simmons+simmons

A comparative review of governmental access and assistance laws

FIRST PUBLISHED: 16 DECEMBER 2019

UPDATED: 14 APRIL 2020

Introduction[1]

As the global economy becomes one that is increasingly online, fast-moving and driven by data, there is a corresponding rise in cyber-related and data-related threats. Moreover, the increasing ubiquity of technologies such as messaging applications that are end-to-end encrypted have increased the possibility of technology being misused to facilitate the activities of bad actors and to frustrate the attempts of law enforcement and national security agencies to investigate and prosecute these crimes.

Against this background, governments are reassessing the strength of their laws on rights of information access by law enforcement and national security agencies, as well as related laws on matters such as data privacy, cybersecurity and the protection of critical infrastructure. There is growing recognition by governments that conventional access and assistance laws may be inadequate when it comes to online and electronic communications, as the information obtainable by these conventional means may be of limited use (for example, because that information is encrypted). Legislation to compel assistance from communications and related industries to provide greater assistance in obtaining and understanding electronic information is increasingly being considered and introduced by governments around the world.

Some of these efforts have been met with criticism – for example, the access and assistance laws introduced in Australia in late 2018 were widely condemned by industry players as too overreaching. Similarly in Europe, the proposed "e-evidence regulations"[2] – which permit judicial authorities in one EU Member State to bypass those in another when making judicial orders for electronic evidence from service providers in criminal matters – have also been much criticised. These laws impact not only telecommunications network operators (who have traditionally been the main players tasked with facilitating access and assistance to communications for law enforcement and national security agencies), but increasingly parallel businesses such as equipment manufacturers, software developers, cloud providers and over-the-top and web-and-app based services.

The extraterritorial application of access and assistance laws is also a concern for businesses. China, in particular, has been perceived to have implemented laws which allow unfettered governmental access to information, whether or not held within Chinese borders. There is a sense of fear among many non-Chinese companies and governments that the Chinese cybersecurity and information laws are open to misuse. Among the most common concerns cited are governmental directives to require Chinese companies to plant "backdoors" or surveillance capabilities into their products, increased risk of intellectual property theft and other compulsory access to information by Chinese authorities for ulterior purposes. Such misconceptions encourage speculation that choosing an ICT vendor in China would create a security threat and so excluding the vendor from China will make network and data more secure and less subject to government access. What is not well understood, however, is whether these concerns are valid based on a proper understanding of the relevant Chinese laws and how these laws compare with other access and assistance regimes around the world.

This paper seeks to examine the governmental access and assistance regimes in seven jurisdictions – China, UK, US, Germany, Australia, Sweden and Finland – and to assist businesses to make more informed decisions about doing – or abstaining from doing – business in or with companies located in these jurisdictions.

(1) This paper is produced by Simmons & Simmons. This paper is provided for general informational purposes only (based on information as at the date of writing) and does not constitute legal or other advice on any specific matter.

(2) See EU Draft of the Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters. These rules attempt to oblige telecommunication service providers who offer services in the European Union to respond to requests for electronic evidence within 10 days, or in an emergency, 6 hours (breach of which may amount to sanctions of up to 2% of total worldwide annual turnover of the preceding financial year). Currently, criminal investigators are required to wait for much longer, with the current time period for a European Investigation Order being 120 days.

Summary of findings

On the fundamental question of governmental rights of access and assistance, we find that governmental rights of access and assistance on the grounds of national security and criminal law investigation and enforcement are common to all seven of the jurisdictions we surveyed.

Perhaps the greatest departures between the seven jurisdictions we surveyed are the availability and nature of procedural requirements to issue assistance orders or requests or to challenge their issuance (either prior to issuance or as a matter of appeal). This ranges from a focus on pre-issuance judicial review and requirements for warrants or court orders in the US and Germany on the one hand, to a quasi-administrative "issue-review" procedure for certain types of warrants in the UK, to more administrative decision-making in Australia and China in relation to certain governmental access rights. What is clear is that there is no one single approach and countries take a range of judicial, quasi-judicial and administrative approaches – each of which have their own advantages and drawbacks. Some of the more recent laws are an attempt by governments to balance the issue of due process against the need for speed of access to information (which is often critical in responding to criminal investigations and matters of national security).

We set out below a tabular summary of the major findings (capitalised terms have the meanings given to them in the detailed discussion sections for each relevant jurisdiction below).

simmons+simmons

Governmental Access and Assistance Laws: A comparison

	China	United Kingdom	United States	Australia	Germany	Sweden	Finland
May law enforcement and intelligence agencies require companies to provide mandatory assistance in the course of an investigation or intelligence gathering?	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Would such access-and-assistance requests have extraterritorial effect? For example, if a company stores data on servers in another country, can the law enforcement and intelligence agencies require the company to access and disclose such data? Or if the data is possessed by an overseas affiliate of the company, can the law enforcement and intelligence agencies require the company to access and disclose it?	Except where extraterritorial effect is explicitly provided for under relevant Chinese law provisions, the access and assistance obligations do not have potential extraterritorial effect.	The access and assistance obligations described in IPA are generally considered to have potential extraterritorial effect. The ISA contains specific provisions enabling applications for warrants affecting property outside the British Islands where the warrant is required for the investigation of certain serious offences. It is not expressly clear whether the powers under the PACE, CJPA, PCA and TA are intended to have extraterritorial effect.	Most laws relevant to communications assistance obligation, such as the Electronic Communications Privacy Act and the Foreign Intelligence Surveillance Act, have extraterritorial application.	Technical Assistance Notices and Technical Capability Notices have extraterritorial effect. However, it is a defence for an organisation not to comply with a notice if compliance would require that organisation to take actions in a foreign jurisdiction that would be illegal in that jurisdiction.	German law enforcement agencies may not access data stored abroad (if such data is protected against unauthorised access) without assistance from the other country's government unless exceptions apply.	Swedish authorities may not access data stored abroad without the assistance of the foreign authorities of the country in which the data is stored. However, if the information is located in another EU country, the Swedish authority may use an European investigation order to conduct secret wiretapping of electronic communication and secret surveillance of such communication in that EU country.	Assistance and access obligations have extraterritorial effect pursuant to mutual assistance arrangements with foreign countries. In addition, telecommunications operators are required to provide assistance under the Electronic Communication Services Act irrespective of the location of the telecommunications equipment and consequently, telecommunications operators may be required to provide access to and information from equipment located outside Finland.

Summary of findings

	China	United Kingdom	United States	Australia	Germany	Sweden	Finland
May law enforcement and intelligence agencies compel companies to proactively collect and provide data they do not possess or provide assistance beyond their current capacity, for example, to build and create new capacity to provide decryption assistance?	Unlikely. Chinese laws require national intelligence agencies and their officers to conduct their work in accordance with laws and prohibit them from abusing their administrative powers, infringing upon the legitimate interest of citizens and organizations.	A Targeted Equipment Interference Warrant or a Technical Capability Notice may, in some cases, require a telecommunications operator to take steps to obtain data that they do not yet possess. However, they are subject to necessity and proportionality restrictions and must be approved by the Secretary of State or a Judicial Commissioner, respectively.	No, companies are generally not required to produce data they do not possess nor compelled to proactively collect data for prospective assistance requests.	Yes, provided that the requirement should be practicable, technically feasible, proportionate and reasonable, as well as meeting the requirements set out in section 317ZG of the *Telecommunications Act 1997 (Cth).*	Authorities may not require a company to provide assistance over and above the search and seizure rights requested in the order. In particular, companies are not obliged to decrypt encrypted data. If data is password-protected, such passwords may be seized and may be used to access the password-protected data.	Yes, Network and Service Providers may be required to disclose information (including the contents of electronic messages) that is otherwise subject to a general duty of confidentiality. This is only possible at the request of specified authorities (for example, the public prosecution authority or the police) and provided that the applicable legislative conditions are met. Subject to certain constraints, Network and Service Providers may also be required to enable secret surveillance, provide related technical assistance and assist secret data reading.	Companies may also be compelled to proactively collect and store data based on a data retention order. However, if complying with a data retention order is not technically possible, a company cannot be compelled to make technical changes to enable the collecting of data under a data retention order.

