Government Access to Encrypted Communications

Australia • Belgium • Brazil • Canada • European Union
France • Germany • Israel • Japan • South Africa
Sweden • Taiwan • United Kingdom

May 2016

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Comparative Summary

Luis Acosta
Chief, Foreign, Comparative, and International Law Division II

This report describes the law of twelve nations and the European Union on whether the government, pursuant to a court order or other government process, can require companies to decrypt encrypted communications or provide the government with the means to do so. Some of the surveys provide additional information on related surveillance issues like the law on monitoring and intercepting communications.

The report finds that while there is a range of approaches among the surveyed countries, a majority make provision for specified intelligence or law enforcement agencies to obtain access to encrypted communications or the means of decryption under certain circumstances.

In France, national intelligence and security services may obtain authorization from the Prime Minister or his delegate, upon the written request of a senior minister, to intercept and read private communications for specifically enumerated purposes, and may request from providers of cryptology services the means to decipher encrypted communications. French law also provides for investigative judges to order the interception, recording, and transcription of private telecommunications in criminal investigations, and law enforcement authorities may obtain authorization to ask any qualified person to perform the technical operations that would allow access to this information.

In Belgium, the intelligence services may obtain authorization from a special independent commission to secretly access, listen to, or recording private communications, and can serve a written demand to the network operator or the service provider for technical assistance; such providers are required to have the technical ability to provide decrypted copies of communications when requested by Belgian intelligence. Also, investigative judges may authorize communication interception operations under certain legally-defined circumstances, and may order anyone who has a particular knowledge of a relevant encryption service to help access communications in a readable format.

Under current law in the UK, specified law enforcement and intelligence officials under certain circumstances may serve written notice on persons or bodies requiring them to disclose encrypted information in intelligible form. A draft revision of the relevant UK law is being considered.

In Australia, under some circumstances, the police may obtain an order from a court requiring certain persons to provide information or assistance to enable the police to unlock a computer or digital storage device that is subject to a warrant, or to provide information on the decryption of data on such a device in order to make it intelligible to the police.

In Japan, law enforcement officials may request the courts to order the decryption of encrypted information during criminal investigations, and courts may also order the decryption of encrypted information during trials.

In South Africa, a law enforcement officer may apply for a "decryption direction" from a court requiring a decryption key holder to disclose the key or provide decryption assistance.

In some countries, such as Canada and Taiwan, the relevant law does not explicitly address decryption, but does provide a framework under which telecommunications companies are required to assist with government surveillance of communications, and the framework would appear to permit orders requiring them to assist with decryption, at least subject to reasonable technological feasibility.

Similarly, in Brazil, while the relevant law does not make direct reference to decryption pursuant to a warrant, the federal telecommunications agency has provided in regulations that communications providers must make available to certain authorities the technological resources and data relating to the suspension of telecommunications confidentiality. Two known cases apparently involving judicial enforcement of decryption orders (albeit subject to judicial secrecy) suggest that companies may be considered obligated to provide decryption assistance to the government.

In Israel, the law does not specifically address orders for decryption. However, encryption activities are regulated and licensed by the Ministry of Defense, and officials of that Ministry may enter any place where an encryption-related activity is being conducted and request information at any time regarding the subject of an encryption license.

In Germany, certain intelligence and law enforcement agencies have authority to access and intercept communications. While they may use whatever technologies they have at their disposal to unlock encrypted communications, and they may demand telecommunications providers to remove encryption put in place by such providers, there is no legal basis in Germany to compel end users to turn over encryption keys they have used, on the principle that suspects cannot be compelled to cooperate in investigations that would incriminate themselves.

Under current Swedish law, it appears unlikely that a Swedish court would force an ISP, encryption firm, or other entity to decrypt data, because warrants must satisfy a proportionality test, and an order of decryption would not likely be considered proportional. There have been some calls and proposals for legislative changes.

At the European Union level, there is no EU legislation that requires tech companies to disclose the keys to encrypted materials to law enforcement authorities, or to decrypt communications upon the request of a government. Relevant agencies on cybersecurity, organized crime, and terrorism have not reached a uniform position on this issue.

Australia

Kelly Buchanan
Chief, Foreign, Comparative, and
International Law Division I

SUMMARY Various federal statutes in Australia relate to the ability of government agencies to intercept and access communications and other data for law enforcement and national security purposes. In terms of requirements for persons to assist in decrypting information, under the Crimes Act 1914 (Cth) federal and state police may obtain an order for certain persons to provide "any information and assistance" necessary to enable an officer to access data in a computer or digital storage device that is subject to a warrant and to make that data intelligible. Such orders can only be made with respect to a "person under investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator."

The Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), which provides a warrant system for intercepting communications and accessing stored communications, does not include a specific requirement for service providers to assist in making encrypted communications or other data intelligible. Under that Act and the Telecommunications Act 1997 (Cth), carriers and carriage service providers are required to provide assistance to officials, including by giving effect to stored communications warrants, providing interception services, and providing "relevant information" about communications.

There have been multiple reviews of the TIA Act and related legislation over the years. Following a report by the Australian Law Reform Commission on privacy issues and recommendations by a parliamentary committee on reforming national security legislation, another parliamentary committee examined the need for a comprehensive revision of the TIA Act. The government has indicated that it will consider possible changes to the Act, including consulting with the telecommunications industry and relevant agencies on the development of appropriate legislative provisions to address issues related to accessing encrypted information.

I. Introduction

There are several federal statutes relevant to the ability of Australian law enforcement and intelligence agencies to access and intercept electronic communications and other data:[1]

- Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act):[2] This Act provides for various federal and state agencies to obtain interception warrants and stored communications warrants for law enforcement and national security purposes.

[1] *See generally Telecommunications Interception and Surveillance: Overview of Legislation*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Overviewoflegislation.aspx (last visited Apr. 8, 2016), *archived at* https://perma.cc/CRE2-EZZF.

- Surveillance Devices Act 2004 (Cth):[3] This Act provides for eligible federal agencies to obtain warrants to install and use surveillance devices, including data surveillance devices.
- Telecommunications Act 1997 (Cth):[4] This Act requires that carriers and carriage service providers provide assistance to relevant agencies for the purposes of law enforcement and safeguarding national security.
- Australian Security Intelligence Organisation Act 1979 (Cth) (ASIO Act): This Act provides the Australian Security Intelligence Organisation (ASIO) with various powers, including the ability to obtain computer access warrants and surveillance device warrants.
- Crimes Act 1914 (Cth):[5] This Act includes various search and information-gathering powers of law enforcement officers, including the ability to access data held in a computer or other data storage device.

The powers and procedures in these laws related to electronic communications and data have been the subject of several reviews, with the discussion encompassing the impact of new technologies (including encryption technologies) and the need to balance privacy considerations with national security and law enforcement interests.[6] The most recent change that has resulted from these reviews was the amendment of the TIA Act in 2015 to put in place a data retention system that requires service providers to retain certain data related to communications (i.e., "metadata" rather than content) for a set period of time.[7]

II. Access to Information Held in a Computer

A. Order to Assist Law Enforcement Officer to Access Data

Section 3LA of the Crimes Act 1914 enables a member of the Australian Federal Police (AFP) or a state police force[8] to apply to a magistrate "for an order requiring a specified person to provide any information or assistance that is reasonable and necessary" to allow the member to

---

[2] Telecommunications (Interception and Access) Act 1979 (Cth) (TIA Act), https://www.legislation.gov.au/Details/C2016C00102, *archived at* https://perma.cc/CD3H-SGW7.

[3] Surveillance Devices Act 2004 (Cth), https://www.legislation.gov.au/Details/C2016C00103, *archived at* https://perma.cc/AA2T-8AM3.

[4] Telecommunications Act 1997 (Cth), https://www.legislation.gov.au/Details/C2016C00107, *archived at* https://perma.cc/4RA5-7YFQ.

[5] Crimes Act 1914 (Cth), https://www.legislation.gov.au/Details/C2016C00121, *archived at* https://perma.cc/Q7XY-ZKJ6.

[6] *See infra*, Part IV.

[7] Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (Cth), https://www.legislation.gov.au/Details/C2015A00039, *archived at* https://perma.cc/TP4K-HQGP. *See generally Data Retention*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/DataRetention/ Pages/Default.aspx (last visited Apr. 8, 2016), *archived at* https://perma.cc/6UFK-W2NF.

[8] *See* definition of "constable" in section 3 of the Crimes Act 1914 (Cth).

- "access data held in, or accessible from, a computer or data storage device"[9] that is on the premises subject to a warrant or has been moved elsewhere for examination or processing, or that has otherwise been seized in accordance with the Act;
- "copy data held in, or accessible from, a computer, or data storage device, . . . to another data storage device"; and/or
- "convert into documentary form or another form intelligible to a constable" data held in, accessible from, or copied from a computer or device.[10]

Therefore, it appears that a person may be ordered to provide information related to (1) unlocking a computer or digital storage device that is subject to a warrant, and (2) the decryption of data on such a computer or digital storage device in order to make it accessible and intelligible to the police.

The magistrate may grant the order if he or she is satisfied that there are "reasonable grounds for suspecting that evidential material is held in, or accessible from, the computer or data storage device."[11] In addition, the magistrate must be satisfied that the person specified in the application is either "reasonably suspected of having committed the offense stated in the relevant warrant," or is the owner or lessee of the computer or device, an employee of or engaged under a contract of service by the owner or lessee, a person who uses or has used the computer or device, or a person who is or was a system administrator for the relevant system that includes the computer or device.[12] The specified person must also have relevant knowledge of the computer or device or the relevant computer network, or of the "measures applied to protect data held in, or accessible from, the computer or device."[13] Thus, if a technology company, or employee of such a company, does not fall within these categories it cannot be subject to an order requiring it to provide access to the data on a device.

If a person does not comply with an order made under section 3LA, he or she may be charged with an offense that is subject to a penalty of two years' imprisonment.[14]

B. ASIO Powers

There is no similar provision in the ASIO Act requiring a person to provide assistance to ASIO in order for it to access or read data on a computer. A computer access warrant issued by the relevant government Minister under the ASIO Act may authorize the agency to do certain things, including using the target computer, a telecommunications facility, any other electronic equipment, a data storage device, another computer, or a communication in transit for the

[9] "Data storage device" is defined in section 3 of the Crimes Act 1914 (Cth) as "a thing containing, or designed to contain, data for use by a computer."

[10] Crimes Act 1914 (Cth), s 3LA(1).

[11] *Id.* s 3LA(2)(a).

[12] *Id.* s 3LA(2)(b).

[13] *Id.* s 3LA(2)(c).

[14] *Id.* s 3LA(5).

purpose of obtaining access to the relevant data held in the target computer. If necessary, this can include "adding, copying, deleting or altering other data in the target computer" or in the other computer, or the communication in transit.[15]

III. Interception of Communications and Access to Stored Communications

A. Warrant System

1. Interception Warrants

Under the TIA Act, the Director-General of Security may request an interception warrant, issued by the Attorney-General, with respect to a telecommunications service,[16] where the interception of communications made to or from that service will assist ASIO in carrying out its function of obtaining intelligence relating to national security.[17] "Named person warrants" can also be issued that allow the interception of communications made to or from any telecommunications service that the particular person uses or those made using a device identified in the warrant.[18]

In the course of investigating serious offenses, federal law-enforcement agencies and anticorruption agencies, as well as designated state police forces and other agencies, can apply for similar warrants with respect to a telecommunications service or person.[19] These are issued by an eligible judge or nominated Administrative Appeals Tribunal (AAT) member.[20]

2. Stored Communications Warrants

The TIA Act "establishes a system of preserving certain stored communications that are held by a carrier" in order to prevent them from being destroyed before they can be accessed under certain warrants.[21] It also authorizes the issuance of stored communications warrants to criminal

[15] ASIO Act s 25A(4)(a) & (ab).

[16] "Telecommunications service" is defined in section 5 of the TIA Act as "a service for carrying communications by means of guided or unguided electromagnetic energy or both, being a service the use of which enables communications to be carried over a telecommunications system operated by a carrier but not being a service for carrying communications solely by means of radiocommunication."

[17] TIA Act s 9(1). Warrants issued to ASIO under chapter 2 of the TIA are also referred to as "Part 2-2 warrants."

[18] *Id.* s 9A.

[19] *Id.* ss 46 & 46A. "Serious offence" is defined in section 5D of the TIA Act.

[20] *Id.* s 39, 46 & 46A. Such warrants are also referred to as "Part 2-5 warrants."

[21] *Id.* s 107G. "Carrier" and "carriage service provider" (included in the definition of "carrier" in section 5 of the TIA Act) are defined in the Telecommunications Act 1997 (Cth). A "carriage service provider" is a person who supplies, or proposes to supply, a listed carriage service using "a network owned by one or more carriers" or "a network unit in relation to which a nominated carrier declaration is in force." Telecommunications Act 1997 (Cth) s 87. "Carriage service" means "a service for carrying communications by means of guided and/or unguided electromagnetic energy." *Id.* s 7. A "carrier" refers to a holder of a carrier license issued under the Act. The Act requires that the owner of a network unit used to supply carriage services to the public must hold a carrier license, unless a declaration or exemption applies. *See id.* s 41.

law enforcement agencies in the course of investigating a "serious contravention."[22] Such warrants can be issued by a judge, magistrate, or certain Administrative Appeals Tribunal members.[23] They authorize access to a stored communication that was made by the person named in the warrant, or by another person with the person named in the warrant being the intended recipient.[24]

Interception warrants issued to ASIO, outlined above, are taken to authorize access to a stored communication where "the warrant would have authorised interception of the communication if it were still passing over a telecommunications system."[25]

B. Requirement for Carriers and Service Providers to Assist Agencies

Carriers and carriage service providers[26] (including Internet service providers) are required to provide certain assistance to ASIO and law enforcement agencies under the Telecommunications Act 1997 (Cth).[27] However, there is no specific requirement for carriers and service providers to assist agencies by making intercepted or stored encrypted communications intelligible.

Part 14 of the TIA Act, titled "National Interest Matters," establishes obligations for such entities to

- "do their best to prevent telecommunications networks and facilities from being used to commit offenses"; and
- "give authorities such help as is reasonably necessary" for the purposes of "enforcing the criminal law and laws imposing pecuniary penalties," "protecting the public revenue," and "safeguarding national security."[28]

Such help includes giving assistance by way of

> (a) the provision of interception services, including services in executing an interception warrant under the Telecommunications (Interception and Access) Act 1979; or

---

[22] TIA Act s 116. "Criminal law enforcement agencies" for the purposes of this part are listed in section 110A of the TIA Act. "Serious contravention" is defined in section 5E of the TIA Act.

[23] *Id.* ss 110, 116 & 6DB.

[24] *Id.* s 117.

[25] *Id.* s 109(a).

[26] *See* definition of "carriers" and "carriage service providers," *supra* note 21.

[27] *See generally Law Enforcement (Telecommunications)*, AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY (ACMA), http://www.acma.gov.au/theACMA/law-enforcement-telecommunications (last updated Feb. 23, 2016), *archived at* https://perma.cc/TTR9-YZY4; *Licensing – I Want to be an ISP: Carriage Service Provider Rules: Law Enforcement*, ACMA, http://www.acma.gov.au/Industry/Internet/Licensing--I-want-to-be-an-ISP/Carriage-service-provider-rules/isps-and-law-enforcement-isp-licensing-i-acma (last updated Mar. 7, 2014), *archived at* https://perma.cc/GC43-7FLA.

[28] Telecommunications Act 1997 (Cth) s 311. *See also id.* s 313(1) & (3).

> (b) giving effect to a stored communications warrant under that Act; or
>
> (c) providing relevant information about:
>
> (i) any communication that is lawfully intercepted under such an interception warrant; or
>
> (ii) any communication that is lawfully accessed under such a stored communications warrant; or
>
> (ca) complying with a domestic preservation notice or a foreign preservation notice that is in force under Part 3-1A of that Act; or
>
> (d) giving effect to authorisations under Division 3 or 4 of Part 4-1 of that Act [related to accessing telecommunications data]; or
>
> (e) disclosing information or a document in accordance with section 280 of this Act [related to disclosures of certain information in compliance with a warrant or as required or authorized by or under law].[29]

Additional obligations are contained in Chapter 5 of the TIA Act. These primarily relate to data retention requirements[30] and interception capability.[31] This includes a requirement to comply with any determinations regarding the interception capabilities that a carrier must develop, install, and maintain.[32] Carriers and nominated carriage service providers must also develop interception capability plans and submit these annually to the Communications Access Coordinator in the Attorney-General's Department for consideration.[33] Approval of such plans may be granted following consultation with interception agencies.[34]

IV. Reviews of the Relevant Laws

The following three reviews or inquiries, conducted in the past ten years, include discussions of the impact of new technologies and privacy considerations in relation to intercepting or accessing electronic communications:

- Australian Law Reform Commission (ALRC) inquiry into Australian privacy law and practice (completed 2008)[35]

---

[29] *Id.* s 313(7).

[30] TIA Act pt 5-1A.

[31] *Id.* pts 5-3 to 5-6.

[32] *Id.* ss 189 & 190.

[33] *Id.* ss 195(2) & 198(1); *Interception Capability Plans*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/InterceptionCapabilityPlans.aspx (last visited Apr. 11, 2016), *archived at* https://perma.cc/WA3B-YJNG. The Communication Access Coordinator "liaises between law enforcement agencies and the telecommunications industry." *Id.*

[34] TIA Act s 198(2).

[35] *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, AUSTRALIAN LAW REFORM COMMISSION (ALRC), http://www.alrc.gov.au/publications/report-108 (last visited Apr. 11, 2016), *archived at* https://perma.cc/497T-FNQM.

- Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into potential reforms of national security legislation (completed May 2013)[36]
- Senate Legal and Constitutional Affairs References Committee inquiry regarding the comprehensive revision of the TIA Act (completed March 2015).[37]

Prior reviews relevant to the TIA Act were also carried out in 1994, 1999, 2000, 2003, and 2005.[38] Various amendments have been enacted implementing some of the recommendations that resulted from these reviews.

A. ALRC Report

Chapter 73 of the ALRC report examined the TIA Act, including its interaction with the Privacy Act 1988 (Cth), and made several recommendations for particular legislative and procedural changes.[39] It also recommended that the government "should initiate a review to consider whether the Telecommunications Act 1997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies."[40]

B. PJCIS Inquiry

Chapter 2 of the 2013 PJCIS report on its inquiry into a package of potential reforms to national security legislation relates to telecommunications interception.[41] The committee recommended various changes to the TIA Act, including in relation to privacy protections.[42] It also recommended that the Attorney-General's Department conduct a review of the legislation and that the TIA Act should be "substantially revised," with a new interception system designed that is underpinned by clear protection for the privacy of communications, provisions that are

---

[36] *Inquiry into Potential Reforms of National Security Legislation*, PARLIAMENT OF AUSTRALIA, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm (last visited Apr. 11, 2016), *archived at* https://perma.cc/XY8C-MC52.

[37] *Comprehensive Revision of Telecommunications (Interception and Access) Act 1979*, PARLIAMENT OF AUSTRALIA, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act (last visited Apr. 11, 2016), *archived at* https://perma.cc/A39M-S6RV.

[38] *Telecommunications Interception Reviews*, ATTORNEY-GENERAL'S DEPARTMENT, https://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/TIReviews.aspx (last visited Apr. 11, 2016), *archived at* https://perma.cc/7GGD-T6GV; *see also* ALRC, 3 FOR YOUR INFORMATION: AUSTRALIAN PRIVACY LAW AND PRACTICE 2530–32 (ALRC Report 108, 2008) (ALRC Report), http://www.alrc.gov.au/sites/default/files/pdfs/publications/108_vol3.pdf, *archived at* https://perma.cc/2W6C-LHLV.

[39] ALRC Report at 2478.

[40] *Id.* at 2395.

[41] PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY (PJCIS), REPORT OF THE INQUIRY INTO POTENTIAL REFORMS OF AUSTRALIA'S NATIONAL SECURITY LEGISLATION (May 2013) (PJCIS Report), http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report/full.pdf, *archived at* https://perma.cc/XXX8-YJAQ.

[42] *See id.* at xxiii–xxv (recommendations 1–4, 6 & 8).

technology neutral, maintenance of investigative capabilities, clearly articulated and enforceable industry obligations, and robust oversight and accountability.[43]

As part of the inquiry, the Attorney-General's Department proposed that an offense should be introduced for failure by telecommunications providers to assist in the decryption of communications. The Department stated that

> Section 3LA of the Crimes Act 1914 (the Crimes Act) sets out provisions concerning decryption regarding information obtained under search warrants; however this does not extend to communications intercepted pursuant to a warrant under the TIA Act.
>
> In summary, section 3LA of the Crimes Act allows a police officer to apply to a magistrate for a warrant to require a person to provide in accessible form (i.e. in decrypted form) data held on a computer or data storage device, where the computer or data storage device had been seized under a warrant. A warrant may be applied to the person under investigation, an owner of the device, an employee of the owner, a relevant contractor, a person who has used the device, or a systems administrator. There is a penalty of up to two years imprisonment for failing to comply with an order.
>
> A consistent approach to that contained in the Crimes Act would ensure that information lawfully accessed for national security or law enforcement purposes under the TIA Act was intelligible.[44]

The PJCIS report noted support for the proposal from certain law enforcement agencies and also reflected the objections of different groups.[45] It considered that there was some lack of clarity and specificity in what was being proposed[46] and recommended that, should the government decide to develop an offense of failing to provide decryption assistance, it should do so in consultation with the telecommunications industry and relevant government agencies.[47]

C. TIA Act Revision Inquiry

The Senate committee's inquiry regarding the comprehensive revision of the TIA Act was carried out over a fifteen-month period, with the report being issued in March 2015.[48] The

[43] *Id.* at xxviii (recommendation 18).

[44] *Id.* at 59–60; Attorney-General's Department, Submission to PJCIS, Inquiry into Potential Reforms of National Security Legislation (submission 218), at 7, http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/subs/sub%20218.pdf, *archived at* https://perma.cc/NXE8-KC62.

[45] PJCIS Report, *supra* note 41, at 60–63.

[46] *Id.* at 63 & 64.

[47] *Id.* at 64 (recommendation 16).

[48] SENATE LEGAL AND CONSTITUTIONAL AFFAIRS REFERENCES COMMITTEE, COMPREHENSIVE REVISION OF THE TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979, at 1 (Mar. 2015), http://www.aph.gov.au/~/media/Committees/Senate/committee/legcon_ctte/tia_act/report/report.pdf?la=en, *archived at* https://perma.cc/KN7S-NLC9.

committee was asked by the Senate to have regard to both the ALRC report and the PJCIS report.[49]

The committee noted that "all law enforcement and national security agencies agreed that the current TIA Act was at risk of becoming ineffective without reform."[50] Of particular concern was that the TIA Act should be modernized in order to keep pace with changes in technology, including the view, expressed by the Australian Crime Commission, that the TIA Act "must be capable of overcoming technical advances which are deliberately used to prevent law enforcement from lawfully intercepting and accessing communications."[51]

The chair of the committee recommended that the TIA Act be "substantially redrafted" to enact a single attribute-based warrant system, and that a Public Interest Monitor should be established to have oversight of the warrant system.[52] Other members agreed with the recommendation for a substantial revision of the Act and the establishment of a single warrant, although some did not think a Public Interest Monitor was necessary.[53]

D. Government Response

In July 2015 the government released its response to recommendations related to the TIA Act that were included in the PJCIS report on national security legislation.[54] It indicated support for nearly all of the recommendations, including the recommendation related to the potential establishment of an offense for failure to assist in decrypting communications. The response stated that

> [t]he Australian government supports strong encryption, which underpins modern, secure communications technologies. These technologies are fundamental to a digital economy, and provide an unparalleled opportunity for exercise of the fundamental freedoms of expression, peaceful assembly and association.
>
> However, the use of encrypted communications for serious criminal purposes and purposes prejudicial to security represents an increasingly significant barrier to the ability of governments to bring serious offenders to justice.

---

[49] *Id.* at 3.

[50] *Id.* at 10.

[51] *Id.*

[52] *Id.* at 41.

[53] *Id.* at 82–87.

[54] AUSTRALIAN GOVERNMENT RESPONSE TO CHAPTERS 2 AND 3 OF THE PARLIAMENTARY JOINT COMMITTEE ON INTELLIGENCE AND SECURITY'S REPORT OF THE INQUIRY INTO POTENTIAL REFORMS OF AUSTRALIA'S NATIONAL SECURITY LEGISLATION (July 1, 2015) (Government Response), http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/govresponse.pdf, *archived at* https://perma.cc/S9XA-CEX4; *PJCIS Committee Activities (Inquiries and Reports), 43rd Parliament (September 2010–August 2013)*, PARLIAMENT OF AUSTRALIA, http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/reports.htm (last visited Apr. 12, 2016), *archived at* https://perma.cc/69ZZ-SMWT.

> Accordingly, the Government will explore, in consultation with agencies and the telecommunications industry, the development of appropriate legislative provisions, including safeguards, oversight and accountability measures.[55]

More broadly, the government stated that it intends to finalize its detailed response to a number of the recommendations related to the TIA Act following the delivery of a report concerning whether the agencies that may access the content of communications should be standardized, which is to be completed by April 13, 2017.[56]

[55] Government Response, *supra* note 54, at 11–12.

[56] *See id*. at 2–3, 4 & 8.

Belgium

Nicolas Boring
Foreign Law Specialist

I. Decryption at the Request of Intelligence and Security Services

The main legislative framework for intelligence-gathering in Belgium is the Law of November 30, 1998, Organizing the Intelligence and Security Services.[1] Article 18/17 of this Law provides that intelligence services may "listen to, gain knowledge of, and record communications" in order to fulfill their missions.[2] An intelligence service must obtain prior authorization from a special independent commission before secretly accessing, listening to, or recording private communications.[3] When an intelligence service has obtained the required authorization to conduct this kind of surveillance on an electronic communications network, it can serve a written demand to the network operator or the service provider, upon which the network operator or service provider is required to give technical assistance to the intelligence service.[4] Any person who refuses to give technical assistance pursuant to a properly authorized demand is punishable by a fine of €26 to €10,000 (about US$29 to US$11,270).[5] On the other hand, companies and individuals who cooperate in giving technical assistance are paid for their services on the basis of government-established rates.[6]

The principal statute governing electronic communications in Belgium requires that network operators as well as end users be capable of allowing the authorities to "listen to, gain knowledge of, and record" communications.[7] A Royal Order from 2010 includes electronic communications service providers alongside network operators as being required to have the technical ability to provide clear and readable (decoded, decompressed, and decrypted) copies of communications requested by Belgian intelligence services.[8] It appears, in other words, that

[1] Loi du 30 novembre 1998 organique des services de renseignement et de sécurité [Organic Law of November 30, 1998, Organizing the Intelligence and Security Services], http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=1998113032, *archived at* https://perma.cc/58QH-E735.

[2] *Id.* art. 18/17.

[3] *Id.* art. 43/1.

[4] *Id.* art. 18/17.

[5] *Id.*

[6] *Id.* art. 18/18.

[7] Loi du 13 juin 2005 relative aux communications électroniques [Law of June 13, 2005, Regarding Electronic Communications] art. 127, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2005061332&table_name=loi, *archived at* https://perma.cc/92QM-7E5S.

[8] Arrêté royal du 12 octobre 2010 déterminant les modalités de l'obligation de collaboration légale en cas de demandes concernant les communications électroniques par les services de renseignement et de sécurité [Royal Order of October 12, 2010, Establishing the Conditions of the Obligation of Lawful Collaboration in Cases of Demands by Intelligence and Security Services Regarding Electronic Communications] art. 8, http://www.ejustice.just.fgov.be/cgi_loi/loi_a.pl, *archived at* https://perma.cc/5ZG7-VUL9.

service providers and network operators may not use or make available any form of encryption that they would be unable to decrypt themselves.

II. Decryption at the Request of Judicial and Law Enforcement Agencies

The Belgian Code of Criminal Investigations allows investigative judges (*juges d'instruction*) to "listen to, gain knowledge of, and record" private communications when warranted by certain legally-defined circumstances.[9] An investigative judge must authorize the communication interception operation by a reasoned ordinance, which must be sent to the Royal Prosecutor.[10] An investigative judge may order anyone who has a particular knowledge of the communication service or, if the communication is protected or encrypted, of the protection and encryption service, to help access the communication in a readable format.[11] Refusal to cooperate is punishable by between six months and one year of incarceration, and a fine.[12] A 2003 Royal Order governing the cooperation of electronic communications providers with judicial authorities was amended in 2011 to require that electronic communications service providers and network operators have the technical ability to provide clear and readable copies of communications requested by Belgian judicial authorities.[13]

[9] CODE D'INSTRUCTION CRIMINELLE [CODE OF CRIMINAL INVESTIGATIONS] art. 90ter, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language= fr&la=F&table_name=loi&cn=1808111730, *archived at* https://perma.cc/N2GE-PMAE.

[10] *Id.* art. 90quater.

[11] *Id.*

[12] *Id.*

[13] Arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques [Royal Order of January 9, 2003, Establishing the Conditions of the Obligation of Lawful Collaboration in Cases of Judicial Demands Regarding Electronic Communications] art. 6, http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?sql=%28text%20contains%20%28%27%27%29%29&language=fr&rech=1&tri=dd%20AS%20RANK&value=&table_name=loi&F=&cn=2003010942&caller=image_a1&fromtab=loi&la=F, *archived at* https://perma.cc/VAA8-ZVBF.

Brazil

Eduardo Soares
Senior Foreign Law Specialist

SUMMARY In Brazil, a constitutional principle provides for the protection of communications. A federal law regulates the breach of such protection by a court order, while a federal agency determines whether the providers of telecommunications and multimedia services must make available to the authorities the technological resources necessary to suspend telecommunications confidentiality in accordance with the law.

The Code of Civil Procedure does not provide any exemption from the duty to cooperate with the Judiciary, the Penal Code imposes jail time on those who disobey a court order, and a federal law punishes with imprisonment anyone who obstructs the investigation of a criminal offense involving a criminal organization.

I. Access to Communications

This report discusses the Brazilian legal framework for privacy of communications. This framework includes the constitutional principle that protects the secrecy of communications in the country and the law that regulates this principle and grants access to an individual's communications, provided that such access has been authorized by a court order. The report also discusses the federal agency that regulates telecommunications in the country and that agency's regulations regarding the suspension of telecommunications confidentiality as a result of a court order.

Provisions of the Brazilian Code of Civil Procedure, the Penal Code, and a federal law that punish disobedience to court orders, is also addressed. The report also offers two examples of application of the abovementioned laws in connection with court orders directing two different companies to grant access to the accounts of individuals who were under criminal investigation.

