with providing legal certainty. The IPB includes definitions of "content" and "communications data" that are supposed to cover all possible circumstances. The government will need to check very carefully that the new approach works, particularly with online communications. And they must make sure the most intrusive types of data attract the strongest legal protection before they can be accessed.

Secrecy

We understand some things have to be kept secret, but there should be a presumption in favour of openness. If things do need to be secret, the government should try to explain why, so far as possible without giving away crucial details to potential wrongdoers being pursued.

Government should be more consistent in how it tries to keep things secret or confidential. At present, there are too many separate restrictions. The IPB proposes a number of further restrictions.

Harmonising these various restrictions would help strike the right balance between necessary secrecy and transparency.

8 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf section 11.7, page 204

Oversight and transparency

Better oversight and transparency is crucial. Strong law, with clear checks and balances in place from the start of the process (authorisation) to the end (audit), should give everyone confidence that intrusive powers will only be used when necessary and that any interference with the right to privacy will be kept to a minimum. Regular review of the operation of the law, with input from stakeholders, is important to keep pace with change.

We welcome the proposed creation of the Investigatory Powers Commissioner (IPC) to provide independent oversight, with an expanded remit and greater resources. It should have full powers to disclose an accurate and complete picture of the total number of requests made which affect individuals.

We think that judicial authorisation is needed for more privacy-intrusive powers. So we're pleased that the IPB mandates this for all warranted activity. We believe there's a case for extending judicial authorisation to data retention notices and national security notices. But it's good to see that the IPB envisages that communications providers will have a direct right of review to the Secretary of State in both cases, and that the Secretary will have to take into account the IPC's views on proportionality. Equally, there is a case for extending the review mechanism to bulk warrants.

The IPC should stick to the same stringent standards whether assessing proportionality for authorisation or review.

Jurisdiction and extraterritoriality

This is another difficult area. Overseas providers offering services in the UK may be asked to disclose information in the UK. But such a request could conflict with their own country's laws.

In the future, an improved Mutual Legal Assistance Treaty process is the best solution. It could be along the lines of the international framework advocated by Sir Nigel Sheinwald. It would mean like-minded countries (with high privacy and human rights standards) would agree a single set of principles on disclosure that would apply to all participants. However, this isn't likely to happen soon – because those types of multi-state agreement take time.

In the meantime, the UK government should apply the new investigatory powers regime equally to all providers offering services in the UK – whilst acknowledging the difficulties of enforcement. We do not believe that government has made a compelling case that UK-based communications providers like us should keep data relating to other providers.

Scope

The rise of encryption is a good example of the challenge government faces in getting the new law right. Both David Anderson QC and the government believe there should be no "dark areas" in communications. Their worry is that if communications can't be decrypted, criminals and terrorists will be able to place themselves beyond the reach of the law.

On the other hand, encryption helps people communicate securely. It reduces the potential for cybercrime. It empowers free expression in countries without strong and independent legal regimes.[9] And there will sometimes be practical constraints on what a provider can do, for example if the data it carries has been encrypted by a third party.

This is a really difficult area. The technology is complex. The arguments on both sides are compelling; the debate is still evolving. Close engagement between government and industry will be key to finding a way forward.

> "the road to a better system must be paved with trust
>
> David Anderson QC

9 Noted by the UN Special Rapporteur on the promotion and protection of the right to free expression and opinion: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

SUMMARY OF PUBLIC BODIES' POWERS TO ACCESS DATA

	Communications data – Retention	Communications data – Disclosure	Interception
What law applies?	The Data Retention and Investigatory Powers Act 2014	The Regulation of Investigatory Powers Act 2000 Part I, Chapter II[i]	The Regulation of Investigatory Powers Act 2000, Part I, Chapter I
What powers are granted?[ii]	The Secretary of State has the power to issue a retention notice. Any such notice would oblige us to retain communications data for up to 12 months. The types of communication data we can be ordered to store are set out here: http://www.legislation.gov.uk/uksi/2014/2042/schedule/made	Various public bodies have the right to obtain communications data from us. The police and law enforcement agencies are the main users of this power (88.9% of requests), followed by the security services (9.8%) and local authorities (0.4%). There are a limited number of other users (0.9%)[iii].	The police, security services, HMRC, the NCA and defence intelligence have the power to intercept communications. Warrants target a single person or premises. There are a small number of "certified" warrants that allow much broader interception of external communications with persons outside the British Isles.
When can those powers be used?[ii]	A retention notice can be served by the Secretary of State.	The key purposes for which communications data can be obtained are if it is necessary for: (a) preventing or detecting crime or disorder (78.5%); (b) national security (15.0%); (c) emergency to prevent death or injury (6.0%); and (d) other (0.5%)[iv].	Interception can take place for a number of limited statutory purposes, for example preventing or detecting serious crime (68%), national security (31%) or a combination of these purposes (1%).
Is judicial approval needed?	No. However, a notice can only be served if it is necessary and proportionate.	No[v]. However, the request must be necessary and proportionate and issued by a senior designated person at the authority. Requests are processed by a specially trained individual known as a single point of contact (SPoC).	No. However, the interception warrant must be necessary and proportionate and signed by the Secretary of State (in urgent cases the Secretary of State can authorise a senior officer to sign a warrant).
What guidance is there?	The Home Office has issued a Code of Practice for the retention of communications data that sets out more detail of the use of these powers in practice.	The Home Office has issued a Code of Practice for the acquisition and disclosure of communications data that sets out more detail of the use of these powers in practice.	The Home Office has issued a Code of practice for the interception of communications that sets out more detail of the use of these powers in practice.
How often are they used?[ii]	There is no public information on how many notices have been served or their contents.	In the UK, there were 517,236 requests in total in 2014.	In the UK, there were 2,795 interception warrants in total in 2014. There are approximately 19[vi] "certified" warrants allowing interception of external communications.
Who oversees these laws?	The Interception of Communications Commissioner has been appointed to oversee compliance with the laws on acquisition of communications data and interception of communications. He produces a report every six months. The Information Commissioner oversees the security of retained communications data.		