Summary of findings

	China	United Kingdom	United States	Australia	Germany	Sweden	Finland
Are intelligence services authorized to compel companies to embed backdoors into the products?	No Chinese laws compel companies to plant backdoors.	While the laws do not expressly authorise governmental authorities to require or prohibit specific designs of telecommunications equipment, features or system configurations for use in commercially-available products, the planting or leaving open of, "backdoors" may be a possibility through Targeted Equipment Interference Warrants or Technical Capability Notices.	The US laws do not explicitly allow the planting of "backdoors" into equipment. However, whether the US government can compel "backdoors" was an issue of substantial debate in the last few years and it is possible that the All Writs Act of 1789, 28 U.S.C. § 1651 could be used to seek compulsory installation of "backdoors".	Although designated communications providers cannot be compelled to introduce or leave open a "systemic weakness or systemic vulnerability" that will render methods of authentication or encryption ineffective where that affects an organisation's customers generally, this can be required for a "targeted technology" being used by the organization or an individual under investigation as long as it does not expose other parties lawfully using the technology to suffer loss or damage.	The TKG obliges telecommunication providers to provide technical facilities for interception measures, including the obligation to implement such measures into new technologies used for telecommunications (such as Voice-over-IP technology) and to allow the installation and operation of equipment to implement interception measures.	Possibly. The Swedish Ministry of Justice has publicly stated that under the Act on Secret Data Reading (effective from 1 April 2020), Network and Service Providers may be obliged to assist with secret data reading. Such assistance could include allowing Swedish authorities to use software or hardware in technical equipment to facilitate access to the contents of messages (including potentially installing trojans to tap calls in encrypted programs and applications).	No. Finnish laws do not authorize intelligence services to require or prohibit specific designs of telecommunications equipment, facilities, services, features, or system configurations in commercially available products. However, telecommunications operators are under obligations in the Electronic Communications Services Act to ensure that networks and communications services are designed and maintained such that access and assistance orders (including those relating to interception and traffic data monitoring) can be implemented.

	China	United Kingdom	United States	Australia	Germany	Sweden	Finland
						In addition, Network and Service Providers[3] may be required to grant Swedish authorities access to communications networks to install equipment that affects the traffic flow between two communicating devices. However, these measures are subject to proportionality restrictions.	
Are there any cases that companies have challenged intelligence agencies' access and assistance request? What were the consequences?	No	No	Certain companies succeeded in challenging gag orders but there have been few publicly-recorded challenges by companies to intelligence assistance requests by intelligence agencies.	No. It is not possible for an organisation to refuse compliance or to challenge a validly issued Technical Assistance Notice or a Technical Capability Notice.	Compliance with compulsory requests may only be refused or challenged on grounds of invalidity (for example, missing formal requirements or not issued in accordance with statutory law) or if such request is technically unfeasible. No public cases available.	The obligations of Network and Service Providers to assist during secret data reading are mandatory. There are possible grounds to challenge requests for access and assistance that are based on other grounds of access (such as search warrants).	No.

(3) While the statutory obligation to assist with secret data reading under the *Act on Secret Data Reading* is limited to Network and Service Providers only, the application of the *Act on Secret Data Reading* appears to have a wider scope and extend to cover communications services, storage services (e.g. cloud services) and similar services. While it is unlikely that upstream equipment vendors and other upstream suppliers will be directly obliged to provide assistance under the *Act on Secret Data Reading*, it remains to be seen whether the obligation on Network and Service Providers to provide assistance might have the de facto effect of requiring them to require their equipment vendors and software providers to facilitate secret data reading by building "backdoor" capabilities into their equipment.

	China	United Kingdom	United States	Australia	Germany	Sweden	Finland
Is there criminal liability for non-compliance of the assistance request raised by intelligence services?	There has been no published case (and we are not aware of any case) that imposes criminal liability on a Chinese person for non-compliance of the assistance request raised by intelligence services.	Yes. Failure to comply with a request under IPA or RIPA or the powers of seizure under the PCA, PACE, CJPA, TA and ISA may lead to criminal liability. In addition, failure to comply with "gag orders" may also amount to a criminal offence.	Yes, contempt of court findings can possibly result in jail terms for individuals.	Yes, it is a criminal offence punishable by up to 5 years' imprisonment to disclose any information obtained about or pursuant to a Technical Assistance Notice or a Technical Capability Notice.	Yes, failure to comply with an access or assistance request may lead to personal liability of the acting persons, which may include a detention order for up to 6 months.	No. There is in general no criminal liability for the failure to comply with assistance requests. While the obligation on Network or Service Providers to assist during secret data reading under Act on Secret Data Reading is mandatory, there is no criminal penalty imposed on the Network or Service Provider if it fails to assist. However, refusal to comply with e.g. the information request of an authority may entail the supervisory authority to impose an injunctive order on the company that also may be combined with a penalty (that will be payable unless the company complies with the request).	Generally, there is no criminal liability for failing to comply with access or assistance orders. However, refusal to comply with a data retention order may amount to contumacy to the police under the Criminal Code. Depending on the circumstances other criminal sanctions against the persons refusing to act on access or assistance request may also be available.

Methodology

Simmons & Simmons has considered and set down in this paper a comparison of access and assistance laws in seven jurisdictions. In preparing the contents of this paper, we consulted with and sought responses from specialist legal counsel across our international network on a detailed questionnaire looking at the relevant laws, processes for seeking access and assistance, extraterritorial effect, processes for challenging requests for governmental access and assistance and consequences of non-compliance.

Jurisdictional Analysis

China

For the purposes of the jurisdictional review in this paper only, references to "China" or "PRC" refer to mainland China, and do not include the Hong Kong Special Administrative Region, Macao Special Administrative Region or Taiwan region.

Relevant laws

The relevant laws include:

- The *Counterespionage Law* which grants national security authorities the power to examine identifications of Chinese and foreign citizens, query relevant organisations and individuals and access private premises. It also requires companies to "facilitate or otherwise assist counterespionage activities", including providing information or evidence when a national security authority investigates espionage acts.[4]
- The *Anti-Terrorism Law* which requires companies to "assist and cooperate with relevant authorities on anti-terrorism activities", including providing requested information and materials and, for "telecommunication service operators and internet service providers", providing "technical support and assistance such as technical interfaces and decryption" for the authorities' investigation of terrorist activities.[5]
- The *Cyber Security Law* which requires "network operators"[6] to provide "technical support and assistance" to public security authorities and national security authorities in their national security protection and crime investigations.[7]
- The *National Intelligence Law* which grants national intelligence agencies the authority to request relevant entities and individuals to provide "support, assistance and cooperation" necessary for their intelligence activities.[8]
- The *National Security Law* which imposes on citizens and entities obligations to protect national security, including without limitation, truthfully providing "evidence to their knowledge" of activities endangering national security, facilitating or providing assistance to national security work, and providing necessary support and assistance to national security, public security and military authorities.[9]

The Chinese law enforcement agencies' requests for access and assistance are subject to general restrictions under these laws. For example, such requests may only be made for the purpose of, and to the extent necessary for, national security protection and criminal investigations, within the scope of authority of the requesting agency; the requested information may only be used for the stated purpose with due protection of business secrets and personal privacy; and the agency must respect lawful rights of the requested entities and individuals. In addition, relevant authorities' exercise of power is subject to general restrictions under the *PRC Constitution*, the *Administrative Review Law*, the *Administrative Procedure Law* and the *Criminal Procedural Law*, which generally limit the authority to examine correspondence of citizens, search private premises and seize documentation and other private properties, restrict employment of "technical investigation measures" and grant citizens and entities rights to challenge administrative actions.[10]

(4) Articles 9, 10, 20 and 22 of the *Counterespionage Law*.
(5) Articles 9, 18, 19(2) and 51 of the *Anti-Terrorism Law*.
(6) "Network operators" are defined as the network owners, managers and network service providers.
(7) Article 28 of the *Cyber Security Law*.
(8) Articles 7 and 14 of the *National Intelligence Law*.
(9) Article 77 of the *National Security Law*.
(10) Article 40 of the PRC Constitution protects "freedom and privacy of personal correspondence" of any PRC citizen and only permits public security or procuratorial authorities to examine correspondence "to satisfy the needs of national security or of an ongoing criminal investigation", provided that the examination is carried out "in accordance with procedures prescribed by law". Article 41 of the *PRC Constitution*, Article 2 of the *Administrative Procedure Law* and Article 2 of the *Administrative Review Law* grant citizens and entities rights to seek administrative review or sue an administrative agency for infringement of their lawful rights by administrative actions of such agency or its officials. Of particular relevance, section 6(5) of the Administrative Review Law permits an entity to seek administrative review on administrative actions that "infringe upon its lawful decision-making power for operation". The Criminal Procedure Law provides for detailed procedural requirement for the scope, process and documentation of search and seizure and technical investigation measures conducted by public security authorities and procuratorial authorities during criminal investigations.