A. Constitutional Principle

According to article 5, section XII, of the Brazilian Constitution, the secrecy of correspondence and of telegraphic, data, and telephonic communications is inviolable. The only exception is for legally defined, court-ordered interceptions of telephonic communications in criminal investigations and fact-finding phases of criminal prosecutions (*instrução processual penal*).[1]

B. Law No. 9,296 of July 24, 1996

On July 24, 1996, Law No. 9,296 was enacted to regulate the final part of section XII of article 5 of the Constitution regarding lawful interceptions of communications. The Law states that the

[1] CONSTITUIÇÃO FEDERAL [C.F.] art. 5(XII), http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituicao.htm, *archived at* https://perma.cc/FH8R-Z4Y6.

interception of telephone communications of any kind, as proof in a criminal investigation or in the fact-finding phase of a criminal prosecution, requires a court order issued by the competent judge in the main legal action, under judicial secrecy.[2] It also says that this provision applies to the interception of the flow of communications on data systems (*sistemas de informática e telemática*).[3]

C. Law No. 9,472 of July 16, 1997

Law No. 9,472 of July 16, 1997, provides for the organization of telecommunications services in the country. The Law created the National Telecommunications Agency (Agência Nacional de Telecomunicações, ANATEL), a federal agency subordinate to the Ministry of Communications and charged with the duty of regulating telecommunications in the country.[4]

"Telecommunications" are defined by Law No. 9,472 as the "transmission, emission, or reception, by wire, radio, optical, or other electromagnetic process, of symbols, characters, signals, writing, images, sounds, or information of any kind."[5]

Pursuant to article 3 of Law No. 9,472, the user of telecommunications services has the right to the inviolability and secrecy of his or her communications, except in the cases and conditions established in the Constitution and the law.[6]

1. Resolution ANATEL No. 73 of November 25, 1998

Fulfilling its duties as established under Law No. 9,472, on November 25, 1998, ANATEL issued Resolution No. 73, which approved the regulation of telecommunications services (*Regulamento dos Serviços de Telecomunicações*).[7] The Resolution defines "telecommunications services" as the set of activities that enables the "transmission, emission or reception, by wire, radio, optical or other electromagnetic process, of symbols, characters, signals, writing, images, sounds or information of any kind."[8]

The provider of telecommunications services is obligated to safeguard the privacy inherent in telecommunications services and the confidentiality of data and information, using all necessary means and technology to ensure this right of users. The provider must make available the technological resources necessary to suspend telecommunications confidentiality when so ordered by

---

[2] Lei No. 9.296, de 24 de Julho de 1996, art. 1, http://www.planalto.gov.br/ccivil_03/leis/L9296.htm, *archived at* https://perma.cc/RB7M-WLTA.

[3] *Id.* art. 1(sole para.).

[4] Lei No. 9.472, de 16 de Julho de 1997, art. 8, http://www.planalto.gov.br/ccivil_03/leis/L9472.htm, *archived at* https://perma.cc/C5QX-AJBP.

[5] *Id.* art. 60(§1).

[6] *Id.* art. 3(V).

[7] Resolução ANATEL No. 73, de 25 de Novembro de 1998, art. 1, http://www.anatel.gov.br/legislacao/resolucoes/13-1998/34-resolucao-73, *archived at* https://perma.cc/B8B6-FZN9.

[8] Resolução ANATEL No. 73, anexo, art. 2.

a judicial authority and "maintain permanent control" of all cases, after the execution of such orders, ensuring that they are strictly fulfilled within the authorized limits.[9]

2. Resolution ANATEL No. 614 of May 28, 2013

To regulate multimedia communications services (*Serviço de Comunicação Multimídia*), on May 28, 2013, ANATEL issued Resolution No. 614.[10] The regulation defines "multimedia information" as "audio signals, video, data, voice and other sounds, images, texts and other information of any kind."[11]

The provider of multimedia communications services must ensure the secrecy inherent in telecommunications services and the confidentiality of data, including connection records and subscriber information, using all means and technology available.[12] The provider must make available to the authorities authorized to request such information data relating to the suspension of telecommunications confidentiality.[13]

D. Code of Civil Procedure

The new Brazilian Code of Civil Procedure determines that no one is exempt from the duty to cooperate with the judiciary for the discovery of truth.[14]

E. Penal Code

The Penal Code provides that disobeying a legal order is punishable by imprisonment for fifteen days to six months and a fine.[15]

F. Law No. 12,850 of August 2, 2013

Law No. 12,850 of August 2, 2013, defines the term "criminal organization" and provides for criminal investigations, the means of obtaining evidence, criminal offenses related to criminal organizations, and criminal prosecution.[16] At any stage of a criminal prosecution, authorities are allowed to access telephone records and data links, records of public and private databases, and

[9] *Id.* art. 26.

[10] Resolução ANATEL No. 614, de 28 de Maio de 2013, art. 1, http://www.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614#art3res, *archived at* https://perma.cc/2HBD-C526.

[11] Resolução ANATEL No. 614, anexo, art. 4(VII).

[12] *Id.* art. 52.

[13] *Id.* art. 52(sole para.).

[14] CÓDIGO DE PROCESSO CIVIL, Lei No. 13.105, de 16 de Março de 2015, art. 378, http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm#art378, *archived at* https://perma.cc/WB5A-79XA.

[15] CÓDIGO PENAL, Decreto-Lei No. 2.848, de 7 de Dezembro de 1940, art. 330, http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm, *archived at* https://perma.cc/QL9V-UZND.

[16] Lei No. 12.850, de 2 de Agosto de 2013, art. 1, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm, *archived at* https://perma.cc/CY4B-26RY.

electoral or commercial information, as well as to intercept telephone and data communications, without prejudice to other means already provided by law, according to the specific legislation.[17]

A person who personally or through an intermediary promotes, creates, finances, or participates in a criminal organization is punishable by imprisonment for three to eight years and a fine, and is also subject to the corresponding penalties for other criminal offenses committed.[18] The same penalties apply to those who prevent or in any way obstruct the investigation of a criminal offense involving a criminal organization.[19]

G. Law No. 12,965 of April 23, 2014

In 2014, Brazil issued Law No. 12,965, which establishes principles, guarantees, rights, and duties for the use of the Internet in the country and guidelines for state action.[20]

Article 7 guarantees to Internet users in the country the inviolability and confidentiality of the flow of their Internet communications and their stored private communications, except as otherwise dictated by court order.[21]

Article 10 determines that the content of private communications can be made available only by court order, in the cases and manner provided by law, subject to the provisions of sections II and III of article 7 of Law No. 12,965.[22]

According to article 11, the right to privacy, the protection of personal data, and the confidentiality of private communications and records must be respected in any activity involving the collection, storage, custody, and treatment of records, personal data, and communications through Internet service providers and Internet applications when at least one of these acts occur in the national territory.[23] This provision applies to the data collected in the national territory and the contents of communications, provided that at least one of the terminals is located in Brazil.[24] The provision also applies even if the activities are carried out by a legal entity based abroad, provided that the services are offered to the Brazilian public, or at least one member of the same group is established in Brazil.[25]

---

[17] *Id.* art. 3(IV)–(V).

[18] *Id.* art. 2.

[19] *Id.* art. 2(§1).

[20] Lei No. 12.965, de 23 de Abril de 2014, art. 1, http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, *archived at* https://perma.cc/CNG4-6AQZ.

[21] *Id.* art. 7(II)–(III).

[22] *Id.* art. 10(§2).

[23] *Id.* art. 11.

[24] *Id.* art. 11(§1).

[25] *Id.* art. 11(§2).

The providers of Internet services and applications must provide, in accordance with the regulation, information allowing verification of compliance with Brazilian legislation on the collection, custody, storage, or processing of data, as well as information demonstrating the protection of privacy and confidentiality of communications.[26]

Pursuant to article 12, the following penalties are applied individually or cumulatively to violations of the rules established in articles 10 and 11 of Law No. 12,965, without prejudice to other civil, criminal, and administrative sanctions:

> I – a warning, with time indication for corrective action;
>
> II – a fine of up to 10% (ten percent) of the economic group revenue [*faturamento*] in Brazil in its previous financial year, excluding taxes, considering the economic condition of the offender and the principle of proportionality between the seriousness of the offense and the intensity of the sanction;
>
> III – temporary suspension of activities involving the acts provided for in article 11; or
>
> IV – a ban on activities involving the acts provided for in article 11.[27]

In the case of a foreign company, the branch, office, or establishment in the country is jointly liable for the payment of fines.[28]

II. Recent Court Cases

Two court cases illustrate the practical application of the legal framework involving the secrecy of communications and its breach by court order. The first occurred in December 2015 and concerned the suspension for forty-eight hours of the WhatsApp application in the country for failure to obey a legal order as determined by article 12 of Law No. 12,965.[29]

The second case involved the use of Law No. 12,850 to arrest the Latin American vice-president of Facebook in Brazil for the apparent obstruction of a criminal investigation because the company refused to provide information requested by a judge related to a criminal investigation involving a criminal organization and drug trafficking.[30]

---

[26] *Id.* art. 11(§3).

[27] *Id.* art. 12.

[28] *Id.* art. 12 (sole para.).

[29] Marcelo Crespo, *Investigação Criminal, Obstrução da Justiça e Bloqueio do WhatsApp*, CANAL CIÊNCIAS CRIMINAIS (Dec. 17, 2015), http://canalcienciascriminais.com.br/artigo/investigacao-criminal-obstrucao-da-justica-e-bloqueio-do-whatsapp, *archived at* https://perma.cc/55UD-5JJB.

[30] Marcelo Crespo, *O Que Ninguém Falou Sobre o Caso Facebook*, JUSBRASIL (Mar. 2016), http://canalciencias criminais.jusbrasil.com.br/artigos/310735589/o-que-ninguem-falou-sobre-o-caso-do-facebook?ref=topic_feed, *archived at* https://perma.cc/Y7NB-7MRM.

Both cases are under judicial secrecy (*segredo de justiça*). Therefore, it was not possible to access the cases to precisely determine the legal basis for the actions taken against the executives of the companies and the current status of access to the users' communications.

III. Conclusion

In Brazil, the secrecy of communications is a constitutional principle that can be violated only by a court order. A specific law enacted in this regard regulates the issue and further determines that the authorized interception of communications also encompasses data systems.

The law does not make direct reference to decryption of communications after a warrant has been issued. However, the federal agency in charge of regulating telecommunications, in its regulations defining telecommunications and multimedia services, has specifically determined that the provider of such services must make available to the authorities authorized to request such information the technological resources necessary to suspend telecommunications confidentiality and the data relating to the suspension of telecommunications confidentiality.

In addition to these regulations, the Code of Civil Procedure states that no one is exempt from the duty to cooperate with the judiciary for the discovery of truth, and the Penal Code provides that disobeying a legal order is punishable by fifteen days to six months in jail and a fine.

Furthermore, whoever prevents or in any way obstructs the investigation of a criminal offense involving a criminal organization is punishable by imprisonment for three to eight years and a fine.

Apparently, the burden imposed on companies to make available the technological resources necessary to suspend telecommunications confidentiality includes the obligation to decrypt the communication. Otherwise, a court order granting access to an individual's communications would be easily avoided. In this sense, it seems that this is what occurred in the two cases mentioned above. As a result, in one instance the service was suspended, and in the other the executive was arrested as a means to compel the companies to grant access to the communications, whether encrypted or not.

Canada

Tariq Ahmad
Foreign Law Specialist

SUMMARY In Canada, the term "lawful access" is used to describe the government's surveillance powers, and primarily involves the interception of communications, the search and seizure of information, and the issuance of production and preservation orders. Part VI of Canada's Criminal Code regulates the powers of the police to engage in electronic surveillance or interception of private communications. With some exceptions, these powers require judicial authorization or a warrant before they can be exercised. Canada's existing legal framework for interception, search and seizure, and production of data also applies to encrypted data. However, there does not appear to be a specific provision that imposes requirements on telecommunications providers to decrypt data.

Since 1995, the Solicitor General's Enforcement Standards (SGES) have been in force. The SGES outline twenty-three technical surveillance standards that must be followed as a condition of obtaining a wireless spectrum license in Canada. Standard 12 establishes an obligation that any type of encryption algorithm initiated by a service provider must be provided to a requesting law enforcement agency. This excludes end-to-end encryption.

I. Introduction

In Canada, the term "lawful access" is used to describe the government's surveillance powers, and primarily involves the interception of communications, the search and seizure of information, and the issuance of production orders.[1] With some exceptions, these powers require judicial authorization or a warrant before they can be exercised.

Lawful access powers of the police are regulated by the Criminal Code,[2] while the surveillance powers of the Canadian Security Intelligence Service (CSIS) are governed by the Canadian Security Intelligence Service Act.[3] These powers are subject to the Canadian Charter of Rights and Freedoms and Canada's other privacy laws. On December 9, 2014, Bill C-13,[4] the most recent amending legislation that contains "lawful access" provisions, was passed. The law

[1] *Lawful Access FAQ*, SAMUELSON-GLUSKO CANADIAN INTERNET POLICY & PUBLIC INTEREST CLINIC (CIPPIC), http://www.cippic.ca/lawful-access-faq (last updated June 2, 2007), *archived at* https://perma.cc/MA4C-AGQU.

[2] CRIMINAL CODE, R.S.C. 1985, c. C-46, http://laws-lois.justice.gc.ca/eng/acts/C-46/, *archived at* https://perma.cc/KRF2-KJFN.

[3] Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23, http://laws-lois.justice.gc.ca/eng/acts/C-23/, *archived at* https://perma.cc/76L5-MHBU.

[4] Act to Amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act (Act) (Protecting Canadians from Online Crime Act), S.C. 2014, c. 31 (in force Mar. 9, 2015), http://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/FullText.html, *archived at* https://perma.cc/Y6ES-Q6AU.

includes "new investigative powers (preservation demands, preservation orders and production orders) for law enforcement officers for the conduct of their investigation."[5]

II. Encryption

A. Criminal Code's Lawful Access Powers

Part VI of Canada's Criminal Code regulates the powers of the police to engage in electronic surveillance or interception of private communications, including real-time communications, while conducting criminal investigations. Apart from certain exceptions outlined in the Code, judicial authorization is required for the interception of private communications, but in comparison to ordinary search warrants "[t]he requirements for obtaining such an authorization are more onerous."[6]

Police officials have the power to make demands to preserve computer data.[7] Subject to certain exceptions, searches and seizures[8] of computer data are also subject to judicial warrants. On application, courts may also issue preservation orders to preserve computer data[9] and production orders for the production of transmission[10] or tracking data.[11] In order to disclose the substance of a communication the police must apply for a general production order, which requires a higher evidentiary standard.[12] According to an RCMP statement reported in the news, "wiretap authorization, a search warrant and a general warrant can also be accompanied by an assistance order issued by a court, which compels a third party to provide assistance where that assistance may reasonably be considered as required to give effect to the authorization or warrant."[13]

---

[5] Sean Griffin, Anne-Elisabeth Simard & Marianne Bellefleur, *Bill C-13: Lawful Access and the Relationship Between Organizations, Cyber-bullying and the Protection of Privacy Rights*, SNIP/ITS (Feb. 25, 2015), http://www.canadiantechlawblog.com/2015/02/25/bill-c-13-lawful-access-and-the-relationship-between-organizations, *archived at* https://perma.cc/8YH7-PEEJ.

[6] Steven Penney, *National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits*, 48 OSGOODE HALL L.J. 247, 284 (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1994525, *archived at* https://perma.cc/KN8Q-X5LK (construing Criminal Code § 184.2).

[7] CRIMINAL CODE § 487.012(1).

[8] *Id.* § 487(1).

[9] *Id.* § 487.013(1).

[10] *Id.* § 487.016(1).

[11] *Id.* § 487.017(1).

[12] *Id.* § 487.014.

[13] Nicole Bogart, *Can Law Enforcement Legally Access Data on Your Smartphone in Canada?*, GLOBAL NEWS (Feb. 24, 2016), http://globalnews.ca/news/2537715/can-law-enforcement-legally-access-data-on-your-smartphone-in-canada, *archived at* https://perma.cc/4GDV-RJST. "Assistance orders" are provisioned under 487.02 of the Criminal Code, which stipulates that,

> [i]f an authorization is given under section 184.2, 184.3, 186 or 188 or a warrant is issued under this Act, the judge or justice who gives the authorization or issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the authorization or warrant.

CRIMINAL CODE § 487.02.

Canada's existing legal framework for interception, search and seizure, preservation and production of data, appears to apply to encrypted data or communications.[14] However, there does not appear to be a specific provision in the Criminal Code that imposes requirements on telecommunications providers to decrypt or establishes backdoor access. According to a recent statement by the Royal Canadian Mounted Police (RCMP) quoted in an investigative report by *Motherboard*, "there is no specific power in the Criminal Code to compel a third party to decrypt or develop decryption tools, nor is there any requirement for telecommunications services to provide these services,"[15] but courts may "compel" third parties like BlackBerry to assist with investigations.[16]

In the same *Motherboard* report defense lawyer Michael Lacy is quoted as saying that the RCMP's statement "is 'an overstatement of the law,' and that even though there is no explicit power relating to encryption backdoors in the Criminal Code, there may still be legal means to order a company to assist the police with decryption."[17]

According to another news report, which quotes Christopher Parsons, a security researcher and postdoctoral fellow at the University of Toronto's Citizen Lab, "[w]e don't actually understand how the RCMP is using the laws that are developed for them."[18] One critic notes that the Canadian government has been successful "at keeping their abilities regarding encryption quiet."[19]

Canada's previous Conservative government introduced lawful access legislation, Bill C-30, which included specific sections that would have imposed decryption requirements on telecommunications service providers, but the Bill was not adopted. Section 6(3) & (4) of the Bill stipulated as follows:

> (3) If an intercepted communication is encoded, compressed, encrypted or otherwise treated by a telecommunications service provider, the service provider must use the

[14] In October 1998 the Government of Canada announced its policy on cryptography, which stipulated that the government would "apply existing interception, search and seizure and assistance procedures to cryptographic situations and circumstances." *See 6.0 Cryptography Policies*, MCCARTHY TETRAULT, http://www.mccarthy.ca/pubs/cicpaper06.htm (last visited Apr. 19, 2016), *archived at* https://perma.cc/YH7W-SRRM; *see also* Christopher Parsons & Tamir Israel, *Canada's Quiet History of Weakening Communications Encryption*, THE CITIZEN LAB (Aug. 11, 2015), https://citizenlab.org/2015/08/canadas-quiet-history-of-weakening-communications-encryption, *archived at* https://perma.cc/HMT9-B3HW.

[15] Jordan Pearson & Justin Ling, *Exclusive: How Canadian Police Intercept and Read Encrypted BlackBerry Messages*, MOTHERBOARD (Apr. 14, 2016), http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada, *archived at* https://perma.cc/JK2T-RDQG.

[16] *Id*.

[17] *Id*.

[18] Justin Ling & Jordan Pearson, *Exclusive: Canadian Police Obtained BlackBerry's Global Decryption Key*, VICE NEWS (Apr. 14, 2016), https://news.vice.com/article/exclusive-canada-police-obtained-blackberrys-global-decryption-key-how, *archived at* https://perma.cc/K9AT-E36K.

[19] Jordan Pearson, *Canada Desperately Needs to Have a Public Debate About Encryption*, MOTHERBOARD (Apr. 14, 2016), http://motherboard.vice.com/read/canada-desperately-needs-to-have-a-public-debate-about-encryption, *archived at* https://perma.cc/9TGC-FZR9.

> means in its control to provide the intercepted communication in the same form as it was before the communication was treated by the service provider.
>
> (4) Despite subsection (3), a telecommunications service provider is not required to make the form of an intercepted communication the same as it was before the communication was treated if
>
> *(a)* the service provider would be required to develop or acquire decryption techniques or decryption tools; or
>
> *(b)* the treatment is intended only for the purposes of generating a digital signature or for certifying a communication by a prescribed certification authority, and has not been used for any other purpose.[20]

B. Solicitor General's Enforcement Standards

Since 1995, the Solicitor General's Enforcement Standards (SGES) have been in force. Those Standards outline twenty-three technical surveillance standards[21] identifying "how mobile telecommunications companies must configure their networks to facilitate telecommunications interceptions."[22] The Standards must be followed as a condition of obtaining a wireless spectrum license in Canada.[23]

Standard 12 stipulates that, "[i]f network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair."[24] The annotation for this standard also provides

> [l]aw enforcement requires that any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted. This would include proprietary compression algorithms that are employed in the network. This does not include end to end encryption that can be employed without the service provider's knowledge.[25]

---

[20] Bill C-30, An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act and to Amend the Criminal Code and Other Acts (Protecting Children from Internet Predators Act), http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5380965&File=59#10, *archived at* https://perma.cc/D3BL-WNPS.

[21] Parsons & Israel, *supra* note 14.

[22] TELECOM TRANSPARENCY PROJECT, THE GOVERNANCE OF TELECOMMUNICATIONS SURVEILLANCE: HOW OPAQUE AND UNACCOUNTABLE PRACTICES AND POLICIES THREATEN CANADIANS 10 (2015), https://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf, *archived at* https://perma.cc/5339-EUYK.

[23] Mathew Braga, *Why Canada Isn't Having a Policy Debate Over Encryption*, THE GLOBE AND MAIL (Feb. 23, 2016), http://www.theglobeandmail.com/technology/why-canada-isnt-having-a-rigorous-debate-over-encryption/article28859991, *archived at* https://perma.cc/YA8W-CDCR.

[24] Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications, Standard 12, https://cippic.ca/uploads/Solicitor_General_Standards_Annotaed-2008.pdf, *archived at* https://perma.cc/NQB9-ZHPY.

[25] *Id.*

Only circuit-based communications are subject to these requirements[26] as opposed to packet-based communications.[27]

These standards were reportedly updated in 2008 and only made public by *The Globe & Mail*, which obtained past and current versions of the documents in 2013.[28] Some critics have pointed to a lack of transparency "surrounding the government's position and policies" with regard to encryption.[29]

C. Police–Telecommunications Provider Cooperation on Encryption

In 2012, Rogers, a Canadian telecommunications provider, and the French telecommunications equipment company Alcatel-Lucent proposed an encryption backdoor for law enforcement at a meeting of the 3rd Generation Partnership Project's (3GPP's) Lawful Interception Working Group.[30] The proposal was for "a next-generation voice encryption protocol, known as MIKEY-IBAKE."[31] The protocol was designed to protect end-to-end conversations.[32] According to Parsons and Tamir Israel of the Citizen Lab this proposal was a discussion on "how to weaken communications-related encryption protocols such as MIKEY-IBAKE."[33] The Telecom Transparency Project describes this process as follows:

> Rogers and Alcatel Lucent proposed that "[i]nstead of deploying the true random number generator to create the random secret" that is used to establish an end-to-end encrypted communication, "a pseudo-random number generator (PRG) is deployed in the client application of the user device." The Rogers/Alcatel Lucent solution would let a TSP either decrypt traffic in real time or retroactively decrypt traffic that had been encrypted using the PRG. As such, their proposal would effectively undermine the core security design decisions that were "baked" into MIKEY-IBAKE.[34]

According to an investigative report by *Motherboard*, Canadian police have been in possession of a BlackBerry master encryption key since 2010. The report states that the RCMP used the key in a criminal investigation into a mafia-related death that took place between 2010 and 2012 to intercept and decrypt over one million BlackBerry messages sent using its proprietary BBM

---

[26] TELECOM TRANSPARENCY PROJECT, *supra* note 22, at 10.

[27] Parsons & Israel, *supra* note 14.

[28] *Id*.

[29] *Id*.

[30] Matthew Braga, *Rogers and Alcatel-Lucent Proposed an Encryption Backdoor for Police*, MOTHERBOARD (Feb. 12, 2016), http://motherboard.vice.com/read/rogers-and-alcatel-lucent-proposed-an-encryption-backdoor-for-police, *archived* at https://perma.cc/4U75-7B5R.

[31] *Id*.

[32] *Id*.

[33] Parsons & Israel, *supra* note 14.

[34] TELECOM TRANSPARENCY PROJECT, *supra* note 22, at 10 (footnote in original omitted).

service. Based on court records in the case, it is unclear how the RCMP actually obtained the key, *Motherboard* said.[35]

III. Conclusion

In conclusion, although there is no specific provision or power in Canada's Criminal Code to compel a third-party telecommunications provider to decrypt or create decryption tools, Canada's existing lawful access provisions in the Code may provide a legal framework for ordering companies to assist the police with decryption.

[35] Pearson & Ling, *supra* note 15.

European Union

Theresa Papademetriou
Senior Foreign Law Specialist

SUMMARY At the European Union (EU) level, there is no requirement that keys to encrypted materials be disclosed to law enforcement authorities, or that companies decrypt communications in response to a government request. A 2001 nonbinding resolution merely calls upon the Member States in cooperation with telecommunications companies to take into consideration the operational needs of law enforcement authorities when data are encrypted. Electronic surveillance is regulated at the EU Member State level.

The EU agencies dealing with security, terrorism, cybercrime, and organized crime have not reached consensus on access to encryption by law enforcement authorities. The EU's cybersecurity agency, the European Union Agency for Network and Information (ENISA), is against creating backdoors in encryption products, whereas the EU Counter-Terrorism Coordinator believes the Commission should contemplate introducing legislation on this matter. In a similar vein, the EU's law enforcement agency, Europol, favors enacting legislation on disclosure as the only practical solution for handling encryption when the keys are held by individual users.

I. Introduction

The European Union (EU) and its Member States share competence in enacting legislation to combat serious crime, including terrorism and organized crime, and to reinforce cooperation between police and judicial authorities to protect people in the EU, while at the same time ensuring compliance with EU rules on personal data protection and privacy.[1] Electronic surveillance conducted by national law enforcement authorities to detect and investigate crimes and the parallel cooperation of telecommunications and Internet service providers to allow access is an issue that is regulated at the Member State level.[2] The Paris and Brussels terrorist attacks reignited the debate across Europe over whether to expand monitoring by law enforcement authorities in light of concerns about potential violations of the privacy and personal data of individuals. A number of Member States have shown a keen interest in granting their law enforcement authorities greater access to personal data.[3]

---

[1] Consolidated Version of the Treaty on European Union art. 3, para. 2, 2012 OFFICIAL JOURNAL OF THE EUROPEAN UNION [O.J.] (C 326) 13, updated version *available at* http://data.consilium.europa.eu/doc/document/ST-6655-2008-REV-8/en/pdf, *archived at* https://perma.cc/7Z7R-5RQ4.

[2] Consolidated Version of the Treaty on the Functioning of the European Union art. 4, para. 2(J), 2012 O.J. (C 326) 47, updated version *available at* http://data.consilium.europa.eu/doc/document/ST-6655-2008-REV-8/en/pdf, *archived at* https://perma.cc/7Z7R-5RQ4.

[3] Patrick Howell O'Neill, *Dutch Government Backs Strong Encryption, Condemns Backdoors*, THE DAILY DOT (Jan. 4, 2016), http://www.dailydot.com/politics/dutch-encryption-cabinet-backdoor, *archived at* https://perma.cc/CTR7-C7GK; Thorsten Benner & Mirko Hohmann, *How Europe Can Get Encryption Right*, POLITICO (Apr. 13, 2016), http://www.politico.eu/article/how-europe-can-get-encryption-right-data-protection-privacy-counter-terrorism-technology, *archived at* https://perma.cc/9N7W-786H; *see also* Paul Hockenos, *Europe Considers Surveillance*

II. Legal Framework

At the EU level, two measures deal with access to personal data by law enforcement authorities: a 2001 nonbinding Resolution[4] establishing guidelines concerning cooperation between law enforcement authorities and the telecommunications industry, and the Authorization Directive (2002/20/EC), which, *inter alia*, makes lawful interception by law enforcement authorities a condition for granting electronic networks and services the authority to operate.[5]

The 2001 Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services,[6] similarly to its predecessor Resolution adopted in 1995 on the Lawful Interception of Telecommunications,[7] contains in the Annex a detailed list of the operational needs of law enforcement authorities.[8] The Resolution calls upon the EU Member States to cooperate with communications service providers and to take into account law enforcement operational needs in the development and implementation of any measures concerning legally authorized forms of interception of telecommunications.[9] It is up to the discretion of the Member States to adopt legislation requiring telecommunications industries to decrypt materials.

The Resolution, which contains language specific to encrypted materials, calls on the Member States to provide that,

> [i]f network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair [in a readable format].[10]

Expansion After Deadly Attacks, THE INTERCEPT (Jan. 20, 2015), https://theintercept.com/2015/01/20/europe-considers-surveillance-expansion, *archived at* https://perma.cc/6VHP-WLGP.

[4] Resolutions adopted by EU institutions are non-binding and are published in the "C" series of the *Official Journal* (O.J.) of the EU rather than in the "L" series of the O.J. where all legislation is published. *Legislation*, EUR-LEX, http://eur-lex.europa.eu/collection/eu-law/legislation/recent.html (last visited Apr. 21, 2016), *archived at* https://perma.cc/P2FA-NXZW.

[5] Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the Authorization of Electronic Communications and Services (Authorization Directive), 2002 O.J. (L 108) 21, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0021:0032:EN:PDF, *archived at* https://perma.cc/V49P-2RDA.

[6] Council of the European Union, Council Resolution on Law Enforcement Operational Needs with Respect to Public Telecommunication Networks and Services, June 20, 2001, *available at* http://www.statewatch.org/news/2001/sep/9194.pdf, *archived at* https://perma.cc/66XC-ZP3R. This Council Resolution was not published in the *Official Journal*.

[7] Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications, 1996 O.J. (C 329) 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML, *archived at* https://perma.cc/QRY9-VXAU.

[8] Council Resolution, *supra* note 6.

[9] *Id*., Annex.

[10] *Id.*, Annex, para. 3.3.

Directive 2002/20/EC contains a number of conditions that may be attached to the general authorization for providing electronic communications networks or services,[11] among them the "[e]nabling of legal interception by competent national authorities in conformity with Directive 97/66/EC and Directive 95/46/EC . . . on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[12]

III. Encryption

Currently, the EU does not require that keys to encrypted material be disclosed to law enforcement authorities or require companies to decrypt encrypted communications on request of a government, nor have its critical agencies on cybersecurity, organized crime, and terrorism reached a clear and uniform position on this issue.

A. Europol

The 2015 Internet Organised Crime Threat Assessment (IOCTA) prepared by Europol, the EU's law enforcement agency, estimates that more than three-quarters of cybercrime investigations in the EU confront the use of some form of encryption to protect data and avoid interception. Both TrueCrypt and BitLocker are commonly and increasingly encountered, despite the cessation of TrueCrypt's development in May 2014. Almost half of all Member States also noted an increased use of encrypted email, typically through PGP (Pretty Good Privacy) software.[13]

The IOCTA explored various options in its debate on encryption, such as using "key escrow" systems, using weakened encryption, or introducing legislation on the mandatory disclosure of encryption keys. It concluded that legislation was the only practical solution for handling encryption, especially in instances where the keys are held by individual users.[14]

In addition, the IOCTA made the following two specific recommendations:

> - Law enforcement would benefit from a central database of VPN [Virtual Private Network] and proxy services used by cybercriminals to determine if any are suitable for either information exchange with law enforcement or intervention if criminal in nature.
> - Legislators and policy makers, including industry representatives and academia, must implement a workable solution to the issue of encryption which allows legitimate users to protect their privacy and property without severely compromising government and law enforcement's ability to investigate criminal or national security threats.[15]

[11] Directive 2002/20/EC, *supra* note 5, art. 6, para. 1.

[12] *Id.*, Annex(A), para. 11.

[13] Europol, *The Internet Organised Crime Threat Assessment (IOCTA) 2015*, at 50, *available at* http://statewatch.org/news/2015/oct/eu-europol-iocta-2015.pdf, *archived at* https://perma.cc/CPA4-58W3.

[14] *Id.* at 69.

[15] *Id*. at 51.

Regarding the enactment of "obligation to disclose" laws, which would oblige individuals to disclose their encryption keys or be subject to a criminal penalty, the IOCTA noted that "this tends to be effective only when data remains on the suspect/criminal's computer. If the keys are transient, especially if they are system generated, it can be practically impossible to recover these."[16]

Finally, the Director of Europol, Rob Wainwright, declared that encrypted communications are the biggest obstacle to monitoring terrorists' actions, adding that "there is a significant capability gap that has to change if we're serious about ensuring the internet isn't abused and effectively enhancing the terrorist threat."[17]

B. EU Cybersecurity Agency

On March 26, 2016, the EU's cybersecurity agency, the European Union Agency for Network and Information (ENISA), declared that it is against forcing Internet and telecommunications companies to create backdoors for authorities to unlock encrypted messages. ENISA's director, Udo Helmbrecht, pointed out that the EU has sufficient legislation on information sharing among the national intelligence agencies of the Member States, and emphasized that available information is not used sufficiently and effectively.[18]

C. EU Counter-Terrorism Coordinator

The EU Counter-Terrorism Coordinator, Gilles de Kerchoven, in a 2015 document addressed to EU Justice and Home Affairs Ministers, expressed the view that the European Commission "should be invited to explore rules obliging internet and telecommunications companies operating in the EU to provide . . . access of the relevant national authorities to communications (i.e. share encryption keys)."[19]

D. EU Internet Forum

In 2015, the Commission announced in its Communication on Security Agenda the creation of an IT forum where Europe's major IT companies would be invited to discuss a number of concerns, including "deploying the best tools to counter terrorist propaganda on the internet and in social networks" and "the concerns of law enforcement authorities on new encryption

[16] *Id.* at 69.

[17] *Europol Chief Warns on Computer Encryption*, BBC (Mar. 29, 2015), http://www.bbc.com/news/technology-32087919, *archived at* https://perma.cc/Q9FQ-JL55.

[18] Catherine Stupp, *EU Cybersecurity Agency Slams Calls for Encryption Backdoors*, EURACTIV (Mar. 30, 2016), http://www.euractiv.com/section/digital/news/eu-cybersecurity-agency-slams-calls-for-encryption-backdoors, *archived at* https://perma.cc/K9U3-NRFW.

[19] Council of the European Union, General Secretariat, EU CTC Input for the Preparation of the Informal Meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015, DS1035/15 (Jan. 17, 2015), *available at* http://www.statewatch.org/news/2015/jan/eu-council-ct-ds-1035-15.pdf, *archived at* https://perma.cc/XA4T-CF2B.

technologies."[20] The EU Internet Forum was established on December 3, 2015, through the joint efforts of Dimitris Avramopoulos, the EU Commissioner for Migration, Home Affairs and Citizenship, and Věra Jourová, the Commissioner for Justice, Consumer and Gender Equality.[21]

IV. Conclusion

Currently, there is no EU legislation that requires tech companies to disclose the keys to encrypted materials to law enforcement authorities, or to decrypt communications upon the request of a government.

[20] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*, at 13–14, COM (2015) 185 final (Apr. 28, 2015), http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, *archived at* https://perma.cc/9NXB-SHLK.

[21] European Commission Press Release IP/15/6243, EU Internet Forum: Bringing Together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online (Dec. 3, 2015), http://europa.eu/rapid/press-release_IP-15-6243_el.htm, *archived at* https://perma.cc/H225-L5CQ.

France

Nicolas Boring
Foreign Law Specialist

I. Decryption at the Request of Intelligence and Security Services

French law authorizes national intelligence and security services to intercept and read private communications for specifically enumerated purposes, including protecting national security, protecting the "safety of essential elements of France's economic and scientific potential," preventing acts of terrorism, repressing organized crime, or preventing the reconstitution of illegal groups (such as banned hate groups or private paramilitary groups).[1]

Such interceptions must be authorized in writing by the Prime Minister or someone specifically and directly chosen by him/her for that purpose, upon the written request of the Defense Minister, the Minister of the Interior, or the minister in charge of customs and border security.[2]

Agents duly authorized to intercept electronic communications for intelligence purposes may request from providers of cryptology services the means to decipher their codes.[3] This refers not just to encryption keys, but also to any software or other information that would allow the encrypted data to be read.[4] A cryptology service provider must submit to the request within seventy-two hours.[5] Furthermore, a cryptology service provider may be required to apply the means of decryption him/herself within that same timeframe, unless he/she can demonstrate an inability to do so.[6]

---

[1] CODE DE LA SECURITE INTERIEURE [INTERIOR SECURITY CODE] art. L811-3, https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000025503132&idArticle=LEGIARTI000030935040&dateTexte=&categorieLien=cid, *archived at* https://perma.cc/Z32U-CVJA & art. L852-1, https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000030935848&cidTexte=LEGITEXT000025503132&dateTexte=20160322&fastPos=1&fastReqId=19915746&oldAction=rechCodeArticle, *archived at* https://perma.cc/28FX-F4S4.

[2] *Id.* art. L821-4, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030935046&cidTexte=LEGITEXT000025503132&dateTexte=20160321, *archived at* https://perma.cc/ V74K-J3AQ.

[3] *Id.* art. L871-1, https://www.legifrance.gouv.fr/affichCode.do?idSectionTA=LEGISCTA000030937374&cidTexte=LEGITEXT000025503132&dateTexte=20160321, *archived at* https://perma.cc/9DPZ-JSK8.

[4] *Id.* art. R871-3, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=64075B6429EC9ED93CFF00D70F55E60E.tpdila14v_1?idSectionTA=LEGISCTA000031944913&cidTexte=LEGITEXT000025503132&dateTexte=20160322, *archived at* https://perma.cc/S6XJ-NS7D.

[5] *Id.* art. L871-1.

[6] *Id.*

II. Decryption at the Request of Judicial and Law Enforcement Agencies

If certain conditions are met, an investigative judge (*juge d'instruction*) may order the interception, recording, and transcription of private telecommunications for the purposes of a criminal investigation.[7] In certain circumstances, telecommunications interception, recording, and transcription may also be ordered by a *juge des libertés et de la detention* (a judge who specializes in determining whether a suspect should be placed in police custody).[8]

When intercepted information is password protected or encrypted, law enforcement authorities may ask any qualified person or corporation to perform the technical operations that would allow access to this information.[9] This requires authorization from the investigative judge, the public prosecutor (*procureur de la République*), or the court that has jurisdiction over the crime being investigated.[10] The Code of Criminal Procedure also provides that law enforcement authorities can request the help of a "Technical Support Center," which was created in 2002 under the authority of the Ministry of the Interior (the ministry in charge of law enforcement in France).[11] Details on this "Technical Support Center" are classified,[12] but it appears to specialize in data decryption.[13]

---

[7] CODE DE PROCÉDURE PÉNALE [CODE OF CRIMINAL PROCEDURE] art. 100, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=42F5EDFF9D0C401F5371916B7A9BDE31.tpdila14v_1?idSectionTA=LEGISCTA000006182887&cidTexte=LEGITEXT000006071154&dateTexte=20160322, *archived at* https://perma.cc/YG4V-8FJT.

[8] *Id.* art. 706-95, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=42F5EDFF9D0C401F5371916B7A9BDE31.tpdila14v_1?idSectionTA=LEGISCTA000006167523&cidTexte=LEGITEXT000006071154&dateTexte=20160322, *archived at* https://perma.cc/V8ZJ-QK5M.

[9] *Id.* art. 230-1, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=42F5EDFF9D0C401F5371916B7A9BDE31.tpdila14v_1?idSectionTA=LEGISCTA000023712010&cidTexte=LEGITEXT000006071154&dateTexte=20160322, *archived at* https://perma.cc/6UWV-3BZJ.

[10] *Id.*

[11] Décret n°2002-1073 du 7 août 2002 d'application de l'article 30 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et portant création du centre technique d'assistance [Decree No. 2002-1073 of August 7, 2002, Applying Article 30 of Law No. 2001-1062 of November 2001 Regarding Everyday Security and Creating the Technical Support Center] (as amended on May 9, 2014), http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D3D3BF1F4D47E24B7C9D0FB4B55005AC.tpdjo06v_2?cidTexte=LEGITEXT000005633260&dateTexte=20150127, *archived at* https://perma.cc/H8C6-RNNP.

[12] *Id.*

[13] *Circulaire relative au fonctionnement du centre technique d'assistance (C.T.A.)* [*Circular Regarding the Functioning of the Technical Support Center (C.T.A.)*], MINISTÈRE DE L'INTÉRIEUR, DE LA SÉCURITÉ INTÉRIEURE ET DES LIBERTÉS LOCALES [MINISTRY OF THE INTERIOR, OF INTERIOR SECURITY, AND OF LOCAL FREEDOMS] (Mar. 27, 2003), http://www.interieur.gouv.fr/content/download/8005/75906/file/INTC0300032C.pdf, *archived at* https://perma.cc/E4Z8-65NX.

Germany

Jenny Gesley
Foreign Law Specialist

I. Interception of Communications Data

Article 10 of the German Basic law provides that the privacy of correspondence, mail, and telecommunications is inviolable. Restrictions may only be imposed pursuant to law. If the restriction serves to protect the free, democratic basic order or the existence or security of the German Federation or of a German state, the law may provide that the affected person will not be informed of the measure.[1]

Several German intelligence and law enforcement agencies have been authorized to access, intercept, and request stored communications data. This authority and its limits are delineated in article 10 of the Basic Law as explained above and in specific acts. For the Federal Intelligence Agencies, the specific authorizations are contained in the Act on the Federal Office for the Protection of the Constitution;[2] the Act on the Federal Intelligence Service;[3] the Act on the Military Counterintelligence Service;[4] and the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications (Article 10 Act).[5]

Furthermore, restrictions on the privacy of mail and telecommunications undertaken by Federal Intelligence Agencies are monitored by the Article 10 Commission of the German Parliament.[6]

The authorizations for the federal law enforcement agencies are contained in the Act on the Federal Criminal Police Office,[7] the Act on the Federal Police,[8] the Act on the Customs

---

[1] GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GRUNDGESETZ] [GG] [BASIC LAW], May 23, 1949, BUNDESGESETZBLATT [BGBL.] [FEDERAL LAW GAZETTE] I at 1, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_gg/basic_law_for_the_federal_republic_of_germany.pdf, *archived at* http://perma.cc/MER4-79JH.

[2] Bundesverfassungsschutzgesetz [BVerfSchG], Dec. 20, 1990, BGBL. I at 2954, 2970, as amended, §§ 8a, 8d, http://www.gesetze-im-internet.de/bundesrecht/bverfschg/gesamt.pdf, *archived at* http://perma.cc/C858-Y6VY.

[3] Bundesnachrichtendienstgesetz (BNDG), Dec. 20, 1990, BGBL. I at 2954, 2979, as amended, §§ 2a, 2b, http://www.gesetze-im-internet.de/bundesrecht/bndg/gesamt.pdf, *archived at* http://perma.cc/7DTM-H656.

[4] Gesetz über den militärischen Abschirmdienst [MADG], Dec. 20, 1990, BGBL. I at 2954, 2977, as amended, §§ 4a, 4b, http://www.gesetze-im-internet.de/bundesrecht/madg/gesamt.pdf, *archived at* http://perma.cc /99CA-LB6W.

[5] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel 10-Gesetz] [G 10], June 26, 2001, BGBL. I at 1254, 2298, as amended, § 1, para. 1, http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf, *archived at* http:// perma.cc/6YVZ-UCCU.

[6] Article 10 Act § 1, para. 2, § 15.

[7] Bundeskriminalamtgesetz [BKAG], July 7, 1997, BGBL. I at 1650, as amended, § 7, paras. 3, 4; § 20b, paras. 3, 4; § 20l; § 20m; § 20m; § 22, http://www.gesetze-im-internet.de/bundesrecht/bkag_1997/gesamt.pdf, *archived at* http://perma.cc/XJ9R-4HUX.

Investigation Bureau and the Customs Investigation Offices,[9] and the Code of Criminal Procedure.[10]

II. Transmission of Communications

The German Federal Constitutional Court has held that the transmission of subscriber data by telecommunications providers to a requesting agency is only permissible if there is a legal norm authorizing the agency to request the data and an additional legal norm obligating the telecommunications provider to transfer the data ("double door model").[11] Telecommunications providers are defined as anyone who exclusively or occasionally provides telecommunications services or who contributes to the provision of such services.[12]

Anyone who operates a telecommunications network that provides publicly available telecommunications services to more than 10,000 participants is obligated to install a surveillance system that complies with the technical requirements set out in the Telecommunications Surveillance Directive and the technical guideline adopted by the German Federal Network Agency.[13] Telecommunications providers must ensure that they are at all times capable of being informed by telephone of incoming requests and their urgency, and that they are able to accept and process such requests during regular business hours.[14]

---

[8] Bundespolizeigesetz [BpolG], Oct. 19, 1994, BGBL. I at 2978, 2979, as amended, http://www.gesetze-im-internet.de/bundesrecht/bpolbg/gesamt.pdf, *archived at* http://perma.cc/LEU5-HE59.

[9] Gesetz über das Zollkriminalamt und die Zollfahndungsämter [ZFdG], Aug. 16, 2002, BGBL. I at 3202, as amended, § 7, paras. 5-9; § 15, paras. 2–6; §§ 23a–23g, http://www.gesetze-im-internet.de/bundesrecht/zfdg/gesamt.pdf, *archived at* http://perma.cc/T7J8-T9TV.

[10] Strafprozessordnung [StPO], Apr. 7, 1987, BGBL. I at 1074, 1319, as amended, §§ 100a, 100b, 100g, 100i, 100j, http://www.gesetze-im-internet.de/bundesrecht/stpo/gesamt.pdf, *archived at* http://perma.cc/ZA7K-47GY, unofficial English translation *at* http://www.gesetze-im-internet.de/englisch_stpo/german_code_of_criminal_procedure.pdf, *archived at* http://perma.cc/A6MH-9KXA (English translation only current up to 2014).

[11] BUNDESVERFASSUNGSGERICHT [BVERFG] [FEDERAL CONSTITUTIONAL COURT], 100 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] [DECISIONS OF THE FEDERAL CONSTITUTIONAL COURT] 313, 366 *et seq.*, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/07/rs19990714_1bvr222694en.html, *archived at* http://perma.cc/QBZ9-3B9A. If the agency is authorized by law to request communications data, the Telecommunications Act requires telecommunications providers to immediately comply with such a request. Telekommunikationsgesetz [TKG] [Telecommunications Act], June 22, 2004, BGBL. I at 1190, as amended, §§ 110–115, http://www.gesetze-im-internet.de/bundesrecht/tkg_2004/gesamt.pdf, *archived at* http://perma.cc/WP2Y-XH69.

[12] Telecommunications Act § 3, no. 6.

[13] Telekommunikations-Überwachungsverordnung [TKÜV] [Telecommunications Surveillance Directive], Nov. 3, 2005, BGBL. I at 3136, as amended, §§ 3, 5, para. 1, http://www.gesetze-im-internet.de/bundesrecht/tk_v_2005/gesamt.pdf, *archived at* http://perma.cc/4MFL-9LW8; Technical Guideline for the Implementation of Legal Measures for the Surveillance of Telecommunications and the Disclosure of Information, Oct. 15, 2015, http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/TechnUmsetzung110/Downloads/TRTK%C3%9CV%20englische%20Version.pdf?__blob=publicationFile&v=7, *archived at* http://perma.cc/F382-S4TE.

[14] Telecommunications Surveillance Directive § 12.

Once a request from an authorized agency is received, a surveillance copy of the communications must be compiled and transmitted without undue delay.[15] It must include informational content and event data.[16] The communications are transmitted in the form in which they were received by the telecommunications provider.[17] If the telecommunications providers do not comply with a lawful transmission request, the Federal Network Agency may impose fines of up to €500,000 (around US$561,100) to force compliance, or partially or completely shut down the operations of the providers.[18]

III. Encryption of Communications

The aforementioned laws, which allow the access, interception, and transmission of communications, make no distinction between encrypted and unencrypted communications. If the communications have been encrypted by the user, federal intelligence agencies and law enforcement agencies are allowed to use whatever technologies they have at their disposal to unlock lawfully intercepted and transmitted encrypted communications. If they discover an encryption or network key during the course of the interception or surveillance of communications or during the course of a lawful search, they may use it to unlock the encrypted communications.[19]

However, there is no legal basis that would compel the user to turn over an encryption or network key, in particular with regard to the *nemo tenetur* principle. The *nemo tenetur* principle, derived from the general right of personality found in the German Basic Law and from section 136, para. 1, sentence 1 of the German Code of Criminal Procedure, states that a suspect may not be compelled to cooperate in an investigation that would incriminate him/herself.

If the communications were encrypted by the telecommunications providers (network encryption), the encryption must be removed at the point of transmission to the requesting agency.[20] Furthermore, if the telecommunications providers support encryption of peer-to-peer communications over the Internet by means of key management provided by them without involving their network elements or those of their partners in the transmission of the content, the providers must make the initial key available to the requesting agency. The telecommunications providers do not need to transmit the exchanged key if they can remove the encryption themselves by means of additional network elements.[21]

[15] *Id*. § 6, para. 1.

[16] *Id*. § 5, para. 1.

[17] *Id*. § 8, para. 2, no. 3.

[18] Telecommunications Act § 115.

[19] Code of Criminal Procedure § 95.

[20] Telecommunications Surveillance Directive § 8, para. 3.

[21] Technical Guideline, Part A, Annex D.1, para. 7.5.1; Part A, Annex H.3.2, para. 5.5; Part A, Annex H.3.3, para. 4.4; Part A, Annex H.3.4, para. 6.2.

IV. European Developments

In an April 2015 communication titled "European Agenda on Security," the EU Commission proposed, among other ideas, to create an EU Forum with IT companies to help counter terrorist propaganda and address the concerns of law enforcement agencies about new encryption technologies.[22] The EU Forum was officially launched in December 2015.[23]

Furthermore, in July 2015, Europol launched the European Union Internet Referral Unit (EU IRU). The goal of the EU IRU is "to combat terrorist propaganda and related violent extremist activities on the internet."[24] Europol Director Rob Wainwright has expressed concerns that encrypted communications pose problems for law enforcement when dealing with terrorism threats.[25] The German government stated that it supports the efforts and goals of the EU IRU, but that it was not aware of specific plans that were discussed with technology firms regarding encryption mechanisms.[26]

[22] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, the European Agenda on Security*, at 16, COM (2015) 185 final (Apr. 28, 2015), http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, *archived at* http://perma.cc/Z8AR-ALEE.

[23] European Commission Press Release IP/15/6243, EU Internet Forum: Bringing Together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online (Dec. 3, 2015), http://europa.eu/rapid/press-release_IP-15-6243_en.htm, *archived at* http://perma.cc/PYG3-3DMD.

[24] Europol Press Release, Europol's Internet Referral Unit to Combat Terrorist and Violent Extremist Propaganda (July 1, 2015), https://www.europol.europa. eu/content/europol%E2%80%99s-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda, *archived at* http://perma.cc/6VA4-5RK2.

[25] Warwick Ashford, *EU Launches Internet Referral Unit to Combat Online Extremism*, COMPUTERWEEKLY.COM (July 1, 2015), http://www. computerweekly.com/news/4500249133/EU-launches-Internet-Referral-Unit-to-combat-online-extremism, *archived at* http://perma.cc/DYN5-UVG2.

[26] DEUTSCHER BUNDESTAG: DRUCKSACHEN UND PROTOKOLLE [BT-DRS.] 18/5144, p. 6, questions 16, 17, http://dip21.bundestag.de/dip21/btd/18/051/1805144.pdf, *archived at* http://perma.cc/YVE2-8DBW.

Israel

Ruth Levush
Senior Foreign Law Specialist

SUMMARY Israel's Secret Monitoring Law, 5739-1979, generally protects privacy rights in Israel by prohibiting the monitoring of conversations, but also carves out certain exceptions to the prohibition in order to protect national and public security. Access to communications data, including traffic data and information regarding the location and identity of a subscriber, may also be authorized for saving or protecting human life, investigating or preventing offenses, identifying and indicting offenders, and lawfully confiscating property. In addition, warrantless orders for access to communications data may be issued under emergency situations to prevent the perpetration of a serious offense, identify the perpetrator, or save human life. Warrantless orders can also be issued for national security purposes under limited circumstances and for a limited duration.

The Order Governing the Control of Commodities and Services (Engagement in Encryption Items) 5735-1974, as amended, prohibits any person from engaging in encryption in the absence of a license issued by the Ministry of Defense and in violation of the conditions enumerated in the license. The Order identifies three types of licenses and exempts certain encryption activities from the licensing requirements.

I. Secret Monitoring

Israel's Secret Monitoring Law, 5739-1979, provides that "listening to the conversation of another" by means of an instrument in order to prevent and detect crimes generally requires a warrant issued by the president of a district court or his designee.[1] However, listening to conversations conducted in the public domain to protect state security and to prevent and detect crimes is exempt from this requirement.[2] Monitoring international conversations for military censorship and monitoring conversations that utilize communications systems used by the Israel Defense Forces (IDF), the Israeli Police, employees of the Ministry of Communication, and licensed service providers are similarly exempt. Wireless communications for the frequency ranges that are used by amateur radio operators and for broadcasting to the public also do not require permission under the law.[3]

The Law also authorizes the Prime Minister or the Minister of Defense, upon a written request by the IDF Intelligence Division or the General Security Service (GSS), to authorize secret monitoring after considering the extent of harm to privacy and determining that the monitoring is

[1] Secret Monitoring Law, 5739-1979, §§ 1, 6, SEFER HAHUKIM [BOOK OF LAWS] [SH] (official gazette) No. 938 p. 118, *as amended*, up-to-date text available in the Nevo Legal Database, *at* http://www.nevo.co.il (in Hebrew; by subscription), *archived at* https://perma.cc/EPD4-BV6R.

[2] *Id*. § 8(1).

[3] *Id*. § 8(2)–(5).

necessary for state security.[4] Granting or extending authorization for secret monitoring for state security reasons is subject to a three-month limit, which can be periodically extended.[5] In emergency situations and subject to conditions enumerated in the Law, the head of the Israel Security Agency (ISA) or the IDF Intelligence Division are also authorized to issue permits for monitoring conversations.[6]

Under the Communications (Communications and Broadcasts) Law, 5742-1982, the Prime Minister may issue instructions to a licensed communications service provider (licensee) to provide or facilitate government surveillance in response to a request by the Minister of Defense, the Minister of Domestic Security, the GSS, or the Institute for Intelligence and Special Operations (the Mossad), on the basis of state or public security considerations, and after consultation with the Minister of Communications.[7]

II. Interception of Communications Data

Access to communications data, including information regarding traffic data and the location and identity of a subscriber, may also be authorized by a warrant issued by a circuit court upon the request of an officer designated for this purpose by the General Police Commissioner or by a representative of another investigative authority defined by law.[8] The court will issue a warrant if it determines that access is required for saving or protecting human life, investigating or preventing offenses, identifying and indicting offenders, or lawfully confiscating property.[9]

Warrantless orders for access to communications data may also be issued by an authorized law enforcement officer for a limited duration when the officer is convinced that there is an imminent need to receive communications data without delay to prevent the perpetration of a serious offense, identify the perpetrator, or save human life.[10]

The GSS Law, 5762-2002, authorizes the Prime Minister to issue rules categorizing data (excluding the content of conversations) that must be made accessible to the ISA by communications licensees for national security purposes.[11] Orders for data transmission issued by the head of the ISA in accordance with these rules must specify the type and purpose of the data and the particulars of the database in which it is stored. Such orders are effective for a limited period of up to six months and may be renewed.[12]

---

[4] *Id*. § 4.

[5] *Id*.

[6] *Id*. § 5.

[7] Communications (Telecommunications and Broadcasting) Law, 5782-1982, § 13, SH No. 1060 p. 216, *as amended*, *available at* http://www.nevo.co.il, *archived at* https://perma.cc/D5CC-UB5B.

[8] Criminal Procedure (Enforcement Authorities–Communications Data) Law, 5768-2007, § 3, SH No. 2122 p. 72, *available at* http://www.nevo.co.il, *archived* at https://perma.cc/Q4MZ-FPYB.

[9] *Id*. § 3(a).

[10] *Id*. § 4.

[11] General Security Service Law, 5762-2002, § 11(b), SH No. 1832 p. 179, *as amended*.

[12] *Id.* § 11(c).

III. Regulation of Encryption

Encryption is regulated by the Order Governing the Control of Commodities and Services (Engagement in Encryption Items) 5735-1974, as amended (the Encryption Order).[13] On the basis of a 1998 amendment to the Encryption Order, the control and licensing of encryption items were transferred "from a military to a civilian licensing authority—i.e., from the IDF to the Ministry of Defense."[14]

The Encryption Order prohibits any person from engaging in encryption in the absence of a license issued by the General Manager of the Ministry of Defense and in violation of the conditions enumerated in the license.[15]

The General Manager of the Ministry of Defense is authorized to enter any place where an encryption related activity is being conducted and request a licensee to provide information at any time before and after the issuance of an encryption license.[16]

The Order provides for three categories of licenses for engaging in encryption:

> A "Restricted License" – a license that imposes restrictions on engagement in encryption items. These restrictions may also apply to permissible forms of engagement in encryption items, or to the nature of permissible sales (e.g. restriction on selling to certain countries and sectors). As a rule, a restricted license is valid for one year.
>
> A "Special License" – is a license for specific engagement; generally involving sale to clients who do not fall under the restrictions imposed on an applicant for a Restricted License. As a rule, a special license is valid for one year.
>
> A "General License" – a license for a particular encryption item which allows the license-holder free use of that item (other than modifications or integration that essentially create a new item for which a separate license is required). The sale of such items of encryption is decontrolled and not subject to reporting procedures. Such general licenses are issued with no time limit to their validity.[17]

[13] Order Governing the Control of Commodities and Services (Engagement in Encryption Items) (Encryption Order), 5735-1974, KOVETZ HATAKANOT 5735 No. 3232 p. 45, *available at* http://www.nevo.co.il, *archived at* https://perma.cc/9KKF-PVJY.

[14] *Encryption Controls in Israel*, MINISTRY OF DEFENSE, http://www.mod.gov.il/English/Encryption_Controls/Pages/default.aspx (last visited Apr. 18, 2016), *archived at* https://perma.cc/X4HB-BEW2.

[15] Encryption Order § 2.

[16] *Id*. §§ 4 & 6.

[17] MINISTRY OF DEFENSE, *supra* note 14.

The Order also provides for a category of "Free Means," which exempts certain encryption activities from licensing requirements. "Free Means" is defined as

> a means of encryption for which a general license has been granted or which the Director-General has declared to be decontrolled. Once an encryption item is defined as a free means, it is free of the licensing restrictions. A periodically revised list of encryption items which have been declared "decontrolled" is published in the Official Gazette of the Government of Israel as well as on [the Ministry of Defense] website.[18]

[18] *Id*.

Japan

Sayuri Umeda
Foreign Law Specialist

Law enforcement officials in Japan may request the courts to order the decryption of encrypted information during criminal investigations. Courts during trials may also order the decryption of encrypted information.

The Criminal Procedure Code states that where an article to be seized is a recording medium pertaining to electronic records, the person executing the search or seizure order may ask the subject of the order to operate the computer or provide "some other form of cooperation,"[1] which includes decryption of encrypted electronic records.[2] However, the subject is not penalized for refusing to provide such cooperation.[3]

A court may order the custodian of the electronic records or a person with authority to use the electronic records to record the necessary records onto the recording medium or print them out, and order the recording medium seized.[4] Commentators explain that the term "to record" includes "de-encrypt[ing] encrypted electronic records and record[ing]" the necessary electronic records onto the recording medium.[5] However, refusing to make such a recording is not penalized.[6]

Law enforcement officials may request telecommunications carriers to cooperate in implementing the interception of communications pursuant to a court order.[7] Telecommunications carriers that encrypt communications may be asked by law enforcement officials to decrypt the communications.[8] Carriers are obligated to cooperate with law enforcement officials but are not penalized for refusing to do so. Carriers are not required to develop systems or software to decrypt communications because doing so is beyond the scope of the Code's requirement for carriers to cooperate in implementing the interception of

---

[1] CODE OF CRIMINAL PROCEDURE, Act No. 131 of July 10, 1948, amended by Act No. 74 of 2011, arts. 111-2 & 222, English translation available on the Japanese Law Translation website, *at* http://www.japaneselawtranslation.go.jp/law/detail/?printID=&ft=2&re=02&dn=1&yo=criminal&ia=03&x=0&y=0&ky=&page=2&vm=02, *archived at* https://perma.cc/8PQ9-CFS2.

[2] 条解　刑事訴訟法(第 4 版) 追補 [ARTICLE-BY-ARTICLE COMMENTARY ON CRIMINAL PROCEDURE CODE (4TH ED.) SUPPLEMENT] 19 (Koya Matsuo et al. eds., 2009), http://www.koubundou.co.jp/files/35467_1.pdf, *archived at* https://perma.cc/GZJ5-5Z9P.

[3] *Id*.

[4] CODE OF CRIMINAL PROCEDURE art. 99-2 & art. 218, para. 1.

[5] SUPPLEMENT, *supra* note 2, at 12.

[6] *Id*.

[7] Act on Interception of Communications for Criminal Investigation, Act No. 137 of 1999, art. 11.

[8] KENZABURO YAZAWA & SHUNJI KATO, Q&A SOSHIKITEKI HANZAI TAISAKU SANPO 135 (2001), *bibliographic information at* https://lccn.loc.gov/2005442553.

communications.[9] Law enforcement officials are required to record all encrypted communications in an appropriate medium and attempt to decrypt it later.[10] Currently, the interception of communications is allowed for the investigation of four organized crimes: drug trafficking, gun running, mass smuggling of people, and murders by crime syndicates.[11] A proposal for an amendment to the law that would expand its application is pending before the Diet.[12]

When law enforcement officials obtain encrypted information through the interception of communications or seizures, they may request private firms to decrypt it.[13] However, such firms are not penalized for declining the request.[14]

[9] *Id*.

[10] *Id*. art. 13, para. 2.

[11] *Id*. art. 3.

[12] Bill to Amend Criminal Procedure Code and Others, Cabinet Bill No. 42 of 189th Diet Session (2015).

[13] CODE OF CRIMINAL PROCEDURE art. 197, para. 2.

[14] *Budget Committee 10th Meeting Minutes, House of Councillors*, 190th Diet 39 (Mar. 7, 2016) (statement of Mitsuhide Iwaki, Minister of Justice) http://kokkai.ndl.go.jp/SENTAKU/sangiin/190/0014/19003070014010.pdf, *archived at* https://perma.cc/F3TB-YYFJ.

South Africa

Hanibal Goitom
Foreign Law Specialist

SUMMARY South Africa permits law enforcement and security agencies to intercept various forms of communication. The applicable law requires telecommunications service providers to ensure that their systems can be intercepted and to store all communication-related information for between three and five years. While the agencies must first obtain an interception direction from the relevant court in order to intercept direct or indirect communications, no direction is required in cases of emergency. An agency petitioning for an interception direction may also seek a decryption direction the issuance of which would entitle it, depending on the terms of the direction, to demand that a decryption key holder disclose the decryption key or provide decryption assistance.

I. Introduction

Surveillance of domestic communications is primarily governed under the Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002 and its subsidiary legislation.[1] With the exception of a few provisions, the Act took effect in September 2005.[2] All of the provisions of the Act had been in effect as of June 2009.[3]

A 2014 report showed which of the country's law enforcement and security agencies obtained court authorizations to monitor communications and how often such authorizations were granted. According to the report, from 2008 through 2011, there was a 170% increase in the number of court authorizations (referred to as "interception directions" throughout this report—see Part III,

[1] Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002, 34 BUTTERWORTHS STATUTES OF THE REPUBLIC OF SOUTH AFRICA (updated through 2015), available on the Southern African Legal Information Institute (SAFLII) website, *at* http://www.saflii.org/za/legis/consol_act/roiocapocia2002925, *archived at* https://perma.cc/9TRT-PFEG; Department of Communications, sched. A, Directive for Fixed Line Operators in Terms of Section 30(7)(a) Read with Section 30(2) of the Regulation of Interception of Communication-Related Information Act, 2002 (Act No. 70 of 2002), Government Notice (GN) No. 1325/2005 (Nov. 28, 2005), http://www.gov.za/sites/www.gov.za/files/28271_0.pdf, *archived at* https://perma.cc/RXS3-ZBCX; Department of Justice and Constitutional Development, Notice in Terms of Section 31 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002): Mobile Cellular Operations, GN No. R93 (Feb. 6, 2009), http://www.gov.za/sites/www.gov.za/files/gg31844_nn93_pg10-15.pdf, *archived at* https://perma.cc/D4D5-TD5H; Department of Justice and Constitutional Development, Notice in Terms of Section 44(1)(a) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002), GN No. R1263 (Dec. 29, 2005), http://www.justice.gov.za/legislation/regulations/r2005/gg28371_r1263_interception-notice.pdf, *archived at* https://perma.cc/XD4V-GBLZ; Department of Justice and Constitutional Development, Notice in Terms of Section 31 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act 70 of 2002): Fixed Line Operations, GN No. R. 92 (Feb. 6, 2009), http://www.gov.za/sites/www.gov.za/files/31844_92.pdf, *archived at* https://perma.cc/888G-F92Y.

[2] Regulation of Interception of Communications and Provision of Communication-Related Information Act § 63.

[3] *Id*.

below) for interception of communications with 206 authorizations in 2008/09 and 418 authorizations in 2010/11.[4] The report indicated a substantial decline in authorizations in the following two years in which 261 authorizations were issued in 2011/12 and 144 in 2012/13.[5] Most of the authorizations were issued to the South African Police Service (SAPS) and the State Security Agency (SSA). For example, SAPS was issued 107 authorizations in 2008/09 and 436 authorization in 2010/11, while the SSA was issued 84 and 127 authorizations during the same time periods.[6] It is important to note that one authorization may represent large numbers of interceptions—for instance, the report indicated that the facility that intercepts communications was able to make over three million interceptions using only 882 authorizations over a three-year period.[7]

The above numbers do not account for interceptions conducted without prior court authorization. Over a nineteen-month period in 2010/11, 3,217 interceptions without court authorization are said to have been carried out by law enforcement and security agencies in South Africa.[8]

II. Interception Capability and Storage

The Communications and Provision of Communication-Related Information Act guarantees the ability of the relevant law enforcement and security agencies in the country to intercept communications by requiring that all telecommunications service providers "provide a telecommunication service which has the capability to be intercepted" and store communications-related information.[9] The provision of telecommunications services that do not have the capability to be intercepted is prohibited.[10] The required period of storage of communication-related information ranges from three to five years.[11] In addition, electronic

[4] RIGHT TO KNOW, STATE OF THE NATION REPORT: TRENDS, PATTERNS AND PROBLEMS IN SECRECY 6 (2014), http://www.r2k.org.za/wp-content/uploads/R2K-secrecy-report-2014.pdf, *archived at* https://perma.cc/CPK5-Z4Z8.

[5] *Id*.

[6] *Id*.

[7] *Id*. at 7.

[8] Jane Duncan, *Securocrats Serious About Cyberwarfare*, MAIL & GUARDIAN (Feb. 20, 2015), http://mg.co.za/article/2015-02-19-securocrats-serious-about-cyberwarfare, *archived at* https://perma.cc/3UUS-UH6F.

[9] Regulation of Interception of Communications and Provision of Communication-Related Information Act § 30. "Communication–related information" is

> any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system. *Id.* § 1.

[10] *Id*. Preamble; Nazreen Bawa, *The Regulation of Interception of Communications and Provisional Communication Related Information Act*, *in* TELECOMMUNICATIONS LAW IN SOUTH AFRICA 296, 300 & 307 (Lisa Thornton et al. eds., 2006), available on the University of Witwatersrand University website, *at* https://www.wits.ac.za/media/migration/files/TeleLawfull.pdf, *archived at* https://perma.cc/YE6L-GLH6.

[11] Regulation of Interception of Communications and Provision of Communication-Related Information Act § 30.

communications service providers[12] that provide mobile cellular electronic communications services must, at their own cost, "record and store" various information regarding their customers.[13]

III. Interception of Communications

The governing law allows law enforcement and security agencies to intercept[14] communications in certain circumstances with or without an interception direction.[15] The law provides that a law enforcement officer "who executes an interception direction or assists with the execution therefore, may intercept any communication . . . to which that interception direction relates," including direct[16] and indirect[17] communication.[18] An interception direction is a court-issued

[12] An "electronic communications service provider" is

> any –
>
> (a) person who provides an electronic communication service under and in accordance with a electronic communication service licence issued to such person under Chapter 3 of the Electronic Communications Act, and includes any person who provides –
>
> (i) a local access communication service, public pay-telephone service, value-added network service or private electronic communication network as defined in the Electronic Communications Act; or
>
> (ii) any other electronic communication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act; and
>
> (b) Internet service provider. *Id*. § 1.

[13] *Id*. § 40.

[14] The term "intercept" is defined as

> the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the –
>
> (a) monitoring of any such communication by means of a monitoring device;
>
> (b) viewing, examination or inspection of the contents of any indirect communication; and
>
> (c) diversion of any indirect communication from its intended destination to any other destination,
>
> and "interception" has a corresponding meaning. *Id.* § 1

[15] *Id*. ch. 2.

[16] This is an

> (a) oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or
>
> (b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication. *Id*. § 1.

[17] This is

> the transfer of information, including a message or any part of a message, whether –
>
> (a) in the form of –
>
> (i) speech, music or other sounds;
>
> (ii) data;
>
> (iii) text;
>
> (iv) visual images, whether animated or not;
>
> (v) signals; or
>
> (vi) radio frequency spectrum; or

authorization to intercept any communication "in the course of its occurrence or transmission."[19] In addition, a law enforcement officer may make an application before the relevant court for

- a real-time communications-related direction;
- an archived communications-related direction; or
- the simultaneous issuing of an interception direction, a real-time communications direction, and an archived communications-related direction, or of an interception direction supplemented by a real-time communications-related direction.[20]

There are instances in which law enforcement officers do not need an interception direction in order to intercept communications. These include instances where the interception is done to prevent impending serious bodily harm and for the purpose of determining location in the case of an emergency.[21]

IV. Decryption of Encrypted Information

A law enforcement officer seeking an interception direction from a court may also make an application for a "decryption direction."[22] With the issuance of a decryption direction, the decryption key holder is required, as per the specifications in the decryption direction, to disclose the decryption key or provide decryption assistance.[23] A decryption key is "any key, mathematical formula, code, password, algorithm or any other data which is used to . . . allow access to encrypted information . . . or . . . facilitate the putting of encrypted information into an intelligible form."[24] A decryption key holder is "any person who is in possession of a decryption key for the purpose of subsequent decryption of encrypted information relating to indirect communications."[25] A decryption direction may only be issued if the judge before whom the application is made is satisfied that

- the indirect information in question is partly or completely encrypted;
- the decryption key holder is in possession of the encrypted information and the decryption key;

(b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system. *Id.*

[18] *Id*. § 3.

[19] *Id*. § 1.

[20] *Id*. §§ 16, 17, 18 & 19.

[21] *Id*. §§ 7 & 8.

[22] *Id*. § 21.

[23] *Id.* §§ 1 & 29.

[24] *Id.* § 1. "Intelligible form" is defined as "the form in which the electronic data was before an encryption of similar process was applied to it." *Id*. § 1.

[25] *Id*.

- failure to issue a decryption direction would defeat the purpose for which the interception direction was issued; and
- it is not "reasonably practicable" for the applicant to acquire the encrypted information in question in "an intelligible form" without a decryption direction.[26]

V. Admissibility in Court

Any information regarding the commission of an offense obtained through interception or the provision of any real-time or archived communications-related information under South African or foreign law (with the authorization of the national director of public prosecutions) may be admissible in criminal or civil proceedings.[27]

[26] *Id.* § 21.

[27] *Id.* § 47.

Sweden

Elin Hofverberg
Foreign Law Research Consultant

SUMMARY Swedish law allows for the issuance of search warrants when a crime with a prison sentence is being investigated. Swedish law does not require encryption companies to decrypt cellphones. Legislation enabling forced decryption has previously been proposed but never adopted. All searches and seizures require a prior proportionality test, weighing the reasons for the measure against the privacy and integrity of the subject of the search. A recent Supreme Court case indicates that searches on devices may be limited because of this test. Legislative proposals are pending that would allow the Swedish police to infect suspects' computers with Trojan horse malware.

I. Background

Swedish police and prosecutors have previously requested authority to use new tools, such as the deployment of Trojan horse malware, to enable decryption of suspects' cellphones, according to news reports.[1]

A 2015 audit by the Swedish National Audit Office revealed that forensic experts at the Swedish (national) Police occasionally hack into cellphones.[2] Police access to cellphones has reportedly only rarely been hampered by encryption or similar preventive efforts.[3] The Swedish Security Police (SÄPO) reports that forensic analyses are part of all its investigations.[4] There are legal restrictions, however, not least in regard to international cloud services, which under Swedish law cannot be searched by Swedish police if the servers are outside of Sweden, as it would be considered a search in a foreign country.[5]

---

[1] *Säpo kräver trojaner*, VECKANSAFFÄRER (Apr. 25, 2014), http://www.va.se/nyheter/2014/04/25/sapo-kraver-trojaner, *archived at* https://perma.cc/2MM7-JBW4; *Prosecutors Want Access to Decryption Tools*, RADIO SWEDEN (Aug. 22, 2012), http://sverigesradio.se/sida/artikel.aspx?programid=2054&artikel=5246277, *archived at* https://perma.cc/N33Z-ZTD2.

[2] RIKSREVISIONEN IT-RELATERAD BROTTLISGHET – POLIS OCH ÅKLAGARE KAN BLI EFFEKTIVARE 18, RIR 2015:21, http://www.riksrevisionen.se/PageFiles/23153/RiR_2015_21_IT-relaterade-brott_Anpassad.pdf, *archived at* https://perma.cc/P5AV-MVR4.

[3] *Id*. at 47.

[4] *IT är med i alla våra brottsutredningar*, SÄKERHETSPOLISEN, http://www.sakerhetspolisen.se/ovrigt/menyer/medarbetarportratt/it-ar-med-i-alla-vara-brottsutredningar-.html (last visited Apr. 12, 2016), *archived at* https://perma.cc/VB83-ZGJL.

[5] Departementsserie [Ds.] 2005:6 Brottsutredning i it-miljö [Crime Investigation in the IT Environment], at 131, http://www.regeringen.se/contentassets/3f7139539cd3460b9ee6c3d343923213/brott-och-brottsutredning-i-it-miljo.-europaradets-konvention-om-it-relaterad-brottslighet-med-tillaggsprotokoll, *archived at* https://perma.cc/7NDN-44K7.

Following the Paris terrorist attacks in November 2015 the Swedish government declared that it would initiate, research, and propose new legislation to enable access to encrypted information.[6] The proposal is forthcoming—no initial committee report has yet been published.[7]

II. Current Law

A. Decryption Pursuant to Warrants

Swedish law provides limited possibilities for decryption pursuant to a warrant. The Swedish Constitution provides protection against unlawful searches of persons and property.[8] Search warrants can only be made under law.[9] The issuance of search warrants is regulated in Rättegångsbalken (the Civil and Criminal Procedure Act).[10] A search warrant can be issued if the crime investigated is sanctioned with a prison sentence.[11] However, in each case the person issuing the search warrant must conduct a proportionality test (*proportionalitetsprövning*), weighing the invasion of the suspect's privacy versus the benefits of issuing the warrant.[12] A police officer may conduct a search without first securing a search warrant if there is an immediate danger in not conducting the search.[13] Subject to a proportionality evaluation, a search warrant may also be issued for a place not directly connected with the crime or suspect if there are extraordinary reasons to suspect that useful information will be found.[14]

The Swedish Supreme Court has found that searches of computers and cellphones are an especially sensitive area of the law, as computers and cellphones "may . . . include evaluation of a significant number of files and large amounts of data that is not sought [by the Police]."[15] This means that the proportionality test is especially important in these cases.[16] Depending on the

---

[6] *Fler insatser för att motverka terrorism*, REGERINGEN (Nov. 19, 2015), http://www.regeringen.se/artiklar/2015/11/fler-insatser-for-att-motverka-terrorism, *archived at* https://perma.cc/6HN4-JR6E.

[7] For an overview of the process for adopting legislation, see *Commissions of Inquiry*, SVERIGESRIKSDAG, https://www.riksdagen.se/en/How-the-Riksdag-works/What-does-the-Riksdag-do/Legislation/Commissions-of-inquiry (click headings under "Commissions of inquiry" in the list of topics on the left) (last visited Apr. 11, 2016), *archived at* https://perma.cc/664Z-29FF.

[8] 2 ch. 6 § REGERINGSFORMEN [RF] (Svensk författningssamling [SFS] 1974:152), https://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Kungorelse-1974152-om-beslu_sfs-1974-152/#K2, *archived at* https://perma.cc/KBQ2-D8BY.

[9] *Id.* 2 ch. 6 & 20 §§.

[10] RÄTTEGÅNGSBALKEN [RB] [CODE OF CIVIL AND CRIMINAL PROCEDURE] (SFS 1942:740), https://www.notisum.se/rnp/sls/lag/19420740.htm, *archived at* https://perma.cc/ULE7-Y8JQ.

[11] *Id*. 28 ch. 1 §.

[12] *Id*. 28 ch. 3a §.

[13] *Id*. 28 ch. 5 §.

[14] *Id*. 28 ch. 1 § 2 st.

[15] Högsta Domstolen [HD] [Supreme Court], 2015-08-18, Ö 3074-15, at 6, http://www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2015/2015-08-18%20O%203074-15%20Beslut.pdf, *archived at* https://perma.cc/A5AA-8JBT (all translations by author).

[16] *Id*. 17, 28–29 ¶¶.

outcome of a proportionality test, seizure of a cellphone may thus be possible under Swedish law, but decryption might be illegal.

B. Seizure of Encrypted Information

Property that can reasonably be presumed to have importance in an investigation can be seized,[17] except for excluded property such as secret information pertaining to information that a person could not divulge in court.[18] Parliamentary committees have interpreted this exclusion to also include electronic property.[19] The Supreme Court in 2015 affirmed that conclusion.[20] If a document (or electronic media) is protected by a prohibition against seizure (*beslagsförbud)*, this is absolute and cannot be overridden by the proportionality test.[21] The reason behind this absolute prohibition is that the police and prosecutor must not be able to circumvent the rules limiting what can be asked of a witness—for example, limitations based on the attorney-client privilege or doctor-patient confidentiality under Swedish secrecy law.[22]

The Supreme Court has previously refused requests for the production of certain data because the data was held by persons who were subject to legally mandated, professional secrecy.[23] Where secret information is present on a device such as a cellphone, that fact alone does not bar a search for information on the device, but does weigh negatively against the search in a proportionality test.[24]

C. Information Owner's Obligation to Decrypt

Sweden is a signatory to the Council of Europe Directive on Cybercrime.[25] In a 2013 government report the Cyber Convention Commission, while evaluating the need for new legislation to enable implementation of the Cybercrime Directive, found that there currently is a possibility under Swedish law to "order a person with knowledge of a computer systems' function or of measures that are used to protect the [desired] information, to provide information

---

[17] 27 ch. 1 § RB.

[18] *Id*. 27 ch. 2 §.

[19] *See, e.g.*, Statens Offentliga Utredningar [SOU] 2011:45 Förundersökning – objektivitet, beslag, dokumentation m.m. [government report], http://data.riksdagen.se/fil/40CFC0F1-4704-4C11-9CA1-D03634483049, *archived at* https://perma.cc/NHV9-68VT.

[20] HD Ö 3074-15, 14 ¶.

[21] *Id*. 20 ¶.

[22] *Id*. 23 ¶.

[23] *Id*. 24 ¶; *see* Nytt Juridiskt Arkiv [NJA] 1981 s. 791 & NJA 1992 s. 307.

[24] HD Ö 3074-15, 29 ¶.

[25] Convention on Cybercrime, Nov. 23, 2001, 185 E.T.S., http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, *archived at* https://perma.cc/AZE4-YJ5M; *Chart of Signatures and Ratifications of Treaty 185, Convention on Cybercrime, Status as of 18/04/2016, Full List*, COUNCIL OF EUROPE, TREATY OFFICE, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=GfgVFijr,l, *archived at* https://perma.cc/R335-RSB7.

that is necessary to enable the execution of the warrant."[26] The Cyber Convention Commission thus concluded that there was no need to change Swedish legislation to adopt the Council of Europe Directive on Cybercrime.[27] It is unclear whether the Commission's interpretation would apply to the creators of encryption software or only to the person who stored the information.

The Swedish Data Protection Authority criticized the Commission's interpretation that a person subject to a warrant can be required to provide keys to his or her computer.[28] The statement could be interpreted by the courts as a requirement to self-incriminate—for example, when an individual is required to present his or her password—and as such could be a violation of human rights as interpreted by the European Court of Human Rights (ECHR).[29]

Another police measure that could potentially be invoked to force access to encryption keys is "testimony before the courts during police investigations" (*vittnesförhör inför rätta under en förundersökning*).[30] Persons who are thought to have information of importance to an investigation may, under the threat of a fine (*vite*), be asked to report to the investigator (generally the police) to divulge their information before the court.[31] This could be interpreted to include requests that third parties aware of a password divulge that information.[32]

D. Obligation of Encryption Companies to Decrypt Data

Swedish law does not require encryption companies to decrypt data. However, members of Parliament have previously made such proposals. For instance, Motion 2013/14:JU277 proposed that encryption companies be required to decrypt files in child-pornography cases, but that proposal was rejected by the Justice Committee, which cited other efforts by the government to address child pornography.[33]

---

[26] SOU 2013:39 Europarådets konvention om it-relaterad brottslighet [government report series], at 146, http://www.regeringen.se/contentassets/b7ef66bff0b94040b781df446546c745/europaradets-konvention-om-it-relaterad-brottslighet-sou-201339, *archived at* https://perma.cc/HN8M-K877.

[27] *Id*. at 150.

[28] *See* DATAINSPEKTIONEN, REMISSSVAR AV BETÄNKANDET EUROPARÅDETS KONVENTION OM IT-RELATEDARD BROTTSLIGHET [CONSULTATION RESPONSE TO THE GOVERNMENT REPORT ON THE EUROPEAN COUNCIL'S CONVENTION ON CYBERCRIME] (SOU 2013:39) 2–3(Sept. 19, 2013), http://www.datainspektionen.se/Documents/remissvar/2013-09-25-konvention-it-brottslighet.pdf, *archived at* https://perma.cc/4V8A-UJKG.

[29] SOU 2013:39, *supra* note 26, at 283; *see also* Johan Holmgren, Kryptering, dekryptering och de mänskliga rättigheterna 20–22 (unpublished thesis, Law Faculty, Lund University), *available at* https://lup.lub.lu.se/student-papers/search/publication/3046392 (last visited Apr. 19, 2016), *archived at* https://perma.cc/ZK9S-MHNN.

[30] SOU 2013:39, *supra* note 26, at 146.

[31] 23 ch. 13 § RB; *see also id.* 23 ch. 6, 6a, 6b §§.

[32] SOU 2013:39, *supra* note 26, at 334.

[33] Justitieutskottet betänkande 2013/14:JuU14 Polisfrågor [Justice Committee Report 2013/14:JuU14, Police Issues], https://www.riksdagen.se/sv/Dokument-Lagar/Utskottens-dokument/Betankanden/Polisfragor_H101JuU14/?html=true, *archived at* https://perma.cc/39D3-WEBY.

E. No Decryption Requirement for Internet Service Providers

Internet Server Providers (ISPs) are required to collect and store metadata on all of its customers for six months.[34] However, ISPs cannot be required to decrypt any information sent over their networks. The extent of the data collected as well as the willingness to produce such data varies among Swedish ISPs.[35]

F. Secret Surveillance

Secret surveillance is regulated in chapter 27 of the Civil and Criminal Procedure Act.[36] The police are allowed to secretly surveil electronic communications for crimes that carry a sentence of at least two years' imprisonment.[37] However, the police may only use secret surveillance if it is of exceptional importance to the investigation and the target is suspected, on reasonable grounds, of having committed the crime.[38] The police are not allowed to surveil electronic communications over communications networks that are of lesser importance from a public communications perspective.[39]

III. Court's Call for Legislative Action

In a 2015 decision denying access to digital images in a robbery case, the Swedish Supreme Court issued a rare statement[40] explaining that it was restricted by the fact that Swedish "legislation regarding the use of coercive measures in the so-called virtual space is outdated."[41] The Court continued, "[i]t is urgent that the legislative branch [Swedish Parliament] correct this [as the Court cannot do this, not least] as good legal custom presumes a significant level of technical or other non-legal expertise."[42]

The case hinged on the fact that the images were protected by a constitutional right of freedom to communicate information (*meddelarfrihet*) and that seizing the images could have exposed the

---

[34] 6a, 16d §§ LAG OM ELEKTRONISK KOMMUNIKATION [LEK] [ACT ON ELECTRONIC COMMUNICATION] (SFS 2003:389), http://www.notisum.se/rnp/sls/lag/20030389.HTM, *archived at* https://perma.cc/3YFS-C9YN.

[35] For example, the ISP Banhof has taken a more restrictive stance on when to provide data to the government. *Advokaten: Det måste finnas gränser för vad polisen ska kunna få tillgång till*, BAHNHOF (Apr. 8, 2016), https://www.bahnhof.se/press/press-releases/2016/04/08/advokaten-det-maste-finnas-granser-for-vad-polisen-ska-kunna-fa-tillgang-till, *archived at* https://perma.cc/PY9X-EWQQ.

[36] 27 ch. RB.

[37] *Id.* 27 ch. 18 § 2 st.

[38] *Id.* 27 ch. 20 § 1 st.

[39] *Id.* 27 ch. 20 § 3 st.

[40] Press Release, HD, Högsta domstolen avslår åklagarens begäran om husrannsakan hos Aftonbladet (Aug. 18, 2015), http://www.hogstadomstolen.se/Mer-om-Hogsta-domstolen/Nyheter-fran-Hogsta-domstolen/Hogsta-domstolen-avslar-aklagarens-begaran-om-husrannsakan-hos-Aftonbladet, *archived at* https://perma.cc/W4KA-CL4S.

[41] HD Ö 3074-15, 43 ¶.

[42] *Id.*

photographer, which was not outweighed by the police's need for the picture. Swedish journalists are not allowed to reveal confidential sources, as specified in the Swedish Constitution,[43] and a proportionality test is always required by law.[44]

IV. Conclusion

In practice it is unlikely that a Swedish court would force an ISP, encryption company, or other entity to decrypt data pursuant to current law, as the measure would not be considered proportional. The matter will likely be addressed by the legislature.

[43] *See* 1 ch. 1 § 3 st TRYCKFRIHETSFÖRORDNINGEN [TF] [FREEDOM OF THE PRESS ACT] (Constitution).

[44] 27 ch. 1 § 3 st RB.

Taiwan

Laney Zhang
Senior Foreign Law Specialist

SUMMARY Under Taiwanese law, an interception warrant generally needs to be sought by a prosecutor upon request by the judicial police authorities and issued by a court before interception can commence. The intelligence agency, however, does not appear to need a warrant from the court when intercepting the communications of foreign governments or cross-border terrorist organizations for national security purposes.

Although the law does not specifically address government access to encrypted communications, it generally requires telecommunications companies to equip their hardware and software "with functions that can cooperate with interception" and to provide "interfacing devices" in assisting government surveillance of communications.

I. Surveillance of Communications

In Taiwan, government surveillance of communications and the legal requirements of telecommunications companies in assisting such surveillance are regulated by the 1999 Communications Protection and Surveillance Act, as amended in January 2014 (Surveillance Act).[1]

"Communications" under the Surveillance Act include telecommunications, emails, letters, speeches not made though telecommunications, and face-to-face conversations.[2] The term "telecommunications" refers to "utilizing wired or wireless telecommunications equipment to send, store, transmit, or receive information."[3]

A. Interception Warrant Issued by Court

In general, an interception warrant is sought by the prosecutor upon request by the judicial police authorities and issued by a court. Such an interception must be for the purpose of investigating the specific crimes set forth by the Surveillance Act, which include all crimes punishable by a minimum of a three-year, fixed-term imprisonment. There must be sufficient evidence that the accused or the suspect is involved in such a crime and that national security or the economic or

[1] 通訊保障及監察法 [Communication Protection and Surveillance Act] (Surveillance Act) (promulgated July 14, 1999, amended Jan. 29, 2014), art. 5, LAWS AND REGULATIONS DATABASE OF THE REPUBLIC OF CHINA, http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=K0060044, *archived at* https://perma.cc/LRH5-4PXZ, English translation *available at* http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=K0060044, *archived at* https://perma.cc/3C86-73PW.

[2] Surveillance Act art. 3; 通訊保障及監察法施行細則 [Implementation Measures of the Communication Protection and Surveillance Act] (Implementation Measures) (Mar. 15, 2000, amended June 26, 2014), art. 2, http://law.moj.gov.tw/LawClass/LawAll_print.aspx?PCode=K0060053, *archived at* https://perma.cc/JJ6M-45V9.

[3] Surveillance Act art. 3.

social order are severely endangered. In addition, there must be a reasonable belief that the content of the communications subject to surveillance is relevant to the case being investigated, and that it is difficult or impossible to collect or investigate the evidence by other means.[4]

Under urgent situations in investigating certain offenses, however, the prosecutor may "verbally inform" the enforcement authority to start intercepting communications and apply for the interception warrant from the court within twenty-four hours afterward. The court must issue the warrant within forty-eight hours, or otherwise the interception must be ended.[5]

B. Interception Warrant Issued by Head of Intelligence Agency

In intercepting the communications of foreign governments and cross-border terrorist organizations for national security purposes, the intelligence agency does not appear to need an interception warrant from the court. Under such circumstances, the head of the national intelligence agency, the National Security Bureau, is able to issue the interception warrant.[6]

II. Obligations of Telecommunications Companies

The Surveillance Act does not specifically address encrypted communications. The Act generally requires telecommunications companies to provide facilities and personnel as needed to assist government surveillance of communications.[7] Such obligations to assist specifically include equipping their hardware and software "with functions that can cooperate with interception" and providing "spaces, electricity, and relevant interfacing devices," pursuant to the implementation measures of the Surveillance Act.[8]

Moreover, telecommunications operators are required by the Surveillance Act to assist law enforcement agencies in setting up and maintaining systems used for surveillance purposes. The obligation is limited to what is "technologically and economically reasonable" at the time of setting up the system and "should not exceed expected possibilities."[9]

A failure to fulfill the obligations of assisting surveillance is punishable by a fine of 500,000–2,500,000 New Taiwan Dollars (about US$15,500–$77,000), an additional accumulative daily fine, and revocation of licenses.[10]

[4] *Id*. art. 5.

[5] *Id*. art. 6.

[6] *Id*. arts. 7 & 8; Implementation Measures art. 9.

[7] Surveillance Act art. 14.

[8] Implementation Measures art. 26.

[9] Surveillance Act art. 14.

[10] *Id*. art. 31.

III. Conclusion

Although the Taiwanese Surveillance Act does not specifically address government access to encrypted communications, the legal obligations of telecommunications companies in assisting government surveillance may include enabling the decryption of encrypted communications.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

I. Decryption at the Request of the Intelligence Services and Law Enforcement

The United Kingdom (UK) has had legislation in place since the early 2000s that enables specified high-ranking law enforcement and intelligence officials to serve a written notice on individuals and bodies that requires them to disclose lawfully held encrypted information in an intelligible form.[1] This notice provides a means for what is described as "enforced decryption."[2]

To obtain a notice, the desired disclosure of information must be proportionate to what the requester is seeking to achieve and necessary in the interests of national security, for the purposes of preventing or detecting crime, or in the interests of the economic well-being of the UK. In addition, acquiring the information in an intelligible form without a notice must not be reasonably practