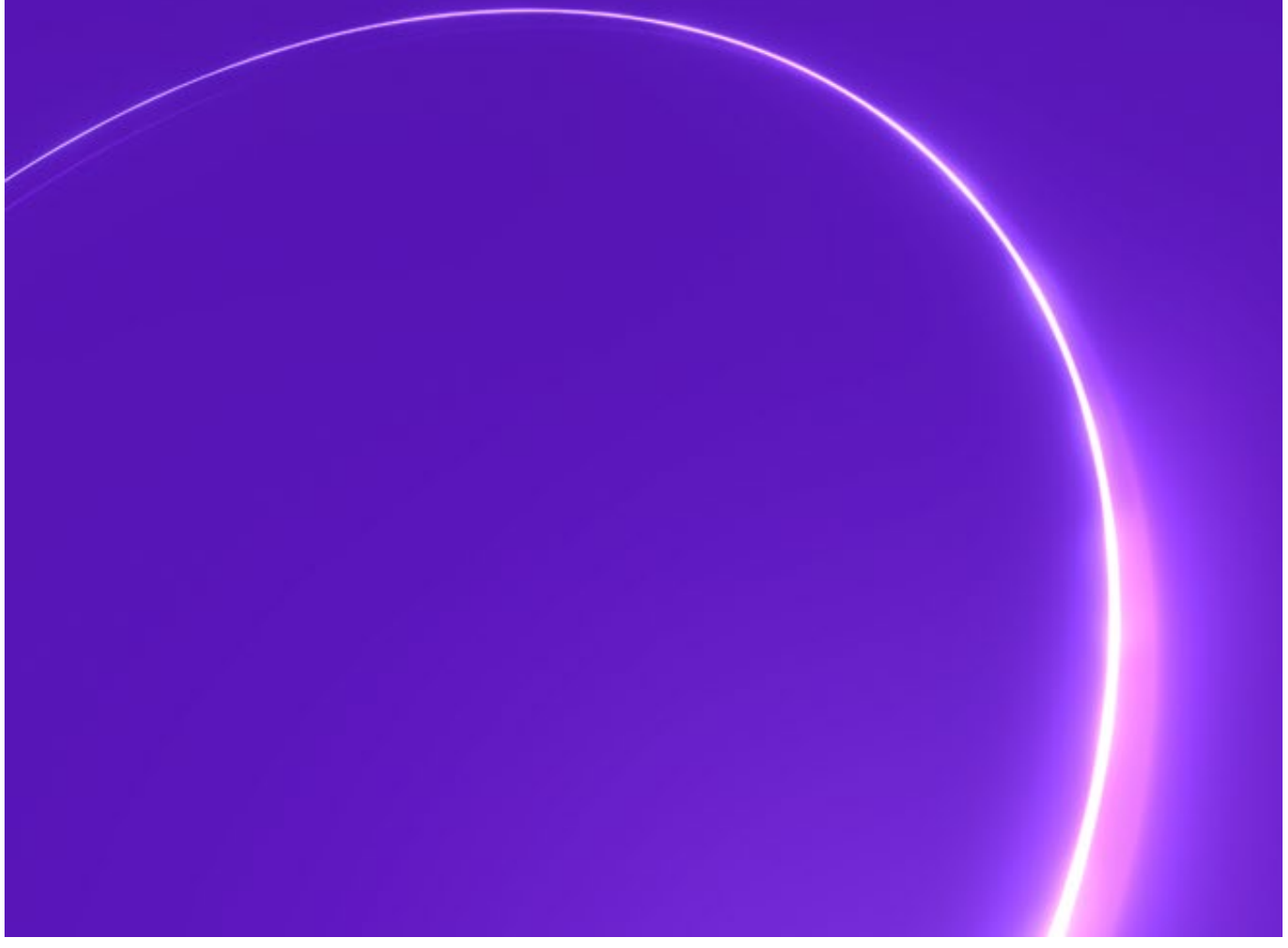
UK and Global Legal Information



UK Legal Information

This page has information on UK laws that apply in the area of privacy and free expression. It also includes details of some of the relevant court cases.

The Investigatory Powers Act 2016

The Investigatory Powers Act 2016 (IPA) became law in December 2016. It brings together nearly all the areas in which the government can ask for help from communication service providers like us, and includes some new safeguards compared with the old law.

We played an active role in getting this Bill passed. We made written submissions about the proposed content of the law, for example suggesting changes to the wording or commenting on appropriate safeguards. We also gave oral evidence to the House of Commons Select Committee.

The IPA is currently subject to a government review and there are expected to be some changes proposed within 2022. Currently it deals with government powers in the following main areas:

1.1 intercepting the contents of a communication

1.2 interfering with equipment (this generally refers to "hacking")

1.3 acquiring and disclosing communications data

1.4 keeping communications data

1.5 bulk acquisition warrants for communications data

Here is some more information on each of these and how things differ from the previous regime.

1.1 Intercepting the contents of a communication

The content of a communication can include:

- What's said in a phone call
- What's written in an email or text message
- A full URL or specific page of a website (see below)

Intercepting communications happens in 'real time'. Interception powers are potentially very intrusive. So authorities can only use them for limited purposes – mostly for national security or for preventing or detecting serious crime. Only a small number of public bodies (like the Intelligence Services and the police) can use these powers.

Authorities can apply for interception warrants which are targeted at a specific person or group of people, an organisation or premises. They can also apply for bulk warrants, which don't refer to a specific person or premises. The main purpose of these must be to intercept communications sent to or from people outside the British Islands. Only the intelligence agencies can apply for a bulk warrant.

'Bulk' isn't defined, either in the context of interception or of other capabilities. This means a bulk warrant covers a very broad area. So it could be anything from a small set of content, data or equipment to potentially a very large one.

The Secretary of State issues warrants, but in a radical change from the Regulation of Investigatory Powers Act (which governed interception before the IPA), these must also be authorised by a judicial commissioner, who is an independent senior judge. Commissioners are appointed to the Investigatory Powers Commissioner's Office (IPCO), a new body which oversees the use of powers under the Investigatory Powers Act. This process has been described by the government as a 'double-lock', adding an independent, judicial safeguard.

1.2 Interfering with equipment

The Investigatory Powers Act is the first time UK law has clearly outlined powers relating to equipment interference. It gives authorities the power to interfere with any equipment so that they can obtain communications, equipment data or any other information. The Act doesn't define 'interference' but

this probably includes listening, tapping, storing, monitoring, and scanning. So, for example, the Investigatory Powers Act allows authorities to access devices like smartphones, routers, servers, computers or tablets (commonly known as "hacking").

Like interception warrants, equipment interference warrants can be targeted or bulk. As they're potentially very intrusive, authorities can use them primarily for national security or for preventing or detecting serious crime.

The process for issuing and approving them is almost identical to the one for interception warrants. The only significant difference is that in limited circumstances, certain senior police officers can issue targeted warrants. These must also be approved by judicial commissioners.

1.3 Acquiring and disclosing communications data

Communications data is information that describes the sender and recipient of a communication and how, when and where it came from and went to. It is essentially everything except the actual content (or meaning) of a communication. Communications data includes domain names up to the first 'slash'. So, for example, 'www.bbc.co.uk' is defined as communications data. But in the URL 'www.bbc.uk/sport/football', "sport" and "football" give more detail about the material someone's accessed, and are classed as content.

The Investigatory Powers Act gives public authorities the right to make communications service providers give them access to communications data. This includes the Department of Health, the Health and Safety Executive and HMRC. This is fewer public authorities than under the Regulation of Investigatory Powers Act. They can ask for communications data for lots of different reasons, including to protect public health or safety and for tax-related purposes.

If one of these authorities asks us we must give them data that we keep for our own business reasons and data that we're made to keep through a compulsory retention notice (there's more information on these below). They can also make us collect and provide data we don't already have, but can get.

When a public authority wants to obtain communications data, it must apply for a notice or authorisation. Under the Regulation of Investigatory Powers Act, authorisations could be granted by senior officers in these public authorities. This has changed with the Investigatory Powers Act. A judicial commissioner must approve an application for an authorisation, unless there is an urgent need to obtain the communications data, or the authorisation is granted by the Intelligence Services for reasons of national security. The Investigatory Powers Commissioner has set up the Office of Communications Data Authorisations (OCDA) to deal with these applications.

1.4 Keeping communications data

Communications service providers can be made to keep communications data that we might not normally keep for up to 12 months. To do this, the Secretary of State issues a retention notice, which a judicial commissioner must approve. The Secretary of State must consider that it's necessary and proportionate to keep the information obtained for one or more of the broad range of purposes allowed under the Act, including for the prevention or detection of crime or in the interests of national security.

The Investigatory Powers Act added a new category of information that communication service providers can be made to keep – internet connection records. These show when and how someone has connected to the internet from a device, but not the content they've looked at. So for example, they could show apps someone has used or websites they've looked at, but not content (as mentioned above, this is only the domain name up to the first 'slash'). Communications service providers don't normally generate and keep this information, so this is a significant development.

There have been a number of legal challenges around the UK's powers to make communications service providers keep data, which also affect other so-called 'bulk' powers under the IPA (see below).

1.5 Bulk acquisition warrants for communications data

Although they're called 'acquisition' warrants, these are actually used to make communications service providers disclose communications data in bulk to the warrant holder. As with all other warrants,

they're issued by the Secretary of State and approved by a judicial commissioner. Only the intelligence agencies can apply for these but only on the grounds of national security or serious crime.

This particular power has not been clearly set out in a law before. But in 2015 in the *Privacy International* case (see below) the government said that it had previously used it under section 94 of the Telecommunications Act 1984.

Our legal obligations under the Investigatory Powers Act

Communications service providers are legally obliged to take all reasonable steps to comply with and help implement the powers in the IPA.

Technical Capability Notices

These underpin all the powers described in this section **except retention notices**. They can be used to make a communications service provider change their systems and products so they can deliver any of the activities described above.

National Security Notices

These can make a communications service provider take 'specified steps' in the interests of national security. They can't be used to make us do something that could be carried out under another section of the Act by issuing a warrant.

Both Technical Capability Notices and National Security Notices must be issued by the Secretary of State and approved by a judicial commissioner.

The Investigatory Powers Commissioner

The Investigatory Powers Act requires the Prime Minister to appoint an Investigatory Powers Commissioner responsible for reviewing public authorities' use of investigatory powers. They also appoint judicial commissioners to the investigatory powers commissioner's office. Sir Brian Leveson was appointed as the commissioner in 2019. And, to date, 14 senior judges have been appointed as judicial commissioners. When it is fully up and running, IPCO expects to have around 70 staff, including inspectors, lawyers and technical experts.

The Watson case

Watson is an important case which challenged the Data Retention and Investigatory Powers Act 2014, which was replaced by the Investigatory Powers Act in 2016. At the end of 2016, just as the Investigatory Powers Act became law, the Court of Justice of the European Union gave its judgment in this case.