Extraterritoriality

Except where extraterritorial effect is explicitly provided for under relevant Chinese law provisions, the access and assistance obligations do not have potential extraterritorial effect. For example, Article 11 of the Anti-Terrorism Law extends criminal jurisdiction over terrorist crimes committed outside PRC[11] . Moreover, the PRC Ministry of Foreign Affairs has repeatedly indicated the PRC government's general objection to extraterritorial or long-arm jurisdiction.

Chinese law does not grant relevant authorities the power to compel an overseas affiliate of a Chinese company to disclose or grant access to data stored overseas. Generally speaking, Chinese law enforcement authorities do not have authority to enforce Chinese laws against or compel assistance from foreign entities, except indirectly via judicial assistance of foreign law enforcement authorities under relevant bilateral treaties.

Scope of access and assistance powers

As stated above, the Chinese law enforcement and intelligence agencies' requests for access and assistance are subject to general restrictions under relevant laws. Such requests may only be made for the purpose of, and to the extent necessary for, national security protection and criminal investigations, within the scope of authority of the requesting agency.

Companies are generally not required to produce data they do not possess nor are they compelled to proactively collect data which they do not possess for assistance requests. The laws generally require law enforcement authorities and national intelligence agencies and their officers to conduct their work in accordance with the law and prohibit them from abusing their administrative powers, infringing on the legitimate interests of citizens and organisations, taking advantage of their positions, seeking personal gains, or disclosing national secrets, commercial secrets or personal information. Officers are required to show identification and search warrants when searching private premises and seizing documentation and properties. Search and seizure activities must be witnessed and properly documented. When investigating national security crimes, terrorism, organised crimes or other crimes of a severe nature, authorities' requests for access and assistance may include employing "technical investigation measures", which are subject to stringent pre-approval by the higher-level public security and procuratorial authorities and procedures and restricted to the approved type of measures, applicable targets and time limits, pursuant to the *Criminal Procedure Law*.

Nevertheless, the scope of the access and assistance obligations would not include embedding "backdoors" into its products, according to public statements and clarifications by the PRC Premier and a number of senior governmental officials in recent years.

Consequences of failure to comply

In general, a failure to comply with the Chinese laws discussed above could lead to a range of disciplinary actions, including administrative fines or criminal sanctions, for a violating individual or entity (or its responsible personnel)[12] . However, a refusal to plant "backdoors" per se would not be considered a violation of Chinese law and further would not expose companies to being prosecuted for any criminal offences under Chinese criminal laws.

(11) Article 11 of the Anti-Terrorism Law recites: "The People's Republic of China has criminal jurisdiction over and will impose criminal liability in accordance with the law for terrorist crimes committed against the People's Republic of China or citizens or organizations thereof outside the territory of the People's Republic of China, or terrorist crimes against international treaties concluded or ratified by the People's Republic of China."

(12) For example, under the *Cyber Security Law*, non-compliance by network operators of an assistance request is subject to rectification, administrative fine of RMB50,000-500,000, and the personal in charge and other directly responsible individuals may be subject to administrative fines of RMB10,000-100,000.

United Kingdom

Relevant laws

The principal items of legislation affecting this area are the *Regulation of Investigatory Powers Act 2000* ("RIPA") and the Investigatory Powers Act 2016 ("IPA") (which replaces Part I of RIPA). These allow for telecommunications operators[13] to be issued with certain requests for mandatory assistance. In addition, police forces and various other UK authorities possess several mandatory assistance powers under the Proceeds of Crime Act 2002 ("PCA"), Police and Criminal Evidence Act 1984 ("PACE"), Criminal Justice and Police Act 2001 ("CJPA"), Terrorism Act 2000 ("TA") and Intelligence Services Act 1994 (ISA). These are broad and generally permit the seizure of information, documentation and hardware, as well as copying of data that are stored electronically and, in the case of the ISA, interference with wireless telegraphy[14].

Under the IPA, the types of mandatory assistance include:

- Interception Warrants – these allow for certain intelligence service personnel[15] to apply for warrants requiring a telecommunications operator to intercept communications. There are three key types of interception warrants:
    - a Targeted Interception Warrant, requiring the interception of communications described in the warrant and/or the obtaining of secondary data (data that are logically associated with or attached to the communication but do not reveal the meaning of the communication);
    - a Targeted Examination Warrant, requiring the selection of communications for examination which were intercepted using a bulk data warrant (referred to below); and
    - a Mutual Assistance Warrant, requiring an intercepting authority to either make a request for assistance in accordance with an EU mutual assistance instrument or an international mutual assistance instrument, or to provide any assistance in accordance with the same.

Except in urgent situations, decisions to issue these warrants must be approved by a judicial Commissioner.[16]

- Technical Capability Notices – these may be issued by the UK Secretary of State and impose on telecommunications operators certain obligations relating to the provision of its facilities or services, equipment, the removal of electronic protection (such as encryption) and the security of its telecommunications services. Generally, the purpose of a technical capability notice is to secure that the operator has the capability to comply with the other access and assistance powers. Therefore, a technical assistance notice may be sought alongside an interception warrant, for example. Both a notice and a warrant specify obligations on the recipient and identify steps which must be taken to comply with those obligations. Technical capability notices are subject to necessity and proportionality restrictions and must be approved by a Judicial Commissioner, an office and process which were specifically established by the IPA. A Judicial Commissioner must have held a judicial position at least as senior as a high court judge to be appointed.

(13) A telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK. "Telecommunications service" means any service that provides access to, and facilities making use of, any telecommunication system, and "telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the UK or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electromagnetic energy. The definitions of "telecommunications service" and "telecommunication system" are intentionally broad.

(14) "Wireless Telegraphy" is defined in the Wireless Telegraphy Act 2006 as the emitting or receiving, over paths that are not provided by any material substance constructed or arranged for the purpose, of electromagnetic energy of a frequency not exceeding 3,000 gigahertz that is, broadly speaking, for the purposes of communicating information.

(15) For example, the Security Service, the Secret Intelligence Service or Government Communications Headquarters), the heads of certain police and law enforcement services, the commissioners for Her Majesty's Revenue & Customs or, in the case of an EU mutual assistance instrument or an international mutual assistance agreement, a person who is the competent authority of a country or territory outside the UK.

(16) If there is an urgent need to issue the warrant before approval can be obtained, approval must be obtained within three working days of the date on which the warrant is issued. If the Judicial Commissioner subsequently refuses to grant approval, then steps taken under the warrant must stop as soon as possible.

- Authorisations – a designated senior officer of a relevant public authority may authorise any officer of the authority to obtain communications metadata from a telecommunications operator by any specified conduct specified in the authorisation.[17] Such conduct may include requiring a telecommunication operator to obtain the data (if it is not already in their possession) and to disclose this data in accordance with the authorisation. An authorisation must specify certain details including: the position held by the designated senior officer granting the authorisation, the limited purposes for which it is being granted, the conduct for which it is authorised, the type of data to be obtained, and to whom the data will be disclosed. The authorisation must be necessary (for certain purposes including national security, UK economic well-being and public safety) and must be proportionate to what is being sought.
- Equipment Interference Warrants – the Secretary of State may require a telecommunications operator to secure interference with any equipment[18] – interference being access to a device, system or network, for example the installation of spyware and monitoring of communications in real time – for the broad purposes of obtaining communications[19] and equipment data[20], or any other information. Equipment interference warrants cannot be used to access live communications (where an interception warrant will be necessary). Equipment interference warrants are subject to necessity and proportionality restrictions and must be approved by a Judicial Commissioner.
- Bulk Data Warrants – the Secretary of State can require the interception of overseas-related communications and/or the obtaining of secondary data from such communications by a telecoms operator on the grounds of national security. The Secretary of State must consider that the warrant is necessary in the interests of national security.