i The government has also acknowledged it has used section 94 of the Telecommunications Act 1984 for bulk acquisition of communications data.

ii Unless otherwise stated, all figures in this section are taken from the Interception of Communications Commissioner's March 2015 Report and relate to the general use of this power, not requests to us.

iii The 0.9% of requests made by other authorities covers a wide range of entities such as the Financial Conduct Authority, Ofcom, the Information Commissioner and the Serious Fraud Office.

iv The 0.5% of other requests were: (a) in the interests of the economic well-being of the United Kingdom; (b) in the interests of public safety; (c) for the purpose of protecting public health; (d) for tax purposes; (e) in relation to a miscarriage of justice; (f) to identify a person unable to identify themselves; or (g) for a combination of these reasons.

v Note that judicial approval is needed for local authority requests or in relation to obtaining journalistic sources for communication data.

vi Figures from the Intelligence and Security Committee's report Privacy and Security: A modern and transparent legal framework, March 2015.

3 Free expression online

- We believe people should be free to access the legal content and services they want on the internet. It's essential for free expression.
- We support the Open Internet Code of Practice where we committed to providing "full and open internet access products" whenever possible, and to being transparent about the circumstances when we can't.
- Our activities in content blocking are limited to the provision of BT Parental Controls, blocking access to child sexual abuse images, complying with court orders, and protecting our customers or network from harmful traffic.
- We offer customers an "unavoidable active choice" for free BT Parental Controls. It leaves choice with customers and helps when it comes to educating people about how to stay safe online.
- We believe parents with children who engage proactively in the decision will be more likely to consider broader online safety measures beyond mere filtering. This is less likely with "default on".
- We take over-blocking of sites very seriously. We quickly look at concerns raised with us and rectify incorrectly blocked sites as fast as possible.

We believe people should have the freedom to access the content and services they want on the internet. Restrictions to this right should only be imposed in very limited circumstances – the rights people have offline should be available online too.[10]

In July 2012, BT signed the Open Internet Code of Practice where we committed to providing "full and open internet access products" whenever possible, and to being transparent about the circumstances when we can't. We've also committed to the Voluntary Industry Code of Practice on Traffic Management Transparency. As part of that commitment, we publish information about our how we manage traffic across our network.[11]

Sometimes, we block certain websites or "filter" content, even though we're only carrying that material across our network. These actions fall into four categories:

Customer choice –
we provide BT Parental Controls for our customers to choose (and filter) what content they can access on the internet. They might restrict access to pornography or social media networks, for example, or choose to limit access to certain content at different times of the day.

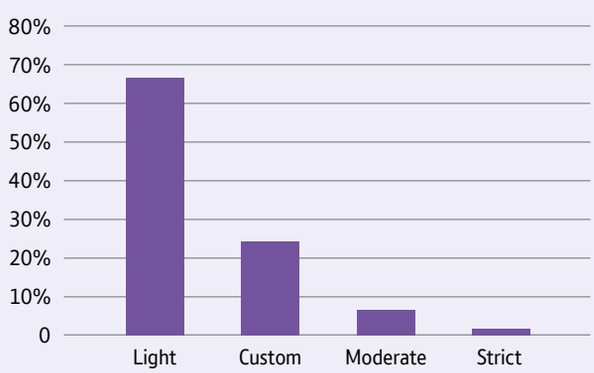
Child sexual abuse images –
we block or filter child sexual abuse images that the Internet Watch Foundation tells us about.

Court orders –
a court requires us, and other communications providers, to block access to content which infringes other people's intellectual property rights, like in films, music and videos.

Protecting our customers –
we may block harmful traffic – such as that generated by malware – which could harm our customers' computer systems and communications or affect our services.

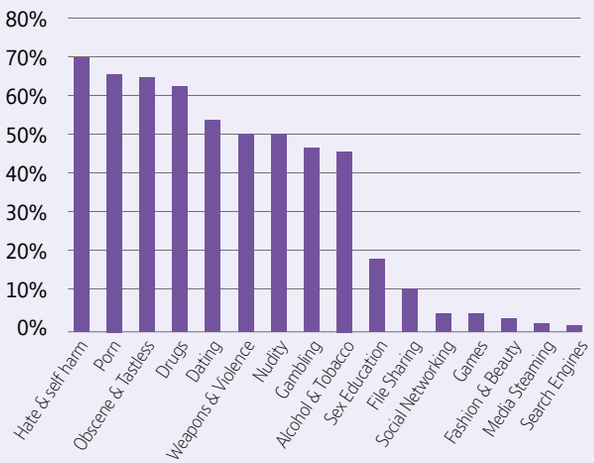
We consider with great care any requests or attempt to restrict our customers' use of the internet. We look at whether restrictions are proportionate and lawful. And we talk about these issues regularly with government and other stakeholders to influence the debate in a way that respects free expression.

Use of BT Parental Controls pre-defined filters



Source – BT Consumer as at 30 June 2015. This shows use of pre-defined filters by those customers who have chosen BT Parental Controls.

Use of BT Parental Controls custom filters



Source: BT Consumer – as at 30 June 2015

The BT Parental Control setup screen

Court proceedings were taken against us because we refused to block content when first asked to do so.[12] (It was alleged that the sites enabled copyright infringement.) We defended these proceedings, to clarify the law that applies when deciding whether content must be blocked. By doing this we've helped develop new processes that provide a fair balance between competing rights.

In 2013 and 2014, we also took part in the public debate about whether adult material online should be automatically blocked by default, with people wanting to access it having to switch off automatic filters. BT and other communications providers took the view that default-on filters (where the communications provider decides to block content in advance, and the customer has to choose to unblock it) would undermine the principle of freedom of access. We argued instead for a system where users have to make a choice about having filters switched on or off.

10 United Nations Human Rights Council resolution 20/8: The promotion, protection and enjoyment of human rights on the Internet

11 See our Key Facts Indicator which we publish as part of our commitment to the Voluntary Industry Code of Practice on Traffic Management Transparency for Broadband Services March 2011: http://bt.custhelp.com/app/answers/detail/a_id/47278/c/346/session/L2F2LzEvdGltZS8xMzg2OTU0MDUzL3NpZC9xamtpLUplbA%3D%3D

12 Twentieth Century Fox & oths v British Telecommunications [2011] EWHC 1981 ('Newzbin case'). This site provided a search engine facility to allow users to find and access music, films, apps and books.

3.1. Customer choice

We believe that our customers should be free to choose what legal content is accessible in their home and decide how best to keep their children safe online. We don't apply these controls by default. Instead we've invested significantly in processes to contact our customers so they understand their options and choose what, if any, filtering they'd like to apply. Customers can apply BT Parental Controls to any internet enabled device in their home.

What type of sites can be blocked?

BT Parental Controls give our customers the flexibility to decide which sites they want to block. We offer three pre-defined filtering levels – light, moderate or strict. The categories of content that get blocked vary according to the filtering level chosen.

We also offer a custom filtering level that lets customers choose which content categories to filter. They can then further personalise the filters, for example, by setting the time of day they're active or for parents to override the filters on a temporary basis or for a specific site in a category which a customer has chosen to filter. We give them the option to make their own choices. There's more information on the BT Parental Controls help pages.[13]

In very limited circumstances we put sites – like ChildLine – on a 'white list'. That means even a parent can't block access to them. We think this is vital to protect vulnerable children.

What's "unavoidable active choice"? Why do we support customers' active choice for BT Parental Controls rather than just turning them on by default for all customers?

Active choice for home-based parental controls is an approach that gives customers the maximum control over the content they access. It engages parents to make sure they actively consider the issue of online safety, which is a much broader issue than the mere application of filters. Over the past year we've invested to make sure our customer base has been asked whether or not they'd like to activate filters. An email verification of their choice is automatically sent to the account holder to confirm their decision.

People should actively consider the use of filters as well as the broad range of online safety issues and not have important decisions about their family's access to online content made for them. That's why we decided not to just apply our parental controls by default.

We also have concerns that it would be disproportionate to apply filtering by default to all of our customers.

Since only around 25 per cent of our consumer broadband customers live in households with children, it would mean the remaining 75 per cent would be treated like they needed protection from a whole array of online content.

Ofcom research[14] has highlighted that many parents choose not to apply filters – with many saying they prefer to use other ways to manage what their children see online. That said, we know that over a third of our broadband customers in households with children have chosen to use them. In fact, the percentage could be as much as 60 per cent when we include those customers who take our Net Protect product, which is a filtering tool and also blocks harmful traffic.

25%

of our consumer broadband customers live in households with children

36%

of those customers have chosen to use network or device level parental controls

~60%

of those customers have chosen network, device or security software parental controls

It would have been far cheaper and easier to simply switch on BT Parental Controls for all of our customers, but we think best practice is to let customers choose what's right for them and their family, even if at times that approach has meant more cost and effort for us.

In December 2013 we started a programme to contact all existing customers individually to make sure they engaged in the issues and made their own (unavoidable)[15] active choice about whether or not they wanted to apply the filters. By January 2015 all our customers had made their decision. Since then all new customers have to choose whether they want the filters when they first set up our broadband service and we proactively give the customer going through the set-up the information they need to make that choice.

Moreover, whilst parental controls are undoubtedly important, they are not a complete safeguard for children and certainly no substitute for education and awareness. Parents need to be actively involved in talking to their children about staying safe online and agreeing how they use the internet and social media. We think applying parental control filters by default does not encourage that proactive approach. To keep parents informed about online safety we helped set up Internet Matters in May 2014.[16]

In 2016, a new EU law (the Net Neutrality Regulation) will come into force. This will make sure that, subject to some limited exceptions, EU citizens will be able to access whatever online content and services they want, without any discrimination or interference. Government might then need to introduce national legislation to let communications providers carry on offering parental controls (or any similar tools). We would support the introduction of a new statutory framework to remove the possibility of a challenge to the current voluntary scheme.

13 http://bt.custhelp.com/app/answers/detail/a_id/46768/c/7338,7388,7390

14 http://stakeholders.ofcom.org.uk/binaries/internet/third_internet_safety_report.pdf

15 We used different methods, including emails and web browser messages to make sure customers were faced with an unavoidable choice and had to choose between having BT Parental Controls switched on or off.

16 BT worked with other communications providers to create Internet Matters which is an organisation with three goals: to promote awareness of parental controls; to encourage parents to stay up-to-date about online safety; to promote discussion with young people about staying safe online.

How do we choose the categories for our parental controls?