It found that:

a) Indiscriminately retaining communications data goes against EU law. Keeping data like this must be objectively justified and targeted, for example, to particular people or a geographic area. This is tricky to understand. For example, if someone committed a serious crime, communications service providers could be forced to keep data for everyone living in that area, even if it's a very large area; this could still be 'targeted' if it had been objectively justified.
b) A court or independent body must authorise access to data (except in urgent cases).
c) Authorities must tell anyone whose data they've accessed as long as it doesn't jeopardise an investigation.
d) Retained data must be held within the EU (this no longer applies to the UK following Brexit).

When the government drafted the Investigatory Powers Act, it didn't anticipate the full extent of the outcome of the *Watson* case. There have been new legal challenges asking the courts to look at whether the Investigatory Powers Act is compatible with the *Watson* case (see below).

After the judgment

Since the judgment, the courts have continued to debate the *Watson* case, in particular in the following two cases:

• *Privacy International* – this challenged the power of intelligence agencies to acquire bulk communications data and collect bulk personal data sets in the Investigatory Powers Tribunal, a special court set up under the Regulation of Investigatory Powers Act. In 2021, the Tribunal found the UK's former bulk data retention scheme (under the Telecommunications Act 1984 and the Regulation of Investigatory Powers Act 2000 (RIPA)) to be incompatible with EU law. Retention of communications data by communications providers must now comply with the *Watson* safeguards, including the prohibition of access to data without prior authorisation by a court or independent authority.

• *Liberty* – this challenged the bulk powers in the Investigatory Powers Act (including the data retention and access provisions), although only the challenge to the retention provisions has been heard so far. The case has been updated following the *Privacy International* judgment above, and is set to be heard in the Supreme Court in 2022.

As things stand at the moment:

• In the Liberty case, the High Court has ruled that the Investigatory Powers Act doesn't allow indiscriminate retention, because it requires the tests of necessity and proportionality to be applied in the exercise of those powers.

• The government amended the Investigatory Powers Act following an earlier judgment in the Liberty case. Communications data authorisations will now need prior approval of a judicial commissioner in most cases.

• The purposes for which an authorisation can be granted were also amended, restricting access to some types of communications data in certain circumstances, for example investigating crime as opposed to serious crime.

Big Brother Watch vs UK

Big Brother Watch vs UK was the first case on bulk interception powers in the European Court of Human Rights. In May 2021, the Court said that bulk interception rules could be legal in principle, as long as there are enough "end to-end" safeguards on access to the data, including an assessment of necessity and proportionality, independent authorisation and an adequate process of supervision and review. It found that the UK's rules under the old Regulation of Investigatory Powers Act 2000 weren't lawful because they didn't have sufficient safeguards in place.

As this case was about the Regulation of Investigatory Powers Act and not the current Investigatory Powers Act, it doesn't affect the current rules. But it's important because it updated the rules which need to be applied to the exercise of investigatory powers in general.

The Digital Economy Act 2017

The Digital Economy Act was designed to help the UK be a world leader in the digital economy. It focuses on three main areas relevant to free expression.

1 Parental controls

The Digital Economy Act introduced a provision which allows communications service providers to keep offering parental controls. It gives us the option to stop or restrict access to sites to protect children. We and other major communications service providers were consulted on this.

2 Age verification for pornography

The Digital Economy Act requires online pornography providers to check the age of their users. This is to try to stop anyone under 18 from accessing their sites. It is regulated by the British Board of Film Classification (BBFC), who can act if pornography providers don't comply. This includes making communications service providers take steps to block pornographic content if they haven't put measures in place to check age – even though the content itself is legal. The Digital Economy Act also gives the BBFC the power to issue notices making communications service providers block 'extreme pornographic material', which is illegal (see the next section).

3 Extreme pornographic material

As mentioned above, the Digital Economy Act gives the BBFC the power to issue notices which make communications service providers block illegal 'extreme pornographic material'.

This is defined in the Digital Economy Act as material of a type described in the Criminal Justice and Immigration Act 2008, which is 'grossly offensive, disgusting or otherwise of an obscene character'.

This approach could also be used for extremist content.

The Online Safety Bill

The Online Safety Bill gained Parliamentary approval on 17 March 2022 and is intended to improve internet safety.

The Bill gives the Secretary of State the power to designate and address a wide range of potentially harmful content, including online trolling, illegal pornography and underage access to legal pornography. It creates a new duty of care for online platforms towards their users, requiring them to take action against both illegal and 'legal but harmful' content. Platforms failing this duty could incur significant fines. In addition, the Bill obliges large social media platforms not to remove journalistic or 'democratically important' content such as user comments on political parties and issues.

We have been consulted on this legislation, and generally support the proposed duty of care on social media platforms and the government's move towards a clear legal framework. As a communications service provider we are willing to play our part in an enforcement regime, up to and including blocking sites or content as a last resort, provided there is a clear legal process and right of appeal.

Case law on content blocking

We only filter or block access to content in certain circumstances. These include if the law or a court says so, for example, if someone posts content that's infringing on someone else's intellectual property rights. Below are some legal cases that have shaped this approach.

Premier League and UEFA blocking orders

Since March 2017 both the Premier League and UEFA have had blocking orders for live football content against major communications service providers. These types of orders are not new. In fact, the law allows them for all types of content. They are used to stop sites that are using, or giving access to, content like music, film and videos without permission from the owners and infringing intellectual property rights.

We agree that these orders are sensible in principle. And normally, in cases like this, we would be neutral. But with these particular orders we, and some other major communications service providers, supported the applications to court and gave evidence. That is because we license content from both the Premier League and UEFA.

So sites streaming that content unlawfully are also damaging our own private rights.

'Real-time' blocking

In 2017, the courts took a new approach to deal with blocking content streams in 'real time'. This is because pirated football streaming can start just before kick-off – so it is impossible for courts to act in advance. But if they acted after the streaming, all the value in the content would have gone because people have already seen the match.

We suggested a new form of court order which would let us, the Premier League and other communications service providers block future live-streamed events we suspect are pirated. We identify these using historical analysis based on key characteristics. To try to stop legitimate content being affected, blocks only apply while a match is on.

As this was a new approach, we used the remaining eight weeks of the 2016/17 season as a trial run. The new process worked well and the court agreed to use the order for the 2017/18 and the 2018/19 seasons.

We understand that other holders of rights or intellectual property may well want to do something similar. But we think they, and not the internet service provider, should pay for these. We only got involved in this case because we have an obvious commercial interest ourselves.

The Cartier case

Cartier brought a case in 2014 to extend the scope of the web-blocking regime to include trademark infringement as well as copyright infringement. The High Court found in their favour, deciding it could extend the scope of blocking injunctions to cover any private law infringement. It also confirmed earlier decisions that communications service providers should pay the implementation costs of these blocking injunctions. BT, EE, Sky, Virgin and TalkTalk appealed this decision, but the Court of Appeal upheld the High Court's decision.

In early 2018, alongside EE, we appealed this on the issue of costs to the Supreme Court. The Court found unanimously in our favour, concluding that in cases where rights holders alone stand to benefit from a blocking order, they should pay communications service providers for the implementation costs.

It remains to be seen what financial impact this judgment has. But we consider there was an important issue of principle at stake. This judgment will help make sure that courts take a proportionate approach with future applications.

Relevant laws around the world

We respect rights to privacy and free expression in every country we work in. In the most part, outside the UK, we provide voice, data and internet access to multinational companies and other organisations around the world. So in this section, we summarise the legal situation in the 20 countries where we do most of our business outside the UK.

Some countries have laws which mean we can't discuss certain issues related to investigatory powers. Where that is the case, we've said that there are restrictions on us and to refer to information published by that country's government (if available).

How our international services work

We make these services available through a core data network, which uses a technology called multi-protocol label switching (MPLS) to carry most of our customers' voice and data traffic around the globe. In that core network, there are routers and other equipment in our points of presence (PoPs), which customers use to connect to our core network.

We have 5,000 PoPs around the world, with the 21 largest country markets (including the UK) making up over 90 per cent of our revenue.

We offer voice services using lots of different technologies. We do this in around 75 countries, where we have our own local operating licences. Where we don't have a licence, we offer voice services from local telecommunications companies. We currently do this in around 100 countries.

We sell internet access to customers in 44 countries, using our own core network. As with voice services, in most countries we need a licence from the local telecommunications regulator to run our own services. If we don't have one, we re-sell local communication providers' internet access instead.

What does this mean for the privacy and free expression of our global customers?

As our customers outside the UK are companies or other types of organisations, we're much less likely to have an impact on individuals' rights to privacy and free expression. But our customers' employees, and potentially their customers, would be affected if we had to give their communications and data to local governments, or block their access to content on the internet. To make sure we understand potential issues like these, we've worked with law firms to review our operations in countries outside the UK. Where we have a local licence or operate our own network, we might have to help legal authorities in ways that could affect people's rights to privacy or freedom of expression.

For example, a legal request could mean we have to hand over information about the services we provide, intercept voice calls or data, or block access to certain material on the internet. Also, because of a licence, we might have to follow requirements of local law enforcement, security and intelligence agencies. But in locations where we use another telecommunications company to deliver services to our customers, then that company will usually get these requests – we'll only be involved if the data involved belongs to us.

We have a specialist assurance team who regularly review our compliance with local investigatory powers and suggest ways to improve and safeguard this. We report any issues they raise to the local security manager and track them until we've resolved them.

The laws in some countries where we do business might be very intrusive when it comes to privacy and free expression. But we believe it is better to keep providing communications services that connect people than not be there at all.

To help businesses deal with these conflicts we sponsored a report from the Business Network for the Rule of Law. This recommends what to do when national law conflicts with international human rights standards.

We are also a member of the Global Network Initiative (GNI), an organisation at the forefront of debates on privacy and free expression, and how they relate to government investigatory powers. This means we can engage with stakeholders to promote and build better understanding of these key human rights issues.

Lawful interception and data disclosure requests

Where we can, we show the following information for:

- **The number of requests for disclosure of data we've had.** This is the total number of legally valid requests (sometimes we don't have the data requested as we don't need it to operate our business. In this case, we will respond to the requestor explaining this but this still counts as a received request).
- **The number of lawful requests for the interception of communications.** Lots of countries put a time limit on how long interception can be carried out for. After this, a new order must be issued to keep intercepting the same communications. This helps make sure that requests are proportionate and that there is the right oversight. But it does mean we can get multiple orders and warrants in one year for the same interception. The numbers we report are for the total number of orders and warrants we've received, including renewals for existing lawful interceptions.

Where we don't provide this information, we give a reason why. This could be because:

- **it's illegal** – in some countries, publishing this type of information is against the law
- **we can't disclose it** – in some countries, while the law might not expressly stop us, authorities have told us we can't publish this type of information
- **it's published somewhere else** – if information is published for the whole industry by a government or other public body, we refer to those publications.

A note about blocking

The specific web pages we have to block change significantly because multiple URLs can relate to one item of illegal content. This means that giving the number of URLs we block in a particular country can be misleading in terms of the volume and type of content we're blocking. We think it is more useful to summarise which countries have a requirement to block content alongside the type of material we're expected to block.

Australia

In Australia, we provide various networked IT services including data, voice and internet services. We operate from our Sydney office and employ more than 200 people.