In addition, under RIPA Part I, Chapter II (which is expected to be repealed later in 2019), broad-ranging powers exist for public authorities (such as the police force, certain criminal and intelligence services, Her Majesty's Revenue and Customs, and other persons), to give a notice to Communications Service Providers[21] requiring access to specified communications data[22] where it is necessary on grounds of public interest such as national security, preventing or detecting crime, the economic well-being of the UK or public health and safety. RIPA also includes provisions that are designed to facilitate access to data that are in encrypted form.

Under the ISA the Security Service, Intelligence Service or GCHQ may apply to the Secretary of State for a warrant authorising the taking of any such action specified in the warrant in respect of any property so specified or in respect of wireless telegraphy. Whilst this is a broad-ranging warrant, the Secretary of State must be satisfied that the action prescribed is proportionate to what it seeks to achieve.

(17) Authorisations only apply to communication metadata (the "who, when, where and how" of a communication) rather than "content data" (what is said or written in the communication that reveals the meaning of the communication.
(18) "Equipment" is defined as any equipment that produces electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment.
(19) "Communication" is defined as including (i) anything comprising speech, music, sounds, visual images or data of any description; and (ii) signals serving either for the impartation of anything between persons, between a person and a thing, or between things, or for the actuation or control of any apparatus.
(20) "Equipment data" is defined as systems data or secondary data (i.e. data logically associated with or attached to the communication). Systems data means any data that enables or facilities or identifies or describes anything connected with enabling or facilitating, the functioning of any telecommunication system (including any apparatus forming part of the system) or any telecommunications service provided by means of a telecommunication system.
(21) A communication service provider is akin to a telecommunications operator under the IPA.
(22) Communications data includes data that identifies (i) the devices called from and to; (ii) the location of the communicating parties; (iii) the nature of the service being used; (iv) the duration of the communication; and (v) any other details held by a communications service provider about the subscriber to the service (for example, their address).

Extraterritoriality

The access and assistance obligations described in IPA are generally considered to have potential extraterritorial effect.

It is not expressly clear whether the powers under the PACE, CJPA, PCA and TA are intended to have extraterritorial effect, but extraterritorial application cannot be excluded in certain cases (for example, where mutual assistance arrangements in place with other countries). The ISA contains specific provisions enabling applications for warrants affecting property outside the British Islands where the warrant is required for the investigation of certain serious offences.

Scope of access and assistance powers

The scope of the access and assistance obligations discussed above are subject to judicial and administrative limitations. For example, search warrants obtained under PACE and CJPA must have court approval confirming the search warrant's lawfulness before it can be exercised.[23] Once issued, these search warrants grant powers of seizure, including the taking of digital copies of data that is stored in electronic form.

For warrants issued under the IPA, the issuer must be satisfied that a telecommunications operator is capable of providing the requested assistance, whether the aims could reasonably be achieved by other less intrusive means and whether the level of protection to be applied to requested information should be higher because of the particular sensitivity of that information. In addition, warrants and notices under the IPA and RIPA are generally only effective for a short period (typically one month), after which the warrant must be renewed, modified or cancelled. This quick "issue-review" framework imposes obligations on the governmental applicant to re-assess whether the warrant or notice continues to be necessary or proportionate.

While Targeted Equipment Interception warrants are subject to limitations, these purposes for which such warrants may be issued are relatively broad. Notably, the Secretary of State must be satisfied that the warrant is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or – rather broadly – the interests of the economic well-being of the UK (so far as those interests are also aligned with the interests of national security). The Secretary of State must also be satisfied that the actions are proportionate to what is sought to be achieved by the conduct – a judgment that will to some extent depend on the exercise of executive discretion.

Technical Capability Notices may also, in some cases, require a telecommunications operator to take steps to obtain data that they do not yet possess. However, as with warrants, Technical Capability Notices are subject to necessity and proportionality restrictions and must be approved by a Judicial Commissioner who will consider necessity and proportionality when deciding whether to approve the decision of the Secretary of State. In addition, the notice may only specify an obligation if the Secretary of State considers that it is practicable for the relevant operators to comply with those requirements.

While the laws do not expressly authorise governmental authorities to require or prohibit specific designs of telecommunications equipment, features or system configurations for use in commercially-available products, the planting or leaving open of, "backdoors" may be a possibility in practice. For example, the Targeted Equipment Interference Warrant can require a telecommunications operator to secure interference with any equipment and to obtain communications, equipment data or other information from the equipment – this could amount to a power to compel the embedding of a form of "backdoor" in the context of an investigation or intelligence gathering. Similarly, the powers of the Secretary of State to issue Technical Capability Notices to assist in giving effect to interception, equipment interference and bulk acquisition warrants and notices or authorisations could also be used to compel telecommunications operators to embed types of "backdoors". There are no specific

(23) The application for a search warrant must set out as much information as possible (otherwise it may be rejected by the court as incomplete), including (i) the grounds on which the application is being made (i.e. that there are reasonable grounds for believing that the material to be seized is evidence in relation to an offence and that it is necessary to seize it in order to prevent the evidence being concealed, lost, altered or destroyed); (ii) the address of the premise to be entered and searched, including the parts of any multiple premises; and (iii) so far as practicable, the articles or persons sought.

obligations in the legislation discussed here for equipment manufacturers to assist telecoms operators to enable them to comply with such requirements. It is however possible that such requirements could be mandated under the contract between the telecommunications operator and the equipment manufacturer.

The concept of "interference" in the context of these laws is broad and can include a range of techniques – including interference carried out remotely or physically by interacting with the equipment or covertly downloading data from a device or remotely installing software enabling material to be extracted or software that enables keylogging and tracking of keystrokes.[24]

There are no specific grounds to resist the other general powers of access and seizure under PACE, CJPA, PCA, TA and ISA (and as a matter of procedure, this is because the relevant checks and balances have been undertaken by way of, for example, court approval prior to the issuance).

Consequences of failure to comply

Failure to comply with a request under IPA or RIPA may amount to criminal liability. In addition, there are also "gag order" provisions, which prohibit a telecommunications operator or any person employed or engaged in its business, to disclose without reasonable excuse the existence of any requirement imposed under an authorization. Breach of these provisions may amount to a criminal offence (including fines and imprisonment imposed on individual employees).

Failure to comply with the powers of seizure outlined above under the PCA, PACE, CJPA, TA and ISA can result in contempt of court proceedings, which could lead to criminal liability, prison sentences, fines or sequestration of assets.

(24) That said, interference will also be subject to considerations against the Human Rights Act 1998, though the balance of individual rights may still fall on the side of a warrant being issued.

United States

Relevant laws

There are three principal laws that govern assistance obligations relating to communications in the US. These provide for:

- Wiretaps – under the *Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010* ("CALEA"), authorities may seek orders, warrants and subpoenas for wiretaps. Under CALEA, communications carriers must ensure that telecommunications equipment is capable of assisting law enforcement in conducting legally authorized wiretaps. Further, equipment manufacturers and providers of telecommunications support services must help carriers meet their CALEA compliance requirements.
- Access to communications content – the *Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2523* ("ECPA") provides authority to compel access to content of communications, and transactional information relating to communications. The ECPA is divided into three primary sections:
  - Title I: Wiretap Act – The Wiretap Act provides for interception of content of communications in-transit.
  - Title II: Stored Communications Act ("SCA") – the SCA provides for obtaining content of communications that are in storage.
  - Title III: Pen Register Act – the Pen Register Act provides for obtaining technical information regarding telecommunications, for example to whom calls were placed and/or from whom received.
- Electronic surveillance – the *Foreign Intelligence Surveillance Act, 50 U.S.C. Chapter 26* ("FISA"), permits the US government to conduct electronic surveillance in international counter-espionage and terrorism investigations. A FISA order may require a service provider to facilitate this surveillance and also prohibit it from disclosing the existence of an investigation. FISA orders are highly classified and rarely disclosed publicly.

In addition, the Federal Bureau of Investigations can also compel disclosure of customer records held by companies through the use of National Security Letters, which are similar to administrative subpoenas. Service providers who turn over customer records are prohibited from disclosing the existence of the investigation without a court order.

General police powers are also reserved for the US states under the 10th Amendment of the US Constitution and vary from state to state. At the federal level, a wide range of law enforcement agencies under all branches of the US government are empowered through various US Code provisions to investigate federal matters. The scope of federal law enforcement powers is broad (including search and seizure), in particular where national security is a concern, and was expanded in 2001 by the *USA PATRIOT* Act and its subsequent amendments. These powers remain limited by constitutional protections such as due process under the 5th and 14th Amendments; and the 4th Amendment right against unreasonable search and seizure.

Extraterritoriality

With the exception of CALEA, which does not apply outside of the US, the laws mentioned above all have extraterritorial application. For example, FISA directly applies both inside and outside of the US.[25]

(25) As explicitly laid out in the *FISA Amendment Act of 2008*.

The ECPA's extraterritorial reach has been the subject of substantial debate since its enactment, with many courts applying a "strong and binding" presumption against extraterritoriality. However, the *CLOUD Act* was enacted in March of 2018 to amend the SCA and clarifies that an SCA warrant requires disclosure of customer or subscriber information regardless of whether the information is located within or outside of the US.[26] Foreign governments that have an executive data sharing agreement with the US are also able to have the benefit of mandatory compliance with disclosure orders.

Scope of access and assistance powers

While the scope of the access and assistance powers depends on the language of the relevant statute, companies are generally not required to produce data they do not possess nor are they usually compelled to proactively collect data for prospective assistance requests.[27]

Companies are compelled to provide assistance only to the extent their technological capacity allows them to do so. CALEA is the only statute that speaks to this technology capacity, by establishing minimum requirements for telecommunications equipment to include capabilities to assist with legally authorized wiretaps.

There are also no specific affirmative obligations under US laws to decrypt content or install software. CALEA explicitly states that carriers are not required to assist with decrypting, or ensuring that the government can decrypt communications, unless the encryption was provided by the carrier and the carrier already possesses the information necessary for decryption. Under the ECPA, sharing agreements between the US and qualifying foreign governments are explicitly prohibited from creating any obligations that require providers to be capable of decrypting data.

In addition, all lawful interception in the US requires some amount of legal process, and standard of proof. For example, under CALEA, absent exigent circumstances, law enforcement or intelligence agencies must obtain a court order, warrant, subpoena, or National Security Letter to compel compliance under CALEA. Similarly, under the ECPA, US government must follow legal process (such as through subpoena, court order, or search order) to compel assistance.[28]

In relation to FISA, the Attorney General or a designated US Attorney must apply for an ex parte court order from the Foreign Intelligence Surveillance Court before it can conduct electronic surveillance in international counter-espionage and terrorism investigations. That said, under FISA the President also has power to bypass judicial process on the grounds of national security and to authorize, without a court order, electronic surveillance for a period of one year.

The US laws have a strong focus on due process. The statutes provide for processes for challenging assistance requests[29] and companies can, and do, challenge the substance of a request.[30]

(26) The CLOUD Act applies to providers of electronic communication services or remote computing services, which encapsulates ISPs, social media providers, cloud service providers and email and text messaging services.

(27) For example, the SCA explicitly clarifies that disclosure is required when within a provider's "possession, custody, or control".

(28) For example, under Title I: Wiretap Act, a law enforcement officer must (i) show probable cause that an interception will reveal evidence of certain delineated serious criminal acts; (ii) the request for interception must include a sworn statement of facts, including details as to the particular offense that has been, is being, or is about to be committed; and (iii) the requesting officer must declare whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.

(29) For example, under the Title I: Wiretap Act, providers of communications services can seek to modify or quash an order for assistance if the assistance "cannot be performed in a timely or reasonable fashion."
Under the SCA, service providers can seek to modify or quash an order for assistance "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." The SCA provides a formal process by which parties can challenge requests for user data, which process varies depending on whether the data is located in the territory of a qualifying foreign government.

(30) Companies have challenged assistance requests in several high-profile cases. For example, Microsoft (Southern District of New York); and Google (Northern District of California), 2016. Both Microsoft and Google challenged requests pursuant to the SCA for data stored overseas. Microsoft won a favourable verdict at the US Court of Appeals for the Second Circuit, and the US government further appealed to the Supreme Court. Conversely, Google lost at the District Court level, and its appeal was stayed pending the resolution of Microsoft. Ultimately, both cases were mooted by the CLOUD Act Amendment to the SCA. Another example is Facebook (Eastern District of California), 2018. The DOJ sought to wiretap ongoing voice communications on the Facebook Messenger app. Facebook challenged the request and DOJ moved to hold Facebook in contempt of court. Although the record is sealed, the Federal judge allegedly found in favour of Facebook.

In addition, companies can generally seek judicial review in US District Court to challenge a request from law enforcement or intelligence agencies for access and assistance (although this will depend on which statute the law enforcement or intelligence agency has relied on in making its assistance request).

Finally, the US laws do not explicitly allow the planting of "backdoors" into equipment and CALEA explicitly does not authorize law enforcement agencies or officers to require or prohibit specific designs of telecommunications equipment, facilities, services, features, or system configurations. However, the US government has attempted to compel Apple to provide access to locked iPhones in a series of US District Court cases, including through an order requesting Apple to effectively create a backdoor into the operating systems installed on specific iPhones. In doing so, the US government cited as a source of authority the All Writs Act of 1789, 28 U.S.C. § 1651, which permits federal courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.

Consequences of failure to comply

Fines for non-compliance with CALEA may apply. In addition, judicial remedies may be issued against companies who fail to comply with requests for assistance (for example, companies or company owners who fail to comply may be held in contempt of court). Contempt of court findings can in turn result in significant fines for companies,[31] and can also possibly also result in jail terms for individuals.

(31) For example, Microsoft and Google were both held in contempt of court for failing to comply with SCA warrants. In Google's case, the Court imposed a sanction of $10,000/day.

Australia

Relevant laws

The principal legislation is set out in Part 15 of the Telecommunications Act 1997 (Cth), which provides for the issuance of:

- Technical Assistance Notices – these allow certain law enforcement and intelligence agencies to compel telecommunications carriers,[32] telecommunications carriage service providers[33] and other designated communication providers[34] to provide assistance in relation to investigations of serious criminal offences or in relation to matters of national security.
- Technical Capability Notices – these allow the Attorney-General and Minister for Communications (jointly) to compel the same types of organisation to ensure they have a particular capability for later assistance that may be requested (including to develop a capability) and to provide similar assistance as under a Technical Assistance Notice.

Technical Assistance Notices and Technical Capability Notices may compel designated communication providers to undertake a broad range of things, including – potentially – providing source code, decrypting encrypted information (where the organisation already has this capability), providing passwords or removing authentication requirements, installing applications or technology on an organisation's systems and providing services in a particular way that suits intelligence and law enforcement agencies' requirements.[35] The scope of the notices may also, potentially, require the creation of new capabilities, provided they meet the requirements set out below relating to practicability, technical feasibility, proportionality and reasonableness (and do not require the introduction of system weaknesses or system vulnerabilities). These notices do not cover the collection and storage of metadata or the provision of interception capabilities, which are governed by separate legislation.[36]

In addition, more general powers of search and seizure also apply. For example, the *Crimes Act 1914 (Cth)* allows for government agencies accompanied by the Australian Federal Police to obtain and execute search warrants on premises where there are reasonable grounds to believe there is evidence at those premises related to a criminal offence.[37] Some searches for serious offences can be carried out covertly where notice of the search does not need to be given until a considerable time afterwards.

(32) A telecommunications carrier is essentially a telecommunications network owner or operator (see section 42 *Telecommunications Act 1997 (Cth)*).

(33) A carriage service provider supplies carriage services to the public using a carrier's network (see section 87 *Telecommunications Act 1997 (Cth)*).

(34) "Designated Communications Provider" is broadly defined and captures anyone other than a carrier or carriage service provider, who provides online services (such as websites, mobile apps, APIs, cloud data storage), hardware and hardware components (such as networks, devices, computers), software (such as VoIP and messaging apps) and installation or maintenance of any of these for use or likely use in Australia.

(35) See section 317E of *Telecommunications Act 1997 (Cth)*, which sets out a broad range of activities which can be compelled, including removing electronic protections, providing technical information, installing or testing software or equipment, facilitating access to services, hardware, software etc, assisting with development and testing of technology or capability, modifying the characteristics of services, notifying of relevant changes to services, hardware software etc and concealing covert access by or in assistance of law enforcement and intelligence services.

(36) Interception capability is an obligation of carriers under section 313 *Telecommunications Act 1997 (Cth)*. Recording metadata and providing access to stored communications such as email, SMS or voicemail is an obligation of carriers and carriage service providers under the *Telecommunications (Access and Interception) Act 1979 (Cth)*.

(37) Similar rights apply in each Australian State relating to offences against State criminal law. See, for example, sections 46-80 of the *Law Enforcement (Powers and Responsibilities) Act 2002 (NSW)*.

Notably, there is also a new 'Computer Access Warrant' that can be issued under recent legislation made in relation to the *Surveillance Devices Act 2004 (Cth)*[38] which allows covert entry to premises to access data on a computer, or remote access to a computer, and taking a copy of any data that appears relevant to the investigation (or if it is encrypted, a copy of all the encrypted data). A computer access warrant has to be issued by a judge or senior member of the Administrative Appeals Tribunal.

Extraterritoriality

Technical Assistance Notices and Technical Capability Notices apply to any designated communications provider, which captures anyone who manufactures or supplies the relevant communications equipment or service for use in Australia, or likely use in Australia, even if they have no local presence. However, it is a defence for an organisation not to comply with a notice if compliance would require that organisation to take actions in a foreign jurisdiction that would be illegal in that jurisdiction.

To the extent that the notices require an activity for which a government agency also requires a warrant or authorisation,[39] it would be necessary to also consider whether such a warrant has extraterritorial effect. Warrants are granted under various legislation in Australia, but notably the Computer Access Warrant[40] permits activities to be undertaken in respect of computers and devices located outside Australia where there has been a request by a foreign law enforcement agency.

In addition, any mutual cooperation arrangements with foreign law enforcement would allow the Australian Federal Police or a State police force to request the issue of a search warrant relating to premises or people in Australia, a Computer Access Warrant for a computer located in Australia or overseas, and a Technical Assistance Notice or Technical Capability Notice, to assist in the enforcement of serious offences in that foreign country.

Scope of access and assistance powers

It is not possible for an organisation to refuse compliance or to challenge a validly issued Technical Assistance Notice or a Technical Capability Notice.[41] Instead, the Australian framework sets out a number of preconditions which should be satisfied prior to issuance. Those requirements are that the notices should be practicable, technical feasible, proportionate and reasonable, as well as meeting the requirements set out in section 317ZG of the *Telecommunications Act 1997 (Cth)*.

Unlike the UK framework which favours an "issue-review" procedure in relation to the issuance of warrants and notices, the Australian framework introduces a pre-issuance consultation period for Technical Capability Notices during which an organisation may discuss issues such as reasonableness, proportionality and other preconditions which should be met. The consultation period allows organisations to seek independent assessment by a retired judge and a technical expert with appropriate security clearances to confirm whether the notice breaches section 317ZG and the consultation period is required, except in urgent situations or where the organization waives the obligation to consult.

Unlike the quick "issue-review" procedure in the UK, Technical Assistance Notices and Technical Capability Notices may be issued for periods of up to twelve months.[42] In addition, the consultation period does not apply for Technical Assistance Notices. Technical Assistance Notices can be issued by the Director-General of Security (for assistance needed by ASIO, the Australian Security Intelligence Organisation) or by the chief officer of the Australian Federal Police, the Australian Crime Commission or a State or Territory police force (for assistance needed by that body) and cannot be refused once issued.

(38) *Surveillance Devices Act 2004 (Cth)*, sections 27A-27J.
(39) See the next section on scope of access and assistance for further information on this point.
(40) Computer Access Warrants can be issued under the *Surveillance Devices Act 2004 (Cth)* and are part of the suite of new access and assistance laws introduced in Australia in December 2018.
(41) However, it is possible to seek judicial review of decisions to issue notices or warrants under established administrative law grounds – for example, that the decision to issue a notice is beyond the power of the issuer or there is a legal or procedural defect in the decision to issue the notice.
(42) However, if no expiry date is specified, the default validity period is 90 days for Technical Assistance Notices and 180 days for Technical Capability Notices.

Technical Assistance Notices and Technical Capability Notices cannot be used if they require an activity for which an agency requires a warrant or authorisation and they do not have such warrant or authorisation.[43] If an organisation is consulted about or given a Technical Assistance Notice or Technical Capability Notice, details of the relevant warrant or authorisation should be given so that the organisation is able to assess whether or not there is any question as to the validity of the notice.[44]

Finally, the issuer of Technical Assistance Notices and Technical Capability Notices must be satisfied that the notices are reasonable and proportionate and that compliance with the notice by the organisation is practicable and technically feasible.[45]

Although designated communications providers cannot be compelled to introduce or leave open a "systemic weakness or systemic vulnerability" that will render methods of authentication or encryption ineffective where that affects an organisation's customers generally, this can be required for a "targeted technology" being used by the organisation or an individual under investigation as long as it does not expose other parties lawfully using the technology to suffer loss or damage.

The definitions of "systemic weakness" and "system vulnerability"[46] – which attempt to draw a distinction between weaknesses that affect a "whole class of technology" as opposed to only a particular "target technology" – are vaguely drafted and there are widely-held industry concerns that the laws could be used to compel the development of "backdoors" or capability to break the encryption of data (depending on whether doing so is proportionate, technically feasible and reasonable and whether doing so compromises the privacy of its customers generally). There will likely be arguments that developing an encryption capability is beyond what can be required by a Technical Capability Notice, but the scope of the laws remain untested at the time of writing this paper.

Consequences of failure to comply

It is not possible to refuse compliance with Technical Assistance Notices or Technical Capability Notices. Penalties for non-compliance with a Technical Assistance Notice or Technical Capability Notice (unless a defence applies) may amount to significant civil penalties.[47] It is also a criminal offence punishable by up to 5 years' imprisonment to disclose any information obtained about or pursuant to a Technical Assistance Notice or a Technical Capability Notice.[48]

Where a search warrant or Computer Access Warrant authorises entry to certain premises, the law enforcement or intelligence officers executing the warrant are entitled to exercise such force as is reasonably necessary to gain access to premises and to conduct the search. Any obstruction of the execution of the warrant may lead to arrest for obstruction of justice.

(43) Telecommunications Act 1997 *(Cth),* section 317H.
(44) Warrants and authorisations are issued under other legislation applicable to the investigation of crime or national security risks, including the newly introduced Computer Access Warrant, which can be issued under the Surveillance Devices Act 2004 (Cth) and allows physical or electronic access to data on computers and other devices.
(45) Reasonableness and proportionality are to be considered against a variety of factors set out in section 317T of the Telecommunications Act 1997 (Cth), including, for example, the interests of national security and the legitimate interests of the Australian community in relation to privacy and cybersecurity.
(46) A "systemic weakness" and "systemic vulnerability" is defined as a weakness or vulnerability that affects a whole class of technology but does not include a weakness or vulnerability that is selectively introduced to one or more target technologies connected with a particular person (but it is immaterial whether the person can be identified). For these purposes, a "target technology" may include a particular electronic service so far as the service is likely to be used by a particular person". If a weakness or vulnerability is to be selectively introduced into a particular target technology, any act or thing that will, or is likely to, jeopardise the security of any information held by any other person (which includes where otherwise secure information can be accessed by an unauthorised third party) is also to be considered a "systemic weakness" or a "systemic vulnerability".
(47) Non-compliance (unless a defence applies) is punishable by fines of approximately AU$10 million for corporations and AU$50,000 for individuals involved in the contravention.
(48) However, designated communications providers may issue reports about how many notices it has received (if any). Information about individual notices, however, must not be disclosed.

Germany

Relevant laws

The principal legislation is set out in the German Code of Criminal Procedure (Strafprozessordnung) (StPO),[49] which provides rights for law enforcement agencies to compel companies to provide access to stored data, provided that these requests meet certain legitimacy requirements. In particular, access to information technology systems and electronically stored data can be enforced by way of search and seizure.

There are a range of further stipulations on investigation or intelligence gathering and corresponding assistance obligations which apply to commercial providers of telecommunications services,[50] and with the exception of the TKG and the G10 (described below), also apply to other companies that may possess data relevant to criminal offences.[51] These laws include:

- *Federal Telecommunications Act (Telekommunikationsgesetz)* ("TKG")
- *Act on the Restriction of the Secrecy of Letters, Posts and Telecommunications (Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses)* ("G10")
- *Customs Investigation Service Act (Zollfahndungsdienstgesetz)* ("ZFdG")
- *Federal Criminal Police Act (Bundeskriminalamtgesetz)* ("BKAG")
- *Federal Intelligence Service Act (Bundesnachrichtendienstgesetz)* ("BNDG")

Extraterritoriality

Under the StPO, German law enforcement agencies may not access data stored abroad (if such data is protected against unauthorized access, such as being password protected or encrypted) without assistance from the other country's government (*Rechtshilfeersuchen*), unless the company provides the relevant access data to the authority, or the access details are found by the authority in the course of search and seizure measures or it is unclear whether the data is hosted abroad or in which country the data is located.

German investigation authorities are dependent on close cooperation with foreign authorities and their assistance.[52] Within the European Union, a competent authority in the requesting Member State may, in accordance with the requirements of its national law, make a request to a competent authority in the requested Member State for interception of telecommunications in criminal investigations.[53]

Scope of access and assistance powers

The assistance measures available under the StPO always require a search warrant to be obtained from a court per request of a public prosecutor and are only permitted in the case of suspicion of serious offences.[54]

(49) See sections 94, 95, 100a (telecommunications monitoring), 100b (online searches), 100j (request for inventory data ("*Bestandsdatenauskunft*")), 103 (search of premises), 110 (electronic storage media).
(50) Telecommunications services are defined as services normally provided for remuneration consisting in, or having as their principal feature, the conveyance of signals by means of telecommunications networks, and includes transmission services in networks used for broadcasting, such as internet access or internet network providers, or providers of Voice-over-IP services.
(51) There is some debate as to whether modern messenger services (such as 'Whatsapp' or 'Gmail') should be characterised as "telecommunications providers" under the TKG (and compelled under the TKG to give authorities access to communications data) or whether they should be characterised as service providers under the Telemedia Act (Telemediengesetzt) ("TMG") which does not impose obligations to implement interception measures. The European Court of Justice has recently decided that Google's Gmail should not be characterised as a telecommunication service under the TKG and should be treated as a service provider under the TMG. As a result, monitoring obligations currently do not apply to Over-the-Top services that function in a similar way to Google's Gmail service.
(52) As set out in section 59 of *Act on International Cooperation in Criminal Matter.*
(53) See Art. 18 Council Act 2000/C 197/01.
(54) Section 100e of StPO

In addition, intelligence and law enforcement agencies are permitted to issue administrative orders to oblige a telecommunications provider to give access to relevant communication data only if strict statutory pre-requisites are met:

- The legal interest to conduct such measures is of constitutional value.
- The investigation of the facts would otherwise be futile or substantially impeded.
- Monitoring is not intrusive to the core areas of a person's private life.
- Where telecommunications are monitored for strategic purposes by the Bundesnachrichtendienst (the German Federal Intelligence Service), such monitoring must be ordered by the relevant Federal Ministry and requires approval by the relevant parliamentary supervisory body.
- Where monitoring is conducted by the BND to monitor foreigners' communication in a foreign country, such monitoring must be ordered by the Federal Chancellery and approved by the Independent Committee (*Unabhängiges Gremium*) and such monitoring may not be used for the purposes of industrial espionage.

In the context of search and seizure orders, authorities may not require a company to provide assistance over and above the search and seizure rights requested in the order. In particular, companies are not obliged to decrypt encrypted data. If data is password-protected, such passwords may be seized and may be used to access the password-protected data.

In addition, the TKG obliges telecommunication providers to provide technical facilities for interception measures, including the obligation to implement such measures into new technologies used for telecommunications (such as Voice-over-IP technology) and to allow the installation and operation of equipment to implement interception measures.

Compliance with compulsory requests may only be refused or challenged on grounds of invalidity (for example, missing formal requirements or not issued in accordance with statutory law) or if such request is technically unfeasible.

Consequences of failure to comply

Non-compliance by an organisation of an access or assistance request raised by law enforcement or intelligence services may lead to personal liability of the acting persons, who may be fined with up to EUR 1,000 or even receive a detention order for up to 6 months.[55]

(55) Section 95 and section 70 of StPO.

Sweden

Relevant laws

The principal legislation targeting the telecommunications and technology sector is the Act on *Electronic Communications* (LEK). The LEK sets out mandatory obligations on providers of public electronic communications networks and publicly available electronic communications services (Network and Service Providers) to support and provide authorities with certain information in the course of investigations or intelligence gathering.

Importantly, the definition of Network and Service Providers covers electronic communications networks (for example, satellite networks, mobile networks, broadcasting networks and cable-TV networks) and services which allow users to access those networks (for example, telephone and internet subscriptions). However, one critical criterion for a service to be included in the definition of Network and Service Providers is that the service must enable communication (i.e. transfer signals) in the relevant network. This means that pure storage or content services, as well as "over the top" services (such as Skype, WhatsApp and other over-the-Internet chat services) are excluded from the definition.

Other relevant legislation includes:

- *Copyright Act* (SFS 1960:729)*;*
- *Act on Obtaining Information on Electronic Communication in the Intelligence Operations of the Crime Preventing Authorities* (SFS 2012:278)*;*
- *Act on Secret Data Reading* (SFS 2020:62 and effective from and including 1 April 2020); *and*
- *secret wiretapping and secret surveillance of electronic communication provisions contained in Chapter 27 of the Code of Judicial Procedure* (SFS 1942:740) *and the Act on Measures to Prevent Certain Specific Serious Crimes* (SFS 2007:979).

Extraterritoriality

Enforcement of the applicable laws outside of Sweden requires the assistance of foreign authorities. For example, to access emails or other data stored on servers outside of Sweden, a decision from the local court in the relevant foreign jurisdiction is required. As a general rule, the Swedish Department of Justice will forward a request for legal assistance to the relevant foreign authority. This may occur via direct engagement with the relevant foreign authority (for example, a direct request to authorities in Denmark, Finland, Iceland or Norway or other relevant authorities where there are binding mutual assistance agreements).

In addition, within the European Union, a competent authority in the requesting Member State may, in accordance with the requirements of its national law, make a request to a competent authority in the requested Member State for interception of telecommunications in criminal investigations.

Scope of access and assistance powers

The scope of the access and assistance obligations are not defined in detail in the legislation. As a general rule, Network and Service Providers have a duty of confidentiality in relation to the contents of electronic messages and other information about electronic messages. However, Network and Service Providers are obliged under the LEK (subject to certain constraints, as set out further below) to disclose such information at request of the following Swedish authorities:

- an authority that in a specific case needs the information for service of documents under the *Service of Process Act* (SFS 2010:1932);
- the public prosecution authority, police authority or other crime preventing authority;

- the enforcement authority (Swe. Kronofogdemyndigheten);
- the tax authority;
- the Swedish financial supervisory authority (Finansinspektionen); and
- the regional alarm centres.

For information that is not subject to the duty of confidentiality (for example, information for Personal Unblocking Keys to a mobile phone stored with a Network and Service Provider) or in relation to providers of technology services or products which fall outside the definition of Network and Service Providers, Swedish authorities may rely on measures under the *Code of Judicial Procedure* to access information by way of search warrant, warrant for seizure of property or court order for discovery.

In addition to the obligations set out above to provide information, under the *Act on Secret Data Reading* (which will be effective from 1 April 2020 and will be in force for five years until 25 March 2025), Network and Service Providers are obliged to assist with secret data reading[56]. While not explicitly stated in the legislation, according to public statements made by the Swedish Ministry of Justice via press conference and press release , some examples of measures that authorities may be permitted to take under this legislation include:

- accessing the content of communications by installing trojan software or devices to read the content of messages and tap calls in encrypted programs and applications as well as access social media accounts and activate the microphone or camera of the relevant equipment;
- requiring Network and Service Providers to grant access to communications networks to install equipment that actively effects and impacts the traffic flow between two communicating devices; and
- requiring Network and Service Providers to provide technical advice.

Importantly, all of these measures (i.e. search warrant, warrant for seizure of property, secret wiretapping and secret surveillance) are subject to overarching requires that (i) use of these measures are only made for the purposes stated in the Swedish legislation; (ii) there is a tangible need to use the measure; (iii) the use of the measure is the only measure available to achieve the intended results; and (iv) the type and duration of the use is in proportion with the desired result.

Other procedural and substantive limits on access and assistance rights also apply, including the following:

- disclosure of information under the LEK requires a request from the relevant authority. In order to access the actual content of messages, the requesting authority must have obtained a permit for secret wiretapping of communication networks under the *Code of Judicial Procedure*;
- secret wiretapping and secret surveillance of communication networks is subject to a court decision at the request of a prosecutor or, if there is a risk that such court decision may entail a material delay, the prosecutor may decide the matter pending the court decision;
- the obligation to provide information under the *Act on Obtaining Information on Electronic Communication in the Intelligence Operations of the Crime Preventing Authorities*, is subject to a decision by the prosecutor at the request of the police authority, the Swedish Security Service or the Swedish Customs;
- secret data reading is subject to court decision at the prosecutor's request (except if such secret data reading is requested for certain deportation or rejection orders, in which case the Swedish Security Service or the police authority may decide the matter);
- warrants for search and seizure of property are subject to a prosecutor's decision and orders for discovery must be decided by a court. Certain substantive conditions must also be met in order to obtain such warrants and orders; for example, for a search warrant to be issued, there must be a reasonable suspicion of a crime punishable by imprisonment.

(56) Here is a link to the relevant press release (including press conference video) from the Swedish Ministry of Justice: https://www.regeringen.se/pressmeddelanden/2019/10/hemlig-dataavlasning--ett-viktigt-verktyg-for-brottsbekampningen/.

While it may be possible to challenge requests under the LEK, search warrants or warrants for seizure of property or appeal court orders for discovery, the obligations to provide assistance in relation to secret data reading under the *Act on Secret Data Reading* are compulsory.

Consequences of failure to comply

- In general, there is no criminal liability for a company that fails to comply with or assist in the execution of a request from an authority. However, if a Network or Service Provider fails to comply with its obligations under the LEK (including but not limited to the obligation to assist the authorities and to adapt public communications networks in order to enable secret wiretapping and secret surveillance), an injunction ordering remediation of its non-compliance in combination with a penalty may be imposed on the Network or Service Provider. In addition, in the event that a certain obligation is included in the licence terms for the applicable licence held by the provider, and the provider is in breach of the terms, the PTA may decide to immediately recall the licence.

Finland

Relevant laws

The principal legislation relating to assistance in criminal investigations are the *Coercive Measures Act* (806/2011) and the *Police Act* (872/2011). Law enforcement officials may confiscate data or objects or request assistance by applying for a warrant for telecommunications interception or traffic data monitoring or for the issue a data retention order.

The *Military Intelligence Gathering Act* (590/2019) may also apply in relation to assistance in military intelligence gathering.

The *Electronic Communication Services Act* (917/2014) also requires public communications networks, and communications services and the communications networks and services connected to them, to meet certain requirements to be designed, built and maintained in such a manner that requests for interception and monitoring, as well as other requests related to an authority's right to obtain information, may be fulfilled.

Extraterritoriality

The obligations to assist or provide access have explicit extraterritorial effect as follows:

- mutual assistance can require the competent authority to either make a request for assistance in accordance with an EU mutual assistance instrument or an international mutual assistance instrument, or to provide assistance in accordance with the same, and therefore have an extraterritorial focus;
- an order issued under any of the laws referred to above may relate to conduct or persons outside Finland which are being investigated by the Finnish authorities;
- a telecommunications operator is required to provide assistance under the *Electronic Communication Services Act* (917/2014) to the authorities. The telecommunications operator has such obligation irrespective of the location of its equipment and consequently, may be required to provide access to and information from equipment outside Finland.

Scope of access and assistance powers

Under the *Coercive Measures Act* (806/2011) and the *Police Act* (872/2011), an object, property or document (including information contained in a technical device or in another information system or data recording platform) may be confiscated if there are grounds to suspect that:

- it may be used as evidence in a criminal case;
- it has been taken from someone in an offence; or
- it may be ordered to be forfeited.

Confiscation or copying of such data only requires an official with the power of arrest to decide to confiscate or copy the data. However, a party concerned in the matter may request the court to consider and rule on whether such confiscation may remain in force or whether copies of such data may be retained to be used as evidence. Furthermore, in apprehending a suspect in an offence or in connection with a search, the police may take possession of an object, property or document for the purpose of confiscation or copying even without an order.

In addition, the police may issue a data retention order if there is reason to suspect that data which may be of significance for the investigation of an offence may be deleted or tampered with. Warrants are not required for data retention orders, though the police must obtain a separate order or warrant to gain access to the retained data.

Importantly, these confiscation and copying powers do not apply to data in the possession of a telecommunications operator which is to be obtained by means of telecommunications interception or traffic data monitoring. Accessing data via telecommunications interception or traffic data monitoring requires a warrant issued by a competent court. In addition, telecommunications interception and traffic data monitoring is subject to the following rules:

- it may only be used if it is likely to produce information of particularly important significance in relation to an offence;
- telecommunications interception may only be directed at a message that originates from or is intended for a suspect of a "serious offence";
- unless the target of traffic data monitoring has specifically consented to it, traffic data monitoring may only be directed on a network address or terminal end device in the possession of or otherwise presumably used by a suspect of a "serious offence" (though as the specific prerequisites for what constitutes a "serious offence" vary for telecommunications interception and for traffic data monitoring, in practice, it is easier to obtain a warrant for traffic data monitoring than it is for telecommunications interception).

Under the *Military Intelligence Gathering Act* (590/2019), a warrant for interception or traffic data monitoring obtained by the Finnish Defence Forces (FDF) for intelligence purposes places similar obligations on telecommunications operators as those set out above in relation to warrants obtained by the police for criminal investigations and requires a warrant from a judge. However, the obligations to assist in military intelligence gathering are broader in that they apply also to operators of lower level OSI-network elements.

Importantly, while Finnish laws do not expressly permit the installation of "backdoors", the obligations imposed by the *Electronic Communication Services Act* to design, build and maintain networks and communications services in a way that facilitates requests by authorities to obtain information (including measures to enable interception and traffic data monitoring) could conceivably be construed broadly to compel the installation of "backdoors" in the context of allowing access and assistance (though access to information which can be obtained by way of such "backdoors" would still require an order to be issued pursuant to the procedural and substantive requirements set out above). However, it is unlikely that Finnish authorities would take such a broad reading of these provisions or attempt to request "backdoors" be installed in the absence of an express statutory power to do so. This is because the Finnish Constitution is generally understood to prohibit a government authority (including intelligence services) from acting beyond the rights granted to them by statutory law and failure of the Finnish intelligence authorities to comply with this requirement may result in potential criminal prosecution and imprisonment.

It is possible that a company may be compelled to proactively collect and store data based on a data retention order. However, if complying to a data retention order is not technically possible, a company cannot be compelled to make technical changes to enable the collecting of data under a data retention order.

As to whether there is scope to challenge access and assistance requests, telecommunications companies are unlikely to be party to the process of obtaining a telecommunications interception or traffic data monitoring order and therefore would not, in principle, be allowed to appeal the issuing of such an order. However, it is possible to appeal orders for confiscation and data retention by appealing.

Consequences of failure to comply

Generally, there is no criminal liability on corporations that do not comply with access or assistance orders. However, depending on the circumstances, other criminal sanctions against the persons refusing to act on access or assistance request may be available; for example, refusal to comply with a data retention order may amount to contumacy to the police under the Criminal Code. In addition, a person refusing to comply with a data retention order may be found guilty of contumacy to the police (i.e. failing to obey an order or prohibition issued by a police officer) under the *Criminal Code* (39/1889).

In addition, technical characteristics of communications networks (for example, the requirement to design, build and maintain networks and communications services in a way that facilitates requests by authorities to obtain information) may form part of a telecommunications company's network licence terms; failure to meet these requirements can be a breach of the operator's network licence terms and result in licence cancellation.

simmons+simmons

5278068V3