We talk with various stakeholders – parent groups, government, other communications providers and customers – about how we categorise, as there are no specific rules or guidelines that say how we should approach it.

We aim to be consistent and non-discriminatory at all times and, in keeping with our commitment to an open internet, we see blocking access to content as the exception, not the rule. We use expert third party companies which create the categories and review them frequently to make sure all sites are categorised appropriately.

Given the fast-paced nature of the internet, there are a small number of sites that sometimes may be blocked incorrectly ("over-blocked") and need to be re-categorised. We have a dedicated email address (categorisation@bt.com) that our consumer customers can use to report any queries.

If we get a complaint that a site has been incorrectly blocked, we'll work with our specialist filtering supplier to review the site and provide a response as quickly as possible, but no longer than seven days. On the few occasions where the person raising the query has questioned the decision, we've held a detailed joint review of the site to reach the final outcome.

Between December 2013 and December 2014, we got 609 reports that sites were wrongly categorised. Following investigation, 26 per cent of them were re-categorised and the rest stayed the same. That's a very small rate of reported incorrectly blocked sites given that in the same period the 'this site is blocked' message was shown (on average) 17,000 times a day.

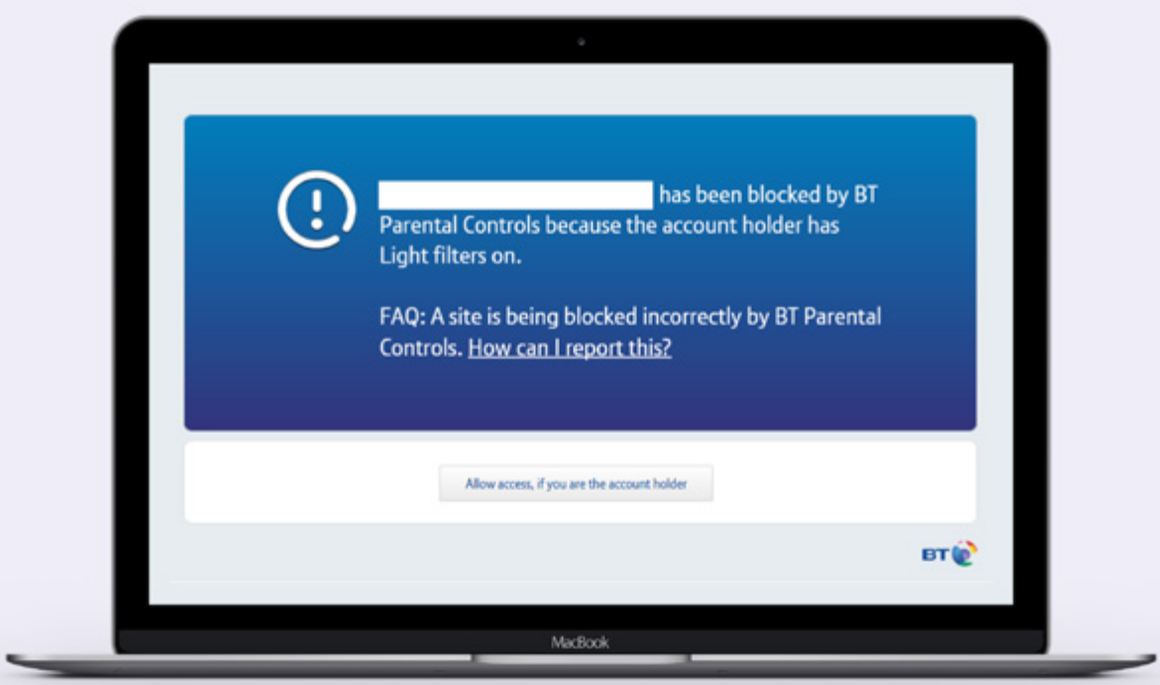
Do parental controls impact free expression?

The concept of restricting access to what children can see isn't new – it's existed for film, video and television content for many years, like age restrictions and the 'watershed' hour.

We note the Government's proposals to introduce mechanisms to restrict under 18s' access to pornographic websites and agree that what's illegal offline should also be illegal online. Measures to tackle the problem should be carefully targeted to make sure that only the sites in question are subject to appropriate controls, and that any unintended blocking of legal material for children and adults is minimised.

What happens if someone attempts to access a site blocked by parental controls?

They'll see a web page message that tells them the site is blocked because BT Parental Controls are on. The message confirms the site they're trying to access and the filter level that's been picked. It looks like this:



The screen that is shown when a website has been blocked by BT Parental Controls

What are the categories and what sort of sites go in them?

The different categories, and the type of site which might go in them, are set out below. Because of the nature of the categories, some of the sites we block under the different categories might also include material which could be unlawful. Find out more about this on page 22. This is how we allocate the categories across the different filter levels. But there's always the choice to allow a particular category or even a specific website within a chosen filter level.

Blocking category	Description	Light	Moderate	Strict
Pornography	This category will block sites that contain explicit sexual content. This includes adult products such as sex toys and videos, adult and escort services, strip clubs, erotic stories and descriptions of sexual acts.	⊘	⊘	⊘
Drugs	This category will block sites that give information on illegal drugs or misuse of prescription drugs.	⊘	⊘	⊘
Alcohol & Tobacco	This category will block sites that promote or sell alcohol or tobacco related products or services.	⊘	⊘	⊘
Hate & Self-harm	This category will block sites that promote or encourage self-harm or self-injury. The category also includes sites that encourage the oppression of people or groups based on their race, religion, gender, age, disability, sexual orientation or nationality.	⊘	⊘	⊘
Nudity	This category will block sites that contain full or partial nudity. The content blocked will not necessarily be of a sexual nature. This will include sites where the main purpose is to advertise or sell lingerie, intimate apparel, or swimwear.		⊘	⊘
Weapons & Violence	This category will block sites that encourage suicide or depict, sell, review or describe guns and weapons. This could be for sport or sites that contain images or text depicting or advocating physical assault against humans, animals, or institutions. Sites where the content is of a gruesome nature will be blocked.		⊘	⊘
Gambling	This category will block sites that offer or are related to online gambling, lottery, casinos and betting agencies involving chance.		⊘	⊘
Dating	This category will block sites that promote networking for interpersonal relationships such as dating and marriage. This includes sites used for m atch-making, online dating, spousal introduction and escort services.	⊘	⊘	⊘
Social Networking	This category will block social networking sites used for friendship, dating, professional reasons and other various topics. It will also block sites used for online chat, like chat rooms and instant messenger sites.		⊘	⊘
File Sharing	This category will block sites used to illegally distribute software or copyrighted materials such as movies, music, software cracks, illicit serial numbers, illegal license key generators and sites used as a direct exchange of files between users.			⊘
Games	This category will block sites relating to computer games, online games or other games. This also includes sites that provide information about game producers, or how to obtain cheat codes. This will include blocking access to online multiplayer gaming servers and online app stores.			⊘
Media Streaming	This category will block sites that deliver streaming content, such as Internet radio, Internet TV or music. It will also block sites that provide live or archived media downloads. Fan sites or an official site run by musicians, bands, or record labels will also be blocked.			⊘
Obscene & Tasteless	This category will block sites that may be offensive or tasteless such as bathroom humour, or gruesome or even frightening content such as shocking depictions of blood or wounds, or cruel treatment of animals. It also blocks sites which offer advice on how to commit illegal or criminal activities, or to avoid detection. These can include how to commit murder, build bombs, pick locks, etc. Sites with information about illegal manipulation of electronic devices, hacking, fraud and illegal distribution of software will be blocked.	⊘	⊘	⊘
Fashion & Beauty	This category will block sites that relate to the advertising and discussion of fashion, jewellery, glamour, beauty, modelling, cosmetics or related products or services. This will also include sites where the main content contains fashion and beauty product reviews, comparisons, and general consumer information.			⊘
Homework	'Homework time' provides an additional layer of protection over and above day-to-day filters. This can be set to turn off/on according to the times customers specify. Homework time will block social networking, gaming and cheating sites in addition to the usual controls.			
Search Engines & Portals	'Search Engines and Portals' will block sites where the main purpose is to enable the searching of the web, newsgroups, images, directories and other online content. Includes portal and directory sites such as white/yellow pages.	Personalise only		
Sex Education	This category is intended to prevent very young children from being exposed to sites that have a significant focus on subjects that might come up in a sex education programme. Parents should carefully consider the possible adverse effects from denying children of an appropriate age access to information on these issues.	Personalise only		

Do we limit access to online material outside the home?
Our consumer broadband customers can use BT Parental Controls to make their choice about what content is available in their household. Those choices will automatically be applied when they access the internet outside the home in the UK if they log in to the BT Wi-fi service using their BT ID.

Of course people can also access the internet when they're outside their home using other public wi-fi services in shops, cafes and travel hubs. The BT Wi-fi service offers commercial public wi-fi services to businesses which might be in charge of those types of premises.

When we do that, we make it clear in our terms and conditions with those businesses that we automatically block access to adult pornographic content. We do that because we think there's a risk that children, unsupervised by adults in those public places, could end up seeing this material. But, under the terms and conditions, our site-partners can ask us to unblock access to that content as they're more familiar with the way the service will be used, and the associated risks. The settings chosen by those businesses are prioritised over any parental control choices made by an individual user accessing that public wi-fi service using their BT ID.

We don't automatically block access to any content when we provide BT Wi-fi as a part of our business broadband services. That's because this service is designed to be used on business premises where we wouldn't expect children to be present. The person signing up for the service must be over 18. If that business does share the use of their wi-fi with people coming on to their premises, we ask them to take responsibility for any filtering of online content.

We're also an associate signatory to the UK Code of Practice for the Self-Regulation of Content on Mobiles. This means we support and comply with the code's requirements which cover, among other things, the filtering of content classified as 18+ behind access controls requiring age verification.

BT has a strong history of commitment to improving online child safety

	1996	BT founding member of Internet Watch Foundation
BT develops world's 1st system for blocking online child sexual abuse images (Cleanfeed)	2004	
	2008	UK Council for Child Internet Safety established – BT joins
ISP Code of Practice for adult content filters agreed / BT sign up BT launches Parental Control (device level)	2011	
	Mar 2013	BT Wi-Fi Protect launched that allows Wi-Fi partners to restrict access to pornographic material
BT 1st to launch enhanced webpage served when attempt to access online child sexual abuse images. Acts as greater deterrent and provides information where people can find counselling	Jun 2013	
	Dec 2013	BT Parental Controls launched to all broadband customers
BT and other major communications providers launch "Internet Matters" a web portal to help children stay safe online BT and Unicef launch "Right Click" online safety campaign for children	Spring 2014	
	Nov 2014	BT and Marie Collins launch "Click: Path to Protection" programme to help online child sexual abuse victims
100% of all broadband customers presented with "active choice" asking if they want to activate BT Parental Controls	Jan 2015	
	Oct 2015	"Right Click" campaign delivered online safety workshops to almost 5,000 parents, teachers and children in 175 UK schools

3.2 Child sexual abuse images

We automatically block access to child sexual abuse images. Our customers don't have to take any action to block these images – nor can they unblock access to it. We're not directly required by law to block child sexual abuse images, but we consider it's legitimate to take this action as it prevents the commission of a crime – the viewing of a child sexual abuse image. We do this voluntarily to protect children.

We were the first communications provider to develop technology to block these images when we introduced our blocking system, Cleanfeed, in 2004. Since then, almost all other communications providers in the UK have introduced similar technology. It's also been adopted in other countries around the world, too.

Who decides which images are blocked?

The Internet Watch Foundation (IWF) gives us a list of images to block. There are around 1000 – 3000 blocked images on their list at any one time. For understandable reasons, the list of blocked images isn't publicly available.

The IWF has detailed procedures it uses when deciding which images should be blocked. There's an appeals procedure against its decisions.

How effective is Cleanfeed?

We don't claim Cleanfeed solves the problem of access to this kind of material. Determined people wanting to find child sexual abuse images can often find ways around blocking mechanisms. But Cleanfeed does help prevent inadvertent access, so cuts the number of successful attempts to access these images overall.

What happens if there's an attempt to access a blocked site?

Until 2013, people attempting to visit blocked sites or images were shown a 404 page error indicating they'd not been found. In 2013, we changed our approach. Today we display a web page explaining that the site contains illegal child sexual abuse images and offering links to counselling services.

This change of approach was significant. Since we introduced Cleanfeed, public concern about online images of child sexual abuse has grown. The new web page acknowledges that some people try to access this material deliberately. The generic message might alarm people who don't intend to access the material. But it's vital we deter people accessing child sexual abuse images. In doing so, we help protect children.

What information do we collect about access to child sexual abuse images?

Using Cleanfeed, we record the number of times we block access to these types of images.

But these statistics can't tell the difference between the deliberate and the accidental. For example, someone might click on an email link not realising it points to child sexual abuse images. On top of that, the email might automatically try to connect to these sites, possibly multiple times, to show hyperlinked images.

From the end of January 2015 to early November 2015, the average number of attempts to retrieve an image of child sexual abuse notified to us by IWF was 36,738 every 24 hours.

What should happen in the future?

By introducing Cleanfeed in 2004 we've played a vital role in blocking access to child sexual abuse images. We are proud of that. But it's helpful to reflect on how we might improve the existing model – to keep it fit for the future.

Under the Protection of Children Act 1978, taking, making, showing, distributing, or possessing with a view to distributing indecent photographs of children is a crime. This is a very important statute in terms of the IWF's assessments. But there's currently no law forcing us or other communications providers to block the child sexual abuse images they identify; we do this voluntarily to protect children and cut crime.

There have been no legal challenges to the IWF model (not surprising, given the nature of the material). But the IWF is a registered charity funded by the EU and the online industry. (We were among the co-founders and are one of the many members which contribute to its running costs.) Despite its expertise it has no official standing to determine whether or not material is unlawful; its blocking list is not decided by any judicial authority.

Where blocking is done by "interception" strict legal rules apply. This is how Cleanfeed works. So this voluntary blocking activity could in principle pose a legal risk for us under those rules. (Although in reality we're comfortable we're within the law because we're seeking to make the web safe for everyone and prevent crime.)

There's a small chance that on occasion some of the material we block may be legal. We may face complaints, or even legal challenges, as a result. On balance, we're happy to take the tiny risk of legal action over our responsibility to protect children.

Nevertheless, we think the current voluntary blocking system could be strengthened by giving it legal force. The work of the IWF is really valuable in setting an internationally-agreed benchmark for judging unlawful material. Few would disagree with that. But a new scheme which gave legal force to the IWF's assessment of materials, alongside compulsory blocking, would reassure everyone that all blocked material was illegal and make all communications providers participate.

Could the IWF approach be used for other types of content, such as extremist material?

Behind every image of child sexual abuse is a grave offence against a child. Publishing or possessing these images is illegal. Other online content on subjects like extremism and radicalisation may of course be similarly reprehensible, but they're often trickier to pin down as unlawful.

The content in question could be open to interpretation. People could have different views on its potential impact and so its lawfulness. Or it could be that the only way to judge the content would be to analyse the intentions of the person who created it.

So, it's complicated. For example, it's an offence under the Terrorism Act 2006 to publish or disseminate, intentionally or recklessly: "a statement that is likely to be understood by some or all of the members of the public to whom it is published as a direct or indirect encouragement or other inducement to them to the commission, preparation or instigation of acts of terrorism".

We provide a reporting button for our customers to alert the Counter Terrorism Internet Referral Unit of any terrorist material online. But it won't always be clear whether material is illegal in this context. The decision would likely need a close look at the words, images and overall impact of the content. That kind of judgement is always going to be subjective in a way that assessing an image of child sexual abuse isn't. Communications providers should not be the people making these judgements.

Furthermore, there's no body with the right standing (like the IWF) to define the boundaries between lawful and unlawful content. And where there's doubt, the tendency might be to over-block material, infringing people's right to free expression.

How do we currently deal with extremist/radicalisation material?
We don't automatically block it. But lots of it will be filtered out by the parental controls we offer our consumer customers.

If someone tells us about this type of content, we use a specialist firm to quickly help us assess the content and determine if it should be blocked. If we agree with the person flagging it to us, we include it on the blocked sites list within the relevant category in BT Parental Controls. There is no expert body or guidance on how to deal with this. We don't make a legal assessment of the material because we have no legal authority to do so. But we believe this approach makes us less likely to infringe the right to free expression – because whatever we put into one of the categories within our parental controls, it is the customer who decides for him or herself whether to apply parental control filters.