Lawful interception

The Telecommunications (Interception and Access) Act 1979 (Cth) regulates access to telecommunications content and data in Australia (including intercepting communications in specific circumstances). Under this Act, intercepting telecommunications is only justified for law enforcement and national security purposes. The only people who can issue a warrant to intercept communications are a judge, a nominated member of the Administrative Appeals Tribunal, the attorney-general or the director-general of security (in an emergency).

Data Retention

There are two ways data is kept in Australia.

• The Stored Communications Regime (Telecommunications (Interception and Access) Act, Part 3-1A) allows certain law enforcement agencies to serve preservation notices on communication service providers. These notices order them to keep any communications stated in the preservation notice.

There are three different types of preservation notice:

– historic domestic preservation notices

– ongoing domestic preservation notices

– foreign preservation notices.

A domestic preservation notice can stay in force over the relevant communications for a maximum of 90 days. A foreign preservation notice can stay in force for 180 days.

• The Data Retention Regime (Telecommunications (Interception and Access) Act, Part 5-1A, as amended by the Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015) requires communication service providers to keep certain categories of data for two years. This data doesn't include the content or substance of a communication. Communication service providers must also keep certain types of subscriber information while an account's active and for two years after it's closed.

Data disclosure

The Telecommunications (Interception and Access) Act also allows certain law enforcement and security agencies to access telecommunications data held by communications service providers.

Requests for access to data are independently overseen by the commonwealth ombudsman or, in the case of the Australian Security Intelligence Organisation, by the inspector-general of intelligence and security.

Web blocking

Under the Telecommunications Act 1997 (Cth), internet service providers must try to stop telecommunications networks and facilities being used for crime. The Australian Federal Police use this power to instruct internet service providers to block websites which contain child exploitation material through the Access Limitation Scheme. It's also used to tackle cyber-crime.

Under the Online Safety Act 2021, internet service providers could be requested or required to block access to material promoting, inciting, instructing in or depicting abhorrent violent conduct.

The Australian Media and Communications Authority has a remit under Schedule 5 of the Broadcasting Services Act 1992 (Cth) to require internet service providers to stop access to certain content (for example, child sexual abuse content) which is hosted outside of Australia. It has a similar remit under Schedule 7 of the Broadcasting Act for content services located in Australia.

Under the Copyright Act 1968 (Cth), rights holders can apply to the Federal Court for an injunction that requires internet service providers to take reasonable steps to block access to overseas operated websites which infringe copyright or facilitate copyright infringement. This power was introduced by the Copyright Amendment (Online Infringement) Act 2015 (Cth).

Belgium

We operate from our Brussels office and employ around 200 people. We provide services to multinational corporate and public sector customers, which have complex communication and information system needs. As part of BT's Global unit, we are a global leader in the provisioning of managed IT services for cyber security, digital workplace, contact centres, multi-cloud and infrastructure services.

Lawful interception

Under Article 90ter of the Code of Criminal Procedure, communication service providers must co-operate with judiciary authorities when it comes to lawful interception.

An examining magistrate must order an interception of the content of communications. This can be a warrant or verbally in an emergency (with confirmation), as defined in Articles 90ter to 90decies of the Code of Criminal Procedure, which was modified by the Law of 25 December 2016 on Internet Investigatory Powers. The examining magistrate can ask for communications to be intercepted:

• in exceptional cases

• when necessary for investigations

• when there are strong indications that the communications relate to offences listed in Article 90ter §2 Code of Criminal Procedure

• when other investigations are not enough to find out the truth.

The warrant must be sent to the public prosecutor (Article 90quater §1 Code of Criminal Procedure).

In exceptional circumstances the public prosecutor can order the content of communications to be intercepted. This can happen when the aim is to catch a suspect while they're committing a crime (the relevant crimes are listed in Article 90ter, §5 of the Code of Criminal Procedure).

If national security is at stake, the director general of the intelligence and safety services can order a draft authorisation for interception. This will either be accepted or rejected by a special committee in charge of surveillance. This process is governed by Articles 18/9, 18/10, 18/17 and 44 of the Intelligence and Safety Services Act of 30 November 1998.

The General Military Intelligence and Safety Service (GMISS) can also intercept communications that come from abroad. In December each year, the GMISS produces a list of organisations and institutions whose communications it plans to intercept, with a justification for each. The minister of defence has 10 days to accept or reject the list.

If it's urgent, and there's a clear need, the GMISS can intercept communications for organisations or institutions that aren't on the list. But the GMISS must let the minister of defence know about this as soon as possible and not later than the next business day after the start of the interception. If the minister disagrees with the interception, they can stop it (Article 44/3, 1° Intelligence and Safety Services Act).

Data retention

Article 126 of the Belgian Electronic Communications Act ("ECA") and its implementing orders required certain providers of electronic communications services (more specifically providers offering (i) mobile telephony; (ii) fixed telephony; (iii) public Internet access services; and (iv) public Internet e-mail services and public Internet telephony services in Belgium) to carry out a general and indiscriminate retention of certain traffic and location data during a certain period of time for the purpose of combating crime or safeguarding national security.

On 6 October 2020, this provision was found to be non-compliant with EU law by the EU Court of Justice (judgment in joined cases C-511/18, C-512/18 and C-520/18) and was subsequently annulled by the Belgian Constitutional Court in its judgment of 22 April 2021.

Since Belgian law enforcement authorities are heavily dependent on identification and meta data for the investigation and prosecution of crime, the Belgian Government launched a public consultation

from 7 May until 4 June to repair the annulled legislation through which it intends to reinstate data retention obligations. Following a second judgement of 18 November by the Belgian Constitutional Court, the Belgian Government launched a new public consultation on the draft amendments to the "data retention" bill which will run until 25 March 2022. An update will be provided once the amendments have been confirmed.

Data disclosure

Operators must co-operate with judiciary authorities when it comes to data disclosure (Articles 46bis of the Code of Criminal Procedure for identification data and 88bis of the Code of Criminal Procedure for geolocation and traffic data).

The public prosecutor and the examining magistrate can require operators to give them retained data to identify an end user, and the electronic communications services the user subscribes to (Article 46bis, §1 Code of Criminal Procedure). In an extreme emergency, the public prosecutor and the examining magistrate can authorise this verbally, but they must confirm it in writing as soon as they can afterwards (Articles 46bis, §1 and 56, §2 Code of Criminal Procedure).

An examining magistrate can require the disclosure of traffic and geolocation data through a written warrant. They can only do this where there are serious indications that crimes are taking place which could result in a sentence of one year or more in prison, and where the examining magistrate believes it is necessary to get to the truth (Article 88bis of the Code of Criminal Procedure). The justified order should describe:

- the circumstances that mean the measure is needed
- why the measure is proportionate in relation to the targeted person's privacy
- the length of the disclosure request (Article 88bis Code of Criminal Procedure).

Web blocking

The public prosecutor (Deputy Public Prosecutor and the authority acting for the Public Prosecutor) can through an order required internet service providers to block access to particular unlawful sites, to stop damage caused by content published online (Article 39 bis Code of Criminal Procedure). Orders often include additional obligations to redirect users to a specific URL or to remove the content if it is hosted on a service provider's internet. And, under intellectual property law, the court can make an internet service provider carry out any measure necessary to stop the infringement of their copyright or associated rights.

Internet service providers might also be required to block sites which carry child sexual abuse material, or promote terrorism, racial violence or hatred.

Brazil

We've worked in Brazil for more than 17 years. We have around 200 employees there who support corporate networks, serving hundreds of organisations from the public and private sectors in various industries. We also have extensive terrestrial networks with several GPoPs and thousands of connections from strategic partners in collaboration to support BT Global Network.

Lawful interception

Under Law No. 9,296/1996 (called the 'Wiretap Law' from now on), a court can issue an order requiring a communications service provider to intercept traffic on its network. Only the police authority or the public prosecutor can request these in specific circumstances, for example as part of a criminal investigation or legal proceedings.

Data retention

The Internet Law (Law No. 12,965/2014) requires communication service providers to keep internet connection logs for a year. The police, an administrative authority or public prosecutor can ask them to keep it for longer than a year. Retention is regulated by Presidential Decree 8,771 of 11 May 2016.

As well as this, ANATEL's Resolution No. 614/2012 requires communication service providers to keep connection logs for at least one year. Under the Resolution, connection records include:

- the date and time of the beginning and end of internet access
- the length of internet access
- the IP address used
- other information that allows the access terminal used to be identified.

The Internet Law stops internet access providers from keeping users' application logs. This means they can't keep the content of internet activity or logs of which applications people have used. The Internet Law also separately provides that an internet access provider must keep its application access logs confidential for six months.

Data disclosure

Under Article 22 of the Internet Law, communications data can only be disclosed when requested by the police authority, the public prosecutor, other law enforcement agencies, or any other interested party. Data can be requested for evidence gathering in civil or criminal legal procedures and must be authorised by a court order.

Users' personal data, particularly their name, marital status, occupation, address and name of parents, must be provided by communication service providers if the police authority, the public prosecutor or other administrative authority ask for it – they don't need a court order. This is defined in law under the Internet Law, the Money Laundering Law (Law No. 12,683/2012) and the Organised Crime Law (Law No. 12,850/2013).

Web blocking

There are restrictions to blocking, monitoring, filtering or analysing the contents of internet data packets that are consistent with the principle of net neutrality.

While judges have the power to issue court orders requiring internet service providers to block access to illegal content, they usually prefer to order the party hosting the illegal content to remove it. This is because blocking access might not be proportionate. In the case of child sexual abuse material or unauthorised disclosure of sexual content, there's a notice and takedown provision under the Internet Law. Otherwise, there are no general laws requiring content to be blocked.

Canada

In Canada, we provide various networked IT products including data, voice and internet services. We operate from our Toronto office and employ around 70 people.

Lawful interception

The Radiocommunication Regulations generally prohibit intercepting radio communications. But there are exceptions – for example, for emergencies, investigations by public officials, government spectrum management and communications service provider network security.

There are several circumstances where interception is allowed under the Criminal Code (as amended by the Protecting Canadians from Online Crime Act in 2015). These are:

- by getting both one of the communicating parties' consent and a public officer's order (a public officer can be a peace officer and any public officer responsible for law enforcement)
- if an agent of the state believes there's a risk of bodily harm to the person who consented to the interception under the previous point
- with a formal warrant from a judge or an urgent warrant from a justice of the peace.

In an urgent situation, where there are no other means available under the Code, interceptions can also be allowed to stop serious harm to people or property.

The Canadian Security Intelligence Services Act establishes conditions where the Canadian Security Intelligence Service can get a warrant from a judge if there's a threat to national security or to collect foreign intelligence.

Part V.1 of the National Defence Act establishes the conditions under which the Communications Security Establishment of Canada can get approval from the minister of national defence to intercept private communications involving foreign entities outside Canada. This is allowed as long as there's no other way to reasonably get the information, and provided that Canadians' privacy interests are protected.

Data retention

The Code can require communications interception over a period of time. A warrant or production order specifies the data to be kept, for example, transmission data or tracking data, and how long for. This is done on a case-by-case basis.

Data disclosure

Law enforcement authorities and the security services can require communication service providers to provide data in the same way as interception (see 'Lawful interception' above).