We follow the same steps regardless of who raises a concern. Adopting our standard process, we have in the past reviewed content from a list of material which in the view of the police was unlawfully terrorism related. Some of this content was already on our list of blocked sites in BT Parental Control's filters – under categories like hate and self-harm, social networking or media streaming. After looking more closely at the other sites, we added many to the Hate blocked list under BT Parental Controls.

There's no perfect solution. BT Parental Controls is not without challenges and compromises when it comes to blocking potentially unlawful material. However, it's a pragmatic solution for a difficult issue with no clear external processes, and one which allows us to pay due regard to the right to free expression.

How will this material be dealt with in the future?
The government and media have called for the internet industry to help tackle extremist content because of the serious threat it poses to UK security. In its recently published "Counter-Extremism Strategy", the government said that communications providers play a critical role in tackling extremist content online.

We understand the government's concern. But there's a limit to what communications providers can do as the extremist material is not always easily or accurately identified and much of this material is on encrypted social media sites that our filters can't easily block. Even when we can block it, content can often quickly reappear on another website.

One suggestion is to strengthen communications providers' Ts&Cs to choke off extremist material.[17] We don't think that's a workable approach. Quite aside from the inherent difficulty in deciding what's "extremist", Ts&Cs will inevitably end up varying from provider to provider. We need a better understanding of the role and function we and our peers in the social media industry play or we could end up straying into an inappropriate situation where corporations are asked to make decisions about people's legal rights.

Any exceptions to the principle of open internet access must be clear and consistent. They should be under a transparent legal framework. There should ideally be a better, independent, legal process to evaluate this type of material and to decide what content should be taken down or blocked, with independent oversight to check requests, on behalf of the general public.

These safeguards are vital when looking at content the impact of which, by its nature, needs carefully weighing up. A court process – like the one we helped establish for blocking access to copyright infringing sites – could work for requests to remove or block access. That way, an expert and independent court makes judgments on what's legal and what's not.

Or an independent and expert body could be empowered to make binding decisions (subject to certain caveats) on illegality. This could work on similar lines to our proposed model for assessing and blocking child sexual abuse images.

Either of these routes would possibly require new legislation. But even voluntary arrangements for automatically blocking intrinsically unlawful material could need a legal framework (because of the Net Neutrality regulation).

This framework would have to consider proportionality, and be in place by December 2016, as required under EU law. And ideally the processes for blocking child sexual abuse images would also be formalised with legislation to remove any residual doubt about their legality.

3.3 Court orders

Some websites can be unlawful because they damage the private rights of individuals. The sites may be using (or providing access to) content such as music, film and videos without permission from the owners – thus infringing intellectual property rights. We don't automatically block access to this content. We need evidence of people's property rights before we block something. That's why we helped establish a formal process where a court decides if access to a particular piece of content should be blocked.

Why don't we automatically block access to this material?
We are strong believers in intellectual property rights. They help promote a vibrant creative sector in the economy. But we also believe that limiting the right to access content online should only be done with a clear legal mandate (unless the customer has requested or consented to limited access).

That's why we refused to block the Newzbin2 site voluntarily when the copyright owners asked us to. Then in 2011 they brought court proceedings to compel us (but not other communications providers) to block the site. So we decided to bring a defence against the claim so that a court could consider the issues. It was the first case of its kind. We couldn't be sure Newzbin2 was infringing copyright, and if so whether it was the whole site or only part. Nor could we be sure we needed proof that our customers were already accessing and downloading that material without permission before we blocked general access.

What was the result of the legal challenge?
Although we attracted criticism, we believe it was right for us to defend the claim. We wanted to be sure that the restriction on people's access to the material was objectively justified and clear. We believed a court should decide what level of infringement meant that access to a site should be blocked. It was important to establish a process for any future similar requests from copyright owners.

As a result of that case, we know now that we don't need to know about specific illegal acts by our customers before we can be forced to block access to these sites. It's also clear that copyright owners should first seek alternative solutions before forcing us to block access to content.

Since the court made the position clear, we've been driving for an agreed process with copyright owners. For example, we insist that they make a court application, to protect our customers' rights and our own position. However we do take a measured approach: if a court's already decided that we must block access to a site, we don't make copyright owners make another court application for each website address that is derived from it.

17 HM Government, Counter-Extremism Strategy, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/470088/51859_Cm9148_Accessible.pdf 67

Does this process apply to other intellectual property rights?
We believe so, but the position is not yet fully clear. Cartier brought a court action in 2014 trying to extend the scope of the regime from copyright infringement to infringement of other types of intellectual property (like trademarks). We and other communications providers challenged it to get the court's view on when to limit access to this type of material. Because of the lack of clarity in the court's initial judgment, we have together brought an appeal, which is likely to come before a higher court in 2016.

Why do we take these issues to court?
We don't take court action lightly. But when it comes to restricting people's right to free expression it's the right thing to do because it makes sure actions are proportionate and based on a clear legal framework.

It's for this reason we went to court for clarity on the Digital Economy Act 2010 when it was brought into law.

The Act would potentially have made us restrict access to content and provide lists of our customers infringing copyright to copyright owners. Together with TalkTalk we needed to better understand the basis for this law. We needed to test whether it struck the right balance between privacy and competing property rights.

Whilst the case itself was unsuccessful, it prompted government to work with us, other communications providers and rights holders to implement an alternative scheme, Creative Content UK. We think this provides a better balance between the interests of copyright owners and customers, as well as helping educate people about online copyright infringement.

What happens if someone tries to access a site blocked by a court order?
If someone tries to access a blocked site, they get this message:

"Access to the websites listed on this page has been blocked pursuant to orders of the high court. More information can be found at www.ukispcourtorders.co.uk".

How many sites are blocked in this way?
All the sites blocked by court order are listed at www.ukispcourtorders.co.uk.

We don't routinely maintain data on the number of attempts to access these sites. We don't think those statistics would reflect the number of people intentionally trying to access those sites. (For example, automated software running on customers' machines might generate multiple access attempts.) Although we don't routinely keep records of the number of attempts to access barred sites, we did look at the period between March and July 2015, and noted that the number of attempts to access these sites averaged 375,000 per 24 hrs.

3.4 Protecting our customers

People have the right to free access to content online. But malicious software can cause someone's computer to act without their knowledge. So with the changing digital threat environment in mind, we are continually looking for ways to protect our customers from these types of threat to their systems and communications.

How does this happen?
People often accidentally install malicious software on their own computers. This lets it control their computer. Hackers use malicious software not only to take personal information from a computer but to use it to attack other computer systems and websites.

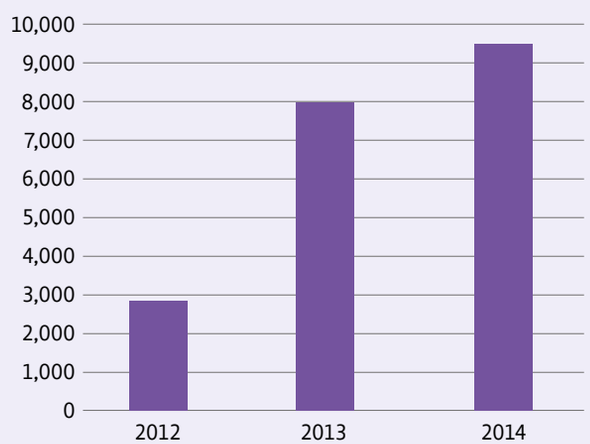
We develop and test technologies continually to protect our customers against such online crimes – usually by disrupting communications between the hacker and the computers they've compromised. We don't believe this infringes rights to privacy or free expression. Our customers wouldn't intentionally be sending such communications to illegitimate sites which our security analysts know are associated with malware. And by blocking these communications, we may stop criminals getting hold of our customers' personal information or attacking other people.

What else do we block?
If we think criminals are using a computer, we may block some traffic from it to protect our network and our customers. Again, we don't believe this infringes rights as our customers won't have sent these communications intentionally.

We also take action to block 'phishing sites' which falsely impersonate BT, often with a view to extracting personal details from our customers. The sites are almost identical copies of our BT website but they link to third party sites, so we know they aren't genuine. Phishing is on the increase: in 2014 we took action to close 9,442 phishing sites.

How can I protect myself online?
Technology gives some protection against viruses and wider online criminal threats. Our help pages[18] have lots more information to help people stay safe online. BT Protect – free to all our consumer broadband customers – helps protect their equipment from viruses, scams and phishing attacks by warning them if they're about to visit a potentially harmful website. Once BT Protect is switched on, all devices on the customer's broadband connection will be protected when on the internet. It will also work when they are out and about in the UK and using their BT ID to log in to BT Wi-fi.

Phishing Sites Closed by BT



Source: BT Security.

18 http://www.bt.com/help/home/security.html

4
Where next?

In these pages, we've explained how we are helping to encourage the debate and shape the law relating to our most significant potential effects on human rights – privacy and free expression. We believe that any limitations of those rights must be within a clear legal framework, with the right checks and balances.

Our commitment to free expression is reflected in our approach to "active choice" for parental control tools. It's also highlighted by our request to have the courts scrutinise the Digital Economy Act 2010 and the processes for blocking content which might infringe copyright. We've suggested that voluntary processes for blocking child sexual abuse images online should be formalised. We have recommended improving the safeguards for blocking content which might be extremist or lead to radicalisation.

We have outlined the current investigatory powers regime and the crucial part we play when government exercises these powers – which are necessary to protect national security and fight serious crime. Protecting our customers' private data is central to what we do, so our internal governance processes and dialogue with government will continue to focus on this. We also highlighted our early views on the IPB; we will make a more detailed submission to the government consultation shortly.

Where next? Privacy and free expression go hand in hand. We welcome the public debate on both.

And, of course, part of that is examining the role that communications providers like us should play.

December 2015

Glossary

Anderson Review	'A Question of Trust – Report Of The Investigatory Powers Review' David Anderson QC, Independent Reviewer of Terrorism Legislation June 2015
CJEU	Court of Justice of the European Union
DRIPA	Data Retention and Investigatory Powers Act 2014
IOCCO	Interception of Communications Commissioner's Office
IP address	Internet Protocol address (the number assigned to a device communicating over the internet)
IPB	Draft Investigatory Powers Bill
IPC	Investigatory Powers Commissioner
IPT	Investigatory Powers Tribunal
ISC	Intelligence and Security Committee
ISIC	A new Independent Surveillance and Intelligence Commission
RIPA	Regulation of Investigatory Powers Act 2000
RUSI	Royal United Services Institute
UN Guiding Principles	UN Guiding Principles on Business and Human Rights

BT Group plc
Registered office: 81 Newgate Street, London EC1A 7AJ
Registered in England and Wales No. 4190816
Produced by BT Group
Designed by mslgroup.co.uk

www.bt.com