Canada's Competition Act allows the commissioner of competition to apply to a judge of a superior or county court for the disclosure of data. This disclosure is made according to the production order.

Under the Competition Act, the commissioner can also get a search warrant, which might include the reproduction of data found on a computer system.

Web blocking

Superior courts have wide powers to grant blocking orders. Under the Child Pornography Reporting Act, internet service providers must notify authorities about any situations involving child sexual abuse material.

The Quebec government had adopted a law (Bill 74) to compel communication service providers to block illegal gambling websites. In July 2018, the Superior Court of Quebec decided that this law was unconstitutional.

Colombia

In Colombia, we provide a range of services including data and internet access. We employ around 100 people in our office in Bogota.

Lawful interception

Generally, intercepting communications can only take place through a judicial order that meets the criteria set out in relevant laws. But interception can also take place without a court order to allow interception for the purposes of a criminal investigation by the public prosecutor. This is allowed as long as the public prosecutor issues an order to the judicial police who'll be in charge of the technical aspects of the relevant operation and processing. This exception is allowed under Law 1453/2011, which amends the Colombian Criminal Procedure Code, and Decree 1704/2012 (compiled in Decree 1078/2015).

These orders last for 3 months. They can be extended if the public prosecutor decides there are still grounds for interception. Any extension must be examined and authorised by a judge (juez de control de garantías). The order must be issued during an ongoing investigation and with the purpose of finding evidence. Within 24 hours of getting a report from the judicial police, the public prosecutor must appear before the relevant judge to examine the legality of the interception operation.

Interception for the purposes of intelligence and counterintelligence is allowed if certain conditions are met, under Law 1621/2013 (regulated by Decree 857/2014).

The government carries out interceptions after the relevant communications service provider grants access. The provider doesn't directly take part in any interception operations.

Data retention

Generally, all information about a subscriber of a service must be kept for at least five years. Under the Commercial Code, all commercial documents and information must be kept for at least ten years.

Decree 1704 states that communication service providers must keep certain subscriber data for five years. This data includes a subscriber's ID, invoicing information and type of connection, for example voice or data. Under this Decree, the communications service provider should also give the Office of the Attorney General specific information, like zone/sector, signal strength and geographic coordinates that might help identify the terminal or devices used in a particular communication. Decree 1704 applies when there's a judicial investigation (criminal prosecution) and the public prosecutor needs to have access to certain information as evidence.

Communication service providers must give information to certain authorities about a subscriber's communications' activities under Law 1621/2013 (see 'Data disclosure' below). This information

includes:

- their technical identification data
- the location of the cells where the relevant terminals are
- any other information that might help identify where someone is.

This law applies to all intelligence and counter-intelligence activity.

Resolutions No. 912/2008 and 3066/2011 (as modified by Resolution 511/2017) require that communication service providers must keep certain subscriber information.

Data disclosure

Any government body which is responsible for law enforcement or prosecuting or investigating crime can ask for data disclosure. This includes the public prosecutor and other government agencies like tax authorities. There are also certain legal requirements which must be fulfilled.

Under Law 1581/2012, personal information can only be provided to a public authority if the authority's carrying out its duties or a judicial order has been issued.

Web blocking

Internet service providers can be asked to block access to internet sites or services either by a judicial order issued by a competent judge or public prosecutor, or by orders issued by administrative authorities with an investigative capacity (for example, the Superintendence of Industry and Commerce, the Banking Superintendence, the Ministry of Communications, and the Financial Analysis and Information Unit). Most web blocking requests in Colombia are to do with child sexual abuse content.

France

We employ around 400 people across France one third of which are Security specialists. Our head office is in Paris. We provide services to large companies, including multinationals and multi-sites, which have complex communication and information system needs. In France, we support major companies in the finance, telecoms, industrial and services sectors by integrating, securing and managing network and cloud infrastructure and services.

Lawful interception

Interception can be required through administrative requests or judicial requests under French law.

• According to the French Homeland Security Code (the CSI), the contents of a communication can only be intercepted for national security purposes – so that's national defence, prevention of terrorism, prevention of organised crime and delinquency. To do this a minister in charge of homeland security, defence, justice, economy, budget or customs (or their delegate) must make an administrative request, which is then approved by the prime minister following an opinion from the National Intelligence Control Commission (CNCTR). If the situation is urgent, then it's possible that the Commission is only informed of the interception.

• Under the French Code of Criminal Procedure a judicial request for interception is needed for detecting or investigating cases of serious crime – for example, money laundering, organised gang crime or where the criminal penalty is three or more years in prison. Depending on the circumstances, an investigative judge, or a public prosecutor can authorise the request with written permission from the liberty and custody judge.

Operators must put measures in place to comply with any requests.

Data retention

Under the Postal and Electronic Communications Code, operators must keep data about voice and data services for up to a year. This includes subscriber information, names, addresses and communications data. It also includes passwords and payment information if the subscription is to online public communications. After the *Digital Rights Ireland*, *Tele2Sverige AB* and *Watson* cases, several associations asked the French Council of State to check if existing legislation governing data retention and administrative data access requests was legal. The claim wasn't upheld.

Data disclosure

The Code of Criminal Procedure and other relevant legislation provides for the disclosure of communications data to judicial authorities, police officers, public prosecutors or an investigative judge. A judicial authorisation isn't always needed.

The protection authorities ARCOM (intellectual property) and ANSSI (information systems security) can also ask operators to give them data for investigations, findings and judicial proceedings related to:

• copyright and related rights infringement

• criminal offences

• preventing unauthorised access to automated data processing systems.

Under the French Homeland Security Code, the public service in charge of security interception (the Groupement Interministériel de Contrôle) can require that communication service providers give them data for security purposes. These requests must be approved by the prime minister or their delegate.

Under Article L.65 quinquies of the Customs Code, French customs agents can require operators to give them data for customs investigations.

Under Article L.96 G of the Tax Proceedings Code, French tax agents can require operators to give them data for tax investigations.

Under Article L.114-19 of the Social Security Code, French social security agents (URSSAF) can require operators to give them data for social security investigations.

Web blocking

A judicial authority can make internet service providers block access to particular sites, to stop damage caused by content published online. And, under intellectual property law, the court can make an internet service provider carry out any measure necessary to stop the infringement of copyright or associated rights.

The Central Office for Action to Fight against Crime related to Information Technology and Communication might also require internet service providers to block sites which carry child sexual abuse material, or promote terrorism, racial violence or hatred. A request to remove this type of

material must first be made to the publisher of the website or the hosting service provider. If they don't reply in 24 hours, the Central Office can ask an internet service provider to block the sites. French internet service providers have also been ordered to block access to pro-terrorism websites.

Germany

We've been working in Germany for more than 20 years and provide global network and IT services to around 900 customers.

We run our own network infrastructure in Germany, as well as our own Cityfibre Networks in four major German cities and three data centres which provide IT services and connections to our international IP network. We have five offices in Germany and around 800 employees. We provide data services including internet access, voice over internet protocol (VoIP) and cloud-based services.

Lawful interception

The German Telecommunications Act allows intelligence and law enforcement agencies to intercept communications, subject to limitations set out in the German Constitution.

The right to privacy of telecommunications is protected under Article 10. Interception is authorised by a court order, which authorities must get beforehand, and must also meet certain requirements – for example, if someone's committed or tried to commit a serious crime, or if there's an imminent risk of a major attack on public security, like a terrorist attack. The legal bases for these court orders are in both federal law (especially section 100e of the German Criminal Procedure Code and section 23a of the German Customs Investigations Act) and in various regional acts on police powers to safeguard public security.

The Criminal Procedure Code allows the public prosecutor's office to issue an interception order in an urgent situation, which the competent court must confirm within three working days (section 100e (1) of the Criminal Procedure Code). The Federal Criminal Police Office Act also allows the president of the Federal Criminal Police Office to grant an interception order, as long as they then get judicial approval.

As well as this, the Law on the Restriction of Privacy of Correspondence, Post and Telecommunications (called the 'G-10Law' from now on) allows the intelligence services to intercept a person's communications without a court order. This can happen if they are suspicious that this person has committed certain offences which, among other things, endanger national security (section 1(1) no.1 and section 3 of the G-10 Law). The federal ministry of the interior must order any interception activities requested by federal intelligence services (section 10 of the G-10 Law) and the G-10 Commission must approve these in advance (section 15(5) of the G-10 Law).

The exception is for situations where danger is imminent – in this case subsequent approval is enough (section 15(6) of the G-10 Law). The competent supreme authority of the state is responsible for orders for interception by state intelligence services (section 10 of the G-10 Law). The provisions for approving these measures must be set out in the respective state law (section 16 of the G-10 Law).

The G-10 Law also allows German intelligence services to carry out untargeted interception in certain circumstances – that is intercepting certain geographic regions, rather than a specific individual suspect. This is allowed when interception is to stop:

- armed attacks, including terrorist attacks, on Germany
- certain serious crimes, including international drugs trafficking and money laundering (section 5 of the G-10 Law)
- danger to the life or wellbeing of an individual who is abroad, where this danger directly affects the interests of Germany (section 8 of the G-10 Law).

An authorised court order isn't needed for this but the federal ministry of the interior must set the geographic parameters of the untargeted interception. The Parliamentary Control Panel must also approve this in advance, unless there is imminent danger, in which case subsequent approval is enough (section 14(2) of the G-10 Law).

Anyone providing publicly available telecommunications services to more than 10,000 subscribers must install a surveillance system which complies with technical requirements set out in the German Telecommunications Surveillance Directive. Communication service providers can choose to carry out legal interception in house or delegate it to agents. Communication service providers, or their agents, must always be available for requests by phone and process them during normal business hours.

Data retention

Under federal legislation adopted in 2008 (sections 113a and following of the Telecommunications Act), providers of public telecommunications services were required to keep subscriber information and traffic data for six months. But in 2010 the German Federal Constitutional Court held this legislation to be contrary to the German Constitution, because it was a disproportionate restriction of the right to privacy.

Data retention legislation adopted in 2015 limits the data that is retained – for example, emails aren't included. It also limits the length of the storage, which is normally ten weeks, but only four weeks for location data. Processes to comply with this legislation had to be implemented by 1 July 2017.

In late 2016, the CJEU held that UK and Swedish legislation that required communication service providers to store subscriber and traffic data wasn't compatible with the EU Charter of Human Rights. One of the reasons the CJEU gave was that the storage requirement must be limited to specific situations that could justify a temporary retention of data (see the *Tele2 Sverige AB* and *Watson* judgments).

Although the CJEU decision didn't directly concern German data retention legislation, the Court's reasoning suggested that Germany's legislation might not conform to EU law. For this reason, a German Superior Administrative Court granted a preliminary injunction to a German internet service provider that had chosen not to implement current legislation because of constitutional and EU law concerns. After this decision, the German Federal Network Agency stated it would stop enforcing the existing legislation until the end of the main proceedings, which might include a referral of the matter to the CJEU. Another German Administrative Court confirmed this position in favour of a German communications service provider in 2019.

Data disclosure

Under the Telecommunications Act, data can only be disclosed if the requesting party is legally authorised, and the disclosing party is legally authorised to disclose the data.

The main avenue for disclosure of subscriber data is an automated procedure under which the German Federal Network Agency is tasked with retrieving data and forwarding it to the public authority that has asked for it (e.g. the police). This means that communication service providers must store all subscriber data on a server that the German Federal Networks Agency can always access (section 112 of the Telecommunications Act). A prior judicial order isn't needed for the disclosure of subscriber data (i.e. not traffic or content data). If the automated procedure doesn't deliver the right results, public authorities can also ask communication service providers directly for so called manual disclosure of subscriber data (section 113 of the Telecommunications Act). Communication service providers can choose to keep these subscriber files in-house or pass this on to a third-party supplier.

By contrast, in general, disclosure of traffic data does need a prior judicial order, usually requested by the public prosecutor's office (sections 100e and 101a of the German Criminal Procedure Code). If the situation is urgent, the public prosecutor's office can issue a disclosure order, as long as it's ratified by a competent court within three working days (sections 100e and 101a of the Criminal Procedure Code). Competent authorities can order disclosure of traffic data obtained as part of any interception activities carried out under the G-10 Law (see 'Lawful interception' above) without a court order, as long as the disclosure serves specific purposes (e.g. where they need it to stop a serious crime) (section 4(4) of the G-10 Law).

Web blocking

Under the German Interstate Treaty on Broadcasting and Telemedia, an internet service provider can be required by court order to block access to sites containing illegal content. Because no blocking

order was ever made, the German Access Impediment Act about blocking child sexual abuse content was repealed after two years and hasn't been replaced. Instead, the German Interstate Treaty on the Protection of Minors in the Media makes it a legal obligation for every internet service provider to check whether its content is appropriate for children.

Under statutory law, various German courts have held that access providers can be liable for failing to block access to websites containing illegal content – for example content that infringes intellectual property rights. But according to a recent decision of the German Federal Supreme Court, there's no room for this liability where rights' owners haven't taken reasonable steps to take direct action against the people responsible for the illegal online content.

Hong Kong

We've been working in Hong Kong since 1985, when we opened our first office in the Asia-Pacific region. We have around 250 employees here and provide various services to multinational customers with global networked IT solutions.

Lawful interception

Law enforcement agencies must get authorisation before intercepting communications or carrying out covert surveillance under the Interception of Communications and Surveillance Ordinance (Cap. 589, Laws of Hong Kong). There are different types of authorisation which depend on the type of interception and surveillance. They can both last for up to three months.

Judicial authorisations must be in writing from a panel judge and supported by an affidavit.

Executive authorisations must also be in writing, with a supporting statement. These come from the authorising officer within the Customs and Excise Department, the Hong Kong Police Force, the Immigration Department or the Independent Commission Against Corruption.

Executive authorisation is used for less intrusive interception and surveillance. The conditions for issuing or renewing an authorisation are:

- the interception or surveillance is to stop or detect serious crime or protect public security
- there is a reasonable suspicion that any person has been, is or is likely to be involved in a serious crime or a threat to public security
- the interception or covert surveillance is necessary for, and proportionate to, these purposes.

The Interception of Communications and Surveillance Ordinance also contains provisions for emergency authorisations, which can be granted for 48 hours.

The Interception of Communications and Surveillance Ordinance doesn't apply to intercepting telecommunications transmitted by radiocommunications (apart from mobile phones) or interceptions authorised in other ways. This includes interception carried out under a court order authorising the search of any premises or the seizure of any evidence. Other examples of interception include postal packets held by the Post Office, communications with inmates in prison, and communications of inmates of psychiatric hospitals with outsiders.

Under the Telecommunications Ordinance (Cap. 106, Laws of Hong Kong), the chief executive of Hong Kong can order any class of messages to be intercepted to carry out authorisations under the Interception of Communications and Surveillance Ordinance. They can also order this to detect whether any communications services are contravening the Telecommunications Ordinance.

At the moment there aren't any rules which require communication service providers to maintain call interception capabilities in Hong Kong.

Data retention

Under the Telecommunications Ordinance, the chief executive can issue regulations about the time and conditions that messages and other documents connected with a telecommunications service can be kept (section 37 of the Telecommunications Ordinance). But as yet, no action has been taken

under this authority. So there is generally no prescribed time period for how long communication service providers must keep call data.

Under the Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong), communication service providers must take all practical steps to make sure they don't keep personal data for longer than necessary to fulfil the original purpose they collected it for.

Data disclosure

There aren't any statutory requirements specifically requiring communication service providers to disclose telecommunications data. But there don't appear to be any restrictions under Hong Kong law to stop someone asking the courts for a disclosure order against communication service providers.

A common example of a court application like this would be an application for a 'Norwich Pharmacal' discovery order. This is where the applicant tries to get a court order to make a person disclose information or documents relevant to the misconduct or wrongdoing of someone else, and which can then be used in an action by the applicant against that person. For example, disclosure orders have been used to compel internet service providers to disclose the identity of internet subscribers who have allegedly infringed music companies' copyright using peer-to-peer technology.

Certain regulatory authorities can compel communication service providers to disclose information as part of a regulatory investigation, subject to exceptions like legal privilege. These include the Competition Commission and the Communications Authority, which have concurrent jurisdiction to enforce the Competition Ordinance (Cap. 619, Laws of Hong Kong).

Web blocking

There aren't any statutory requirements specifically requiring communication service providers to block access to internet content in Hong Kong. But there don't appear to be any restrictions to stop someone seeking an injunction order that would compel communication service providers to block websites. For example, section 21L(1) of the High Court Ordinance (Cap. 4, Laws of Hong Kong) gives courts a broad power to grant injunctions as long as it's 'just or convenient to do so'. So it's possible that a court order could order a communications service provider to block a website.

India

We have a long history of operating and investing in India, having started in 1987. With headquarters in New Delhi, BT India has operations in six key cities: New Delhi, Bangalore, Mumbai, Pune, Kolkata and Chennai. We started our commercial operations in 2007 when we got a licence to operate international and national long distance services.

Our main delivery hub is based in Gurgaon, New Delhi. It covers all our lines of businesses and customers, from UK consumers to large multinational businesses. It's also the largest BT building in the world, with almost 5,000 people working there.

Lawful interception

Interception, monitoring and collection of any information (including traffic data) are governed by:

- the Information Technology Act 2000 (the 'IT Act')
- the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009
- the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules 2009.

(Collectively, these are called the 'IT Rules'.)

'Information' is broadly defined as including data, text, images, sound, voice, codes, computer programs, software and databases, microfilm and computer-generated microfiche.

The Indian Telegraph Act 1885 and the Indian Telegraph Rules 1951 (the 'Telegraph Laws') regulate the monitoring of messages. This is again broadly defined to include any communication sent by telegraph or given to a telegraph officer to be sent or delivered.

The terms 'information' and 'messages' are collectively referred to as 'communications'. The IT Act, IT Rules and Telegraph Laws are collectively referred to as the 'Data Interception Laws'.

The telecom licence agreements we've entered into with the Indian Department of Telecommunications (the 'Licence Agreements') also allow certain government agencies (the 'Monitoring Agencies') to monitor communications traffic on a communications service provider's network.

Typically, an authorised government agency will serve a communications service provider with an order to intercept communications. This must be issued by a competent authority under the Data Interception Laws. Competent authorities include the secretary to the government of India in the Ministry of Home Affairs, the secretary in charge of the Home Department and the secretary to the government of India in the Department of Information Technology under the Ministry of Communications and Information Technology.

The interception regime in India is evolving. Since October 2014, the government has required all communication service providers to connect their networks to a centralised monitoring system (CMS) under the terms of the Licence Agreements.

The CMS was set up by the government to allow certain law enforcement agencies to intercept and monitor mobile and landbased telecommunications and internet-based traffic in India in real-time. This includes all communications. The CMS allows authorised law enforcement agencies to remotely access a communications service provider's network at any time without the provider knowing about this.

Data retention

The Data Interception Laws govern the retention of intercepted and monitored communications. An authorised government agency can compel a communications service provider to keep communications through an order from the competent authority. Under the Licence Agreements, communication service providers must keep records of all communications exchanged on their network for one year. This can include detailed call logs showing dates, and duration and time of each call. Relevant authorities can require that this data is kept for longer periods of time.

Data disclosure

The Data Interception Laws also govern the disclosure of intercepted or monitored communications. An order from the competent authority directing a communications service provider to intercept or monitor communications can also ask for their disclosure. The Monitoring Agencies are also allowed to access the communication records maintained by the communications service provider under the terms of the Licence Agreements.

Web blocking

BT India's operations don't control access to the internet or information held on it. And we don't do any form of web blocking.

Indonesia

We've been working in Indonesia since 2006. We have around 130 employees based in our office in Jakarta. We provide coverage throughout Indonesia through partnerships with local providers.

Lawful interception

In general, interception is allowed for investigations into criminal acts that are punishable by more than five years in prison. The relevant laws are: Law No.36 of 1999 on Telecommunications (as amended) (the 'Telecommunications Law') and Law No.11 of 2008 on Information and Electronic Transactions Law (the 'IET Law').

Interception can take place after a formal written interception request from the attorney general, the chief of the police or a government investigator.

Interception requests don't need to be ratified by a court order and there are no general limitations on how long a request can last. The length of an interception order depends on the offence and the subject-specific legislation used to grant the order. For example, under Law No.15 of 2003 on the Enactment of Government Regulations In Lieu of Law No.1 of 2002 on the Eradication of Terrorism Criminal Act (as amended) (the 'Terrorism Law') the limitation time is one year. Under Law No.17 of 2011 on State Intelligence (the 'Intelligence Law'), it is six months, which can be extended as necessary. Both the Telecommunications Law and Regulation 52/2000 state that interception must happen within 24 hours of a formal interception request being received.

The Telecommunications Law and the IET Law contain general principles for interception. Other laws outline a more detailed interception procedure for a particular crime – for example, the Terrorism Law and Law No.35 of 2009 on Narcotics. Parliament approved an amendment to the Terrorism Law and there have been discussions on changing the requirements for lawful interception when it applies to terrorism. So far the amendment to the Terrorism Law is still to be finalised and hasn't yet been published.

There are also other laws permitting interception without being subject to the requirements of the Telecommunications Law and the IET Law. For example, the anti-corruption agency and intelligence services are authorised to conduct their own interception activities under Law No.30 of 2002 on the Corruption Eradication Commission (as amended) and the Intelligence Law.

Data retention

The Telecommunications Law and Regulation 52/2000 state that communication service providers must keep data about the use of telecommunications services for at least three months. There is no guidance on the type of data that they should keep though. In practice, it is billing information, like details on outgoing and incoming calls, duration of calls, geo-location of calls and internet data plans (called 'customer usage data').

Data disclosure

Under the Telecommunications Law and Regulation 52/2000, customers can ask communication service providers for their customer usage data. The attorney general, chief of police or government investigator can also ask communication service providers for this. They must give the data confidentially to the authorised party within 24 hours of them asking for it.

Web blocking

As a general principle, Regulation 19/2014 compels internet service providers to block access to sites containing content like pornography and other illegal content, or material that infringes copyright. If internet service providers don't do this, they can be sanctioned. This can range from a written warning to revoking their licence.

Other laws also authorise the government to stop the public accessing certain content. For example, Law No.44 of 2008 regarding Pornography and Government and Regulation No.5 of 2014 regarding Conditions and Procedure on Creation, Dissemination and Use of Pornography Products (the 'Anti-Pornography Laws') give the government the power to block pornography sites. This includes the ability to cut network connections to stop pornographic materials being produced and distributed, and to restrict access through blocking and filtering.

Italy

BT Italia was formed after we acquired Albacom in 1995. We changed its name to BT Italia in 2006. Our head office is in Milan and we employ over 700 staff nationwide.

In Italy, we operate a 9,800-kilometre long haul fibre optic infrastructure which connects the domestic PoPs, nationwide spread, and GPoPs, running global MPLS. We also locally serve BT's global

multinational customers and some of the major Italian financial services firms, utilities, fashion, retail and manufacturing companies, providing them networking, cloud and security solutions.

Lawful interception

There are a number of laws which govern interception and surveillance in Italy. The Code of Criminal Procedure allows a public prosecutor to ask a judge to authorise all forms of interception of communications in criminal cases, provided that it meets certain statutory conditions. In particular, interception is only permitted if there's strong evidence that serious crimes are taking place – for example crimes punishable by at least five years in prison, drug or weapon trafficking, or child sexual abuse. Interception of communications can also only be permitted if it's absolutely necessary for the purposes of the investigation.

The authorisation issued by a judge is valid for 15 days, or 40 days in cases about the prosecution of organised crime. This can be extended for another 15 days at a time, or 20 days in cases of organised crime. If it's urgent and a delay could seriously prejudice an investigation, the public prosecutor can order interception without judicial authorisation, as long as the order is immediately (at least within 24 hours) communicated to a judge. The judge has to decide whether to confirm or revoke the order within 48 hours. If they don't confirm this within 48 hours, the interception is stopped and any data collected can't be used.

Under the Implementation Rules of the Code of Criminal Procedure, the Italian Home Office or senior officers of the main Italian police forces can ask the public prosecutor to authorise an interception to stop terrorism or organised crime. The prime minister or the directors of the secret services empowered by the prime minister can also make the same request, permitted by Law Decree no.144.

As a general rule, interception must be carried out using equipment installed at the public prosecutor's office dealing with the investigation. But if it's urgent and the equipment doesn't work properly or isn't right, the public prosecutor can issue a reasoned order authorising the interception to be carried out using the equipment of the judicial police. When intercepting electronic communications like emails, the public prosecutor can order that the operation is made through equipment owned by private entities or individuals.

The Italian rules around lawful interception were recently amended by Legislative Decree no.216 of 29 December 2017. This modified some rules of the Italian Code of Criminal Procedure, extending obligations of confidentiality for intercepted communications. In particular, the new rules provide that intercepted communications – and, when relevant, their transcriptions – must be stored at the public prosecutor's office. Only the preliminary investigations judge, the lawyers of the relevant parties and other authorised roles (for example court officers) can access these. As well as this, the Legislative Decree reinforces the protection of private conversations between an accused person and their lawyer. If the lawyer asks, interceptions that aren't relevant to a trial (including those containing sensitive data) must be destroyed.

Data retention

Data retention requirements for preventing and punishing crime were originally contained in the Data Protection Code. This required telephone traffic data to be kept for 24 months and internet traffic data for 12 months (Article 132 of Data Protection Code).

Following the judgment in Digital Rights Ireland, which invalidated the underlying EU Data Retention Directive, Italy introduced an anti-terrorism law. This required all telephone and telematics data kept and collected on 21 April 2015 to be retained until 30 June 2017. This law then expired, which meant the general data retention rule under the Data Protection Code applied again. No specific government order is required for these general obligations.

Recently, Law 167/2017 provided a new exemption from the data retention requirements of the Data Protection Code. Under Article 24 of Law 167/2017, telephony and telematics traffic data can be kept for 72 months where necessary to stop certain types of serious crimes, for example terrorism or organised crime.

The law doesn't provide a way to target specific individuals, whose data should be kept on the basis that there is objective evidence showing links to the planning or commission of serious crimes. In

practice it is likely that those people will only be able to be identified afterwards, for example, by the public prosecutor when they start an investigation into the serious crime.

Data disclosure

The disclosure of retained data is mainly governed by the Electronic Communications Code and the Data Protection Code. In general, the competent judicial authority can request that communication service providers provide data for the purposes of justice, with a detailed order referring to the criminal proceedings concerned and outlining the specific data required. The obligation of a communications service provider to comply is set out in Article 96 of the Electronic Communications Code.

Under Article 132 of the Data Protection Code, the public prosecutor, a person accused of a crime or their counsel can ask for retained data to be disclosed during the relevant retention periods.

Under Article 55 of the Electronic Communications Code, a judicial authority can also access, for purposes of justice, data held by the Home Office. Each communications service provider will have passed this data to the Home Office about their own subscribers.

Under Article 226 of the Implementation Rules of the Code of Criminal Procedure, the public prosecutor, the Home Office, directors of the national secret services or senior police officers can request data disclosure in terrorism or organised cases.

Communication service providers must disclose any requested information and grant access to their databases to the Italian secret services for national cyber-security reasons. This is under Act No.124 of 23 August 2007 and the Decree of the Prime Minister No.110835 of 17 February 2017.

Web blocking

Either a judicial authority (in criminal or civil proceedings) or a competent independent supervisory administrative authority (for specific crimes) can require a communications service provider to block access to internet sites or services.

The National Centre Against Child Pornography Centre, established by the Home Office, publishes a list of sites containing child abuse material. Internet service providers must block these within six hours of getting the list, which is continuously updated. Internet service providers must also tell the Centre if they become aware of any of this content. They must also block any material if a judicial authority orders them to for a criminal investigation.

There are also regulations which require internet service providers to block access to copyright infringing material if the Italian Communications Authority orders it. This can include removing single instances of copyright infringing material where the internet service provider hosts the material, or blocking access in the case of a serious infringement, including where the material's on a website hosted in Italy.

Law 167/2017 requires the Authority to issue a new regulation which governs cases of online copyright infringement, specifically to include interim injunctions that rights holders can apply for from the Authority. This new regulation will, among other things, provide an appeal mechanism against the Authority's decisions as well as appropriate measures to make sure violations aren't repeated. So far this regulation hasn't been adopted.

Japan

We've been working in Japan since 1985, with offices in Tokyo and Osaka that employ over 50 people. We provide network coverage to 11,200 customer sites in Japan. This includes three IP Connect Global PoPs and voice connectivity from Tokyo, which provides inbound and outbound voice calls.

We also run a 24x7 multilingual network operations centre in Tokyo and provides hosting services, with support on site and a helpdesk. In Japan we cater for both domestic customers and large multinational companies.

Lawful interception

Under the Act on Wiretapping for Criminal Investigation, a district court judge can issue a warrant to competent investigation authorities who are investigating crime to intercept communications. Communication service providers must cooperate fully with investigation authorities.

There isn't a law in Japan which justifies interception for state security.

Data retention

There aren't any general requirements for communication service providers to keep data. But the Code of Criminal Procedure allows competent investigation authorities to order a provider to keep a history of communications relating to criminal investigations for up to 60 days, on a case-by-case basis.

Data disclosure

The Code of Criminal Procedure also allows the competent investigation authorities to carry out searches or seize electromagnetic records. This includes communication histories, like names and dates and times. They can do this to investigate an offence, and a judge must issue a warrant.

Web blocking

There aren't any legal requirements to block access to internet content in Japan.

Some legislation requires internet service providers to make an effort to co-operate with investigating agencies or take action to stop people sending information about child sexual abuse material, or hacking websites. One way this is done is by actively managing passwords. These actions are on a best-efforts basis. But there are also efforts in both the public sector (by the Ministry of Internal Affairs and Communications) and the private sector (by the Internet Content Safety Association) to identify and filter inappropriate content like child sexual abuse materials.

The Netherlands

In the Netherlands, our head office is in Amsterdam where we employ over 500 people.

We have had a presence in the Netherlands since 1989. We provide network and IT services, professional services and wholesale services as well as a range of domestic VPN, ethernet and internet services, including more than 6,700 km of fibre network nationwide. BT also has its own data centres in Amsterdam, Rotterdam and Nieuwegein.

Lawful interception

Under Chapter 13 of the Dutch Telecommunications Act providers of public telecommunications networks and services are required to provide a permanent capability for interception and to co-operate with judiciary authorities when it comes to lawful interception.

The powers of the Dutch judiciary authorities to intercept communication for law enforcement purposes are laid down in Art. 126la-126nb of the Dutch Code of Criminal Procedure.

Under Art. 126m of the Code of Criminal Procedure, the public prosecutor can order officers charged with an investigation – for example, the police – to carry out an interception of communication. Such an order can only be given in case of a suspicion of a crime punishable by imprisonment of four years or more (with the suspect being eligible for pre-trial detention) which constitutes a serious breach of the legal order, if the interception is urgently needed for the investigation and following a written court order.

When the order relates to communication over a public telecommunications network or using a public telecommunications service, the public prosecutor must issue a formal request to the telecommunications service provider to assist with the interception activities, unless this is not possible or not in the interest of the investigation to ask for this cooperation. The telecommunications service provider must comply.

Art. 126t and Art. 126zg of the Dutch Code of Criminal Procedure provide for similar powers in case of organised crime or indications of a terrorist crime.

The powers of the intelligence and security services to intercept communication are laid down in the Act on the Intelligence and Security Services 2017 (the 'WIV').

Under the WIV the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) may carry out targeted interception, recording and tapping of any form of conversation or electronic communication, inter alia by means of a telephone or internet tap. They are also allowed to carry out untargeted or bulk interception of electronic communication, subsequently determining its nature, determining or verifying the persons or organizations involved, and applying automated data analysis to the metadata and selectively selecting the content data for further analysis. Operators must help them do this – for example, by decrypting encrypted data.

The AIVD and the MIVD may use these powers if this is necessary for the tasks of the intelligence and security services, the means are proportionate in relation to the purpose and there are no less intrusive means available. The powers should also be deployed as targeted as possible. The use of these powers requires the prior authorisation of the concerned minister: for the AIVD this is the minister of the interior and kingdom relations, for the MIVD the minister of defence. At the written request of the head of the relevant service, the competent minister can grant this permission for a maximum period of 3 months, after which a request can be made for an extension for the same period. Judicial authorisation isn't needed.

Data retention

Art. 13.2a of the Dutch Telecommunication Act contains a data retention obligation for providers of public telecommunication networks and/or services but it is currently not in effect. This provision is the Dutch implementation of the EU Data Retention Directive which was invalidated in 2014 by the EU Court of Justice in case C-293/12 and C-594/12 (Digital Rights Ireland), because it violated the right to respect for private life and the right to protection of personal data as laid down in Art. 7 and 8 of the EU Charter of Fundamental Rights. After that, the Dutch implementation act continued to be in force, until on 11 March 2015 the District Court of The Hague following the EU Court of Justice, declared Art. 13.2a Dutch Telecommunication Act non-binding and put it out of effect. As a result, there is currently no obligation regarding for communications service providers to retain communications data for law enforcement and national security purposes in the Netherlands.

This might change in the future. In October 2016, the secretary of state for justice and security submitted a proposal for a new data retention law to parliament which require communication service providers to keep internet related data for six months and telephone data for 12 months. Following the judgments of the EU Court of Justice in the *Tele2 Sverige AB* and *Watson* cases (cases C-203/15 and C-698/15), the minister announced that the proposal would be significantly amended and the mandatory retention would be limited to the identification data (e.g. IP addresses or phone numbers) of the user of a communication service. It is currently not clear if, when and in what form this law will enter into force.

Data disclosure

The Code of Criminal Procedure and the WIV allow the public prosecutor, the AIVD, the MIVD and, in some cases, officers in charge of an investigation to request providers of telecommunication service to provide communications meta data and/or data concerning the subscriber or users of the service.

Web blocking

Under Art. 6:196c of the Dutch Civil Code and Art. 54a of the Dutch Penal Code online intermediaries such as internet providers, hosting providers and online platforms service are exempted from civil and/or criminal liability for their customers' content on and use of their services. They can only be held liable if they are (made) aware of clearly unlawful content and fail to take action to promptly remove this content or make it inaccessible.

The Dutch government and the internet industry have agreed on a code of conduct with a procedure for handling notice and take down requests with regard to unlawful or criminal content on the internet. When service providers comply with this procedure, they cannot be held liable for the unlawful actions

of their users. They can however still be required by a court or public prosecutor to block or remove unlawful content and/or to provide identifying information.

Republic of Ireland

BT Ireland provides data, voice and internet services to government and major businesses in the Republic of Ireland. We also provide wholesale network services, supplying telecommunications products and services to key communications providers.

Until 2009, BT Ireland also provided voice and internet services to consumers and small businesses. Most of these customers were transferred to Vodafone via a wholesale agreement. But we still provide services to a small number of consumers and small businesses on our dial-up internet service.

Lawful interception

Historically, the Postal and Telecommunications Services Act 1983 (as amended by the Postal Packets and Telecommunications Messages (Regulation) Act 1993) was taken to mean that a communications service provider must intercept any form of communications, including post, phone and email. These had to be issued with a written authorisation by the minister for communications or the minister for justice.

But in 2016 the Irish Department of Justice stated publicly that it doesn't interpret the 1993 Act as giving a lawful basis for intercepting email communications. They laid this out in a policy document called 'Amendments to the legislative basis for the lawful interception of communications', in November 2016.

Under the Criminal Justice (Surveillance) Act 2009, senior law enforcement officers can apply to a district court for a court order to allow interception in specific circumstances in criminal investigations.

A High Court judge is designated to review the use of powers under both the Postal and Telecommunications Services Act 1983, the Postal Packets and Telecommunications Messages (Regulation) Act 1993 and the Criminal Justice (Surveillance) Act 2009.

Data retention

Under the Communications (Retention of Data) Act 2011, communication service providers must keep specific data about voice services (for example traffic data) for two years and specific data about internet services for one year. Under the Act, an officer of the Garda Síochána can require them to keep certain data if they have grounds to believe someone has committed an arrestable offence (i.e. one that's punishable by five years or more in prison). In these circumstances, the officer must get written confirmation from a senior officer or district judge as soon as is reasonably possible.

The Communications (Retention of Data) Act has been challenged in the Irish High Court. This led to a referral to the CJEU, which found that the Data Retention Directive (Directive 2006/24/EC) wasn't valid (see the case *Digital Rights Ireland v Minister for Communications and Others*, joined cases C-293/12 and C-514/2). As the original Irish High Court case hasn't, to date, been concluded, the Communications (Retention of Data) Act continues to apply in Ireland. Another challenge to the Act recently started in the Irish High Court (*Dwyer v Commissioner of An Garda Síochána & Others* 2015/351 P).

In late 2017, the government published the general scheme of the Communications (Retention of Data) Bill 2017, which they intend to replace the Communications (Retention of Data) Act 2011. The full text of the draft Bill hasn't been published yet, or initiated in the Oireachtas (the Irish Parliament), but will likely take into account the outcome of the *Dwyer* CJEU referral.

Data disclosure

The Retention Act gives specified senior law enforcement officers (including the revenue commissioners, Competition and Consumer Protection Commission and the Garda Síochána Ombudsman Commission), military officers and judges power to order communication service providers to disclose data for certain purposes (for example, to safeguard security or prevent a serious offence). Disclosure requests must be made in writing, unless they're urgent, in which case they can be made verbally.

Other law enforcement agencies can get search warrants under a wide range of legislation, like the Criminal Justice Acts, the Competition and Consumer Protection Act 2014, the Companies Act and the Taxes Consolidation Act 1997. Search warrants that mean a communications service provider must provide copies of retained data can be issued by a district court judge or a peace commissioner.

Web blocking

A copyright holder can apply to the Irish High Court to grant an injunction requiring internet service providers to block specific IP addresses which are infringing copyright. This is allowed under the Copyright & Related Rights Act 2000 (as amended by the European Union (Copyright and Related Rights) Regulations 2012).

In 2016, the Irish Court of Appeal affirmed the power of the High Court to order non-infringing internet service providers to put a graduated response system in place for customers who infringe copyright under the Copyright & Related Rights Act 2000 (see the case Sony Music Entertainment (Ireland) Ltd & Others v UPC Communications Ireland Ltd [2016] IECA 231). We aren't aware of any further orders being granted by the High Court. But it is possible they have been granted but not publicised.

BT Ireland is a member of the Internet Service Providers Association of Ireland (ISPAI). Their code of practice requires members to comply with notices from www.hotline.ie that ask for potentially illegal material to be removed from websites or newsgroups hosted by members, as long as it is technically practical to do that.

Singapore

BT Singapore provides various BT products including voice, data and internet services. It is one of BT's Asia-Pacific hubs, employing over 200 people.

Lawful interception

Certain legislation grants specific rights for local public agencies to intercept communications.

The Telecommunications Act (Cap. 323) gives the minister for communications and information broad powers. These include requiring telecommunications licensees to intercept communications in certain circumstances – for example, public emergencies, or in the interests of public security or national defence. Under the Kidnapping Act (Cap. 151), the public prosecutor can authorise a police officer to intercept any communications that might contain information about a kidnapping.

Warrants or court orders aren't needed to authorise interception under either the Telecommunications Act or the Kidnapping Act. State agencies or government ministries and departments aren't prohibited from monitoring people's private communications.

Telecommunication operator licences also contain broad obligations for licensees to follow the instructions of the licensor, the Infocommunications Media Development Authority of Singapore (MIDA), in relation to emergency activities. The MIDA is also granted a broad right under these licences to issue any directions to licensees.

Data retention

There isn't a law in Singapore that specifically requires telecommunications licensees to keep data about their subscribers or customers. But telecommunication operator licences contractually require them to keep a register of subscribers for between six and 12 months, depending on the services they offer. This might include names, addresses, phone numbers and 'call detail records' made and received through the communications service provider's network.

Telecommunication licensees also need to keep data to comply with the Telecoms Competition Code. This is to make sure there is minimal disruption to people when they terminate a service. This is relevant when someone wants to change to another operator.

Data disclosure

The Telecommunications Act permits the minister to request disclosure of retained data.

Under the Criminal Procedure Code, a police officer who is a sergeant or above can issue a written order that requires the production of anything necessary or desirable for an investigation, inquiry, trial or proceeding.

There are various other laws in Singapore that give law enforcement agencies, regulators and specific personnel in government departments and agencies broad powers of investigation to request disclosure of or access to data. These include the Computer Misuse and Cybersecurity Act (Cap. 50A), the Misuse of Drugs Act (Cap. 185), the Electronic Transactions Act (Cap. 88), the Official Secrets Act (Cap. 213) and the Personal Data Protection Act 2012.

Web blocking

The MIDA has the power to issue a blocking order under rule 16 of the Schedule to the Broadcasting (Class Licence) Notification. The MIDA can use this power if a website:

- goes against the Internet Code of Practice
- is contrary to the public interest, public order or national harmony
- is offensive and against good taste or decency.

The Copyright Act (Cap. 63) allows rights holders to issue a takedown notice to an internet service provider to block access or remove copyright-infringing material from its network.

South Africa

In South Africa we offer voice and data services and internet access through our own network infrastructure. We employ over 200 staff across our three regional offices and PoPs in Johannesburg, Cape Town and Durban, and customer support service centres in Durban and Cape Town.

We have invested in our own network connection between Johannesburg, Cape Town and Durban. This makes us one of the first global operators in control of its own network infrastructure in South Africa.

Lawful interception

The interception of communications for law enforcement purposes is mainly governed by the Regulation of Interception of Communications and Provision of Communications Related Information Act 2002. The Criminal Procedure Act 1977 also gives law enforcement authorities powers to gather evidence from any person who is likely to give material or relevant information about an alleged criminal offence at a court hearing of a criminal trial. But any ongoing information gathering processes must be authorised directly under the Communications and Provision of Communications Related Information Act.

Both these Acts require law enforcement agencies to apply for judicial authorisation for interception of communications content and metadata. The Communications and Provision of Communications Related Information Act 2002 defines this as 'communication-related information'.

Authorisation can be granted by a designated judge under the 2002 Act when:

- there are reasonable grounds to believe that a serious criminal offence has been, is being or probably will be committed
- the gathering of information concerning an actual or potential threat to public health or safety or national security is necessary
- the gathering of information concerning an actual threat to compelling national economic interests is necessary
- the gathering of information concerning property which is or could probably be an instrument of a serious offence or the proceeds of unlawful activities is necessary.

The Regulation of Interception of Communications and Provision of Communications Related Information Act 2002 also allows authorisation for interception to be granted where South Africa

provides or asks for foreign help in connection with interception of communications about organised crime or terrorism.

There are also emergency provisions in the Act that allow law enforcement agencies to track the location of someone's mobile phone without getting pre-authorisation from a judge. This is allowed when there are reasonable grounds to believe that someone's life is in danger or they might be seriously injured. Authorisation must later be got from the designated judge.

Warrants are called interception directions, and can apply to both internet service providers and communication service providers, who must comply with them.

Data retention

The Regulation of Interception of Communications and Provision of Communications Related Information Act 2002 makes a distinction between communications content and metadata.

Internet service providers must immediately store real-time communications content which is the subject of an interception direction for at least 90 days. All telecommunications companies and internet service providers must keep all users' metadata for at least three years under the Act. The protections against interception of metadata are lower than those for communication content. Metadata that is older than 90 days is classified as 'archived information' under the Act. Law enforcement agencies can seek an interception direction for this from any High Court judge or magistrate.

Data disclosure

Law enforcement authorities can ask for data to be disclosed under the Regulation of Interception of Communications and Provision of Communications Related Information Act 2002 and the Criminal Procedure Act 1977. They can also gather evidence for the preparation of criminal prosecutions under section 205 of the 1977 Act, as long as their written request is endorsed by a judge of a High Court, a regional court magistrate or a magistrate. They will issue an order for disclosure if a given set of grounds are met.

Web blocking

Under the Electronic Communications and Transactions Act 2002, people can ask internet service providers to take down illegal content like child sexual abuse material, defamatory material and copyright violations. The Act further imposes civil liability on anyone who knowingly misrepresents the facts when they lodge a take-down notice.

South African courts also have the power to order people, including internet service providers, to remove unlawful online publications, or to remove specific information from publications.

Spain

We have provided services in Spain for 25 years. Our headquarters are in Madrid and we employ around 220 people.

Lawful interception

Interception powers are governed by the Criminal Procedure Act, which was approved by Royal Decree of 14 September 1882, as amended by Act 13/2015 of 5 October 2015. A competent court can order communications to be intercepted if the judicial police, the intelligence agencies or the customs agencies ask them to, and it is for a criminal investigation about certain serious offences – for example organised crime or terrorism.

In urgent cases, and where an investigation is being carried out into crimes by armed gangs or terrorists, the ministry of Home Affairs, or the secretary of state for security, can order the interception of communications. The courts must review and confirm or revoke the order within 72 hours.

Requests for interception must be based on objective evidence that they'll help verify facts or circumstances that are relevant to a criminal investigation.

Under the Organic Act 2/2002, the Supreme Court can authorise the secretary of state for directorship of the National Intelligence Centre to adopt measures that might affect the secrecy of communications, including intercepting them. This is as long as these measures are necessary to perform the tasks assigned to the NIC – for example to protect national security and prevent crime.

Under Law 9/2014 of the General Telecommunications and the Royal Decree 424/2005, a communications service provider must intercept communications when asked by a court or the NIC. So communication service providers must maintain a permanent technical interface for this purpose, based on government technical specifications. They must use this to transfer intercepted information to interception reception centres, where authorities can access it.

Data retention

Data retention is governed by Law 25/2007 on retention of data related to electronic communications and public communication networks.

Operators that provide publicly available electronic communications services or operate public communications networks must keep traffic data about voice services, including fixed and mobile, and internet services for 12 months. Communication service providers and internet service providers must keep data for crime-fighting purposes, even if a specific order hasn't been issued. This period can be reduced to six months or extended up to two years by the government, after consulting with the communication service providers, and depending on the data in question.

Law 25/2007 expressly states that content data can't be retained.

Data disclosure

Law 25/2007 allows authorised agents to ask for data for detecting, investigating or prosecuting serious criminal offences. These agencies include members of the state security forces, Customs Surveillance Directorate or agents from the National Intelligence Centre, who must get an order from the competent court. Data disclosure is also regulated by Act 13/2015, which modifies the Criminal Procedure Act.

Web blocking

Under Act 34/2002 on Information Society Services and Electronic Commerce, authorities can block access to a website if it infringes certain principles of public policy and human dignity, including intellectual property rights and the protection of children. In certain cases – for example if the measure to be adopted might affect fundamental rights like freedom of speech or right to information – the competent court must authorise the web blocking.

Any provider of information services, including internet service providers, must co-operate with authorities when it comes to blocking internet sites.

Sweden

We have been offering services in Sweden since 1989.

We have two offices, one in Stockholm and one in Malmö, and employ 45 people. We provide secure networked IT services, voice services and internet access for corporate customers. We also offer solutions for managed IT services and lease infrastructure capacity from domestic communication service providers.

Lawful interception

Lawful interception is regulated under the Electronic Communications Act, the Act on Signal Surveillance for Defence Intelligence Activities and the Swedish Code of Judicial Procedure.

Under these laws, the public prosecutor and the National Defence Radio Establishment need a court order for interception. In exceptional circumstances, like where waiting for a court order would substantially affect an investigation, the public prosecutor or the Försvarets Radioanstalt (a Swedish

Intelligence agency) can approve their own interception request. The relevant court must then review their decision.

Suppliers of public communications networks must allow interception, including installing necessary technical equipment and software so this can be carried out.

Data retention

Data retention is required under the Electronic Communication Act and the Electronic Communications Regulation. Under current legislation, no court order is needed and communications service providers must keep data for ten months from when a communication ends. If someone makes a disclosure request before the ten-month retention period runs out, the communications service provider must keep data until the disclosure request has been met. After that, they must immediately delete it. They must keep data for voice, message and internet services, including IMSIs, IMEIs, IP addresses, location data, timing, subscriber names, addresses and any other data necessary to identify a perpetrator.

In 2016, the CJEU held that legislation requiring communication service providers to store subscriber and traffic data wasn't compatible with the EU Charter of Fundamental Rights. In March 2017, a Swedish court repealed an order to store data for crime-fighting purposes as the relevant Swedish data retention legislation had been deemed to be incompatible with EU law.

Data disclosure

The Swedish Prosecution Authority, the police or any other relevant Swedish authority can ask for data in connection with a suspected criminal offence.

Depending on the type of data, disclosure to Swedish authorities can also be permitted in the following ways:

- through a secret interception court order made under the Swedish Code of Judicial Procedure
- following a decision by the Swedish Security Service, the Swedish Police or the Swedish Customs Authority under the Act on the Retrieval of Data about Electronic Communications in the Activities of Law Enforcement Authorities
- through a request from the Swedish Tax Authority or the Swedish Enforcement Authority.

Web blocking

The Swedish Post and Telecom Authority doesn't have the power to order internet service providers to block websites. But in civil intellectual property infringement cases, a court can issue an injunction against an internet service provider to block websites. They can fine providers if they don't comply.

As well as this, the Swedish National Police Board sends internet service providers a list of sites containing child sexual abuse material, although they don't have to block these.

Switzerland

In Switzerland, we provide various networked IT services including data, voice and internet services. We have operated in Switzerland since 1992. Our headquarters are in Zurich-Wallisellen and we have offices in Berne, Basel and Geneva, which employ more than 200 people.

Lawful interception

The revised Postal and Telecommunications Surveillance Act, along with the Federal Act on International Judicial Assistance in Criminal Matters, allow certain law enforcement authorities to carry out surveillance of telecommunications networks. They need communication service providers to provide access to their premises and systems for real time and retroactive surveillance. Other providers and company network and public access point operators must also provide access. Authorities can ask for surveillance:

- in criminal proceedings

- to search for missing people or for people who have to serve a custodial sentence
- to provide international legal assistance
- as required under the Federal Intelligence Service Act (see below).

Law enforcement authorities must get court approval for surveillance requests. The Surveillance Office runs a centralised data processing system. Surveillance data collected from communications service providers goes through this database. The Surveillance Office can then give it to the authority who has asked for it. While communication service providers have only very limited rights to challenge surveillance requests, people who are the target of the surveillance can challenge them.

The Federal Intelligence Service Act allows the Federal Intelligence Service to ask for help from communication service providers for interception activities. It's possible for a private operator to challenge these requests under Federal Intelligence Service Act in the Federal Administrative Court.

In exceptional circumstances, like an emergency or when national interests or security are at risk, the Federal Telecommunications Act allows the Federal Council or the Federal Department on the Environment, Transport, Energy and Communications to order communication services to be intercepted, limited or interrupted.

Data retention

Under the Postal and Telecommunications Surveillance Act, communication service providers must keep certain information about users for the length of their contractual relationship, and then for six months after this ends. It also requires communication service providers to keep certain identification, traffic and marginal communications data for six months.

Data disclosure

Communication service providers must keep their users' communications confidential. But if the Surveillance Office asks for them, they must give them the data.

Web blocking

At the moment there are no laws specifically regulating website blocking in Switzerland. But these requirements might arise either to limit our own potential liability for contributing to the distribution of unlawful content, or where courts order certain unlawful content (like copyright infringing material or illegal pornography) be blocked.

USA

We've provided telecommunications services in the United States for more than 30 years. Our US headquarters are in Dallas, Texas. We employ more than 2,000 people and have offices in more than 16 cities across the US.

We own and operate our own network infrastructure in North America. This includes nationwide coverage in all major US cities, making ours one of the largest networks of this type in the region. Around half of our top 2,000 customers operate in North America, which is why we have such a large presence here.

Lawful interception

There are separate laws for law enforcement access to communications data and access for national security and intelligence purposes.

Under the Wiretap Act, a federal or authorised state judge can issue a wiretap order that allows law enforcement agencies to intercept oral, wire or electronic communications. The application must meet certain conditions, which include probable cause that the interception will reveal a federal crime.

A court can also issue a pen/trap order, which is authorised by the Pen/Trap Statute, as long as an executive officer provides the required certification. The order can be used to get dialling, routing, addressing or signalling information, but not the contents of a communication.

The Foreign Intelligence Surveillance Act allows the Foreign Intelligence Surveillance Court to authorise a federal officer to conduct certain surveillance if there's probable cause that the target is a foreign power or an agent of one (among other requirements). In an emergency, the Attorney General can authorise the order to get foreign intelligence information, but they must also inform a judge and apply for an order in the usual way within seven days.

The Attorney General can also authorise interception without a court order under the Attorney General Foreign Intelligence Surveillance Act directive. This allows an interception for up to one year if it only targets communications between foreign powers, and if other conditions around the impact on US citizens are met.

The Foreign Intelligence Surveillance Act also allows the Attorney General to order a communications service provider to provide information, facilities or technical assistance for interception. They don't need a court order for this, but the communications service provider can ask for a judicial review.

The Communications Assistance for Law Enforcement Act states that communication service providers and related equipment manufacturers must have a permanent capability on their networks which allows law enforcement officers to carry out electronic surveillance.

Data retention

The Stored Communications Act regulates the government's ability to get the stored content of electronic communications and subscriber data from communication service providers. They can order providers to preserve communications records for 90 days and extend this for a further 90 days.

Under the Federal Communications Commission Regulations, telecommunication carriers must keep any records that are necessary for billing information about telephone toll calls for 18 months.

Civil litigants also have the right to require communications data to be preserved under the Federal Rules of Civil Procedure.

Data disclosure

Law enforcement officials and intelligence agency officials can make a communication service provider disclose data they hold through court orders, warrants or subpoenas. These must be authorised under the Stored Communications Act.

The intelligence agencies can ask for data about foreign powers, either by National Security Letters, under the PATRIOT Act, or by a Foreign Intelligence Surveillance Act court order. The CLOUD Act amended the Stored Communications Act to allow federal law enforcement to compel communications services providers to provide requested data stored on servers regardless of whether the data is stored in the US or overseas.

The Communications Act also gives consumers the right to require reasonable disclosure of their own data from companies that store it.

Web blocking

Blocking internet content generally isn't authorised under current legislation. The US Supreme Court has invalidated blocking orders made in the lower courts on the basis that they breach the right of free expression in the First Amendment to the American Constitution. This includes indecent material likely to be accessible to under 18s.

There are exceptions to this, including in the Digital Millennium Copyright Act. Here copyright holders can ask for injunctions against internet service providers which force them to take down infringing content.

Find out more at bt.com/privacyandfreeexpression

Offices worldwide

Registered office: 1 Braham Street, London E1 8EE

Registered in England No. 1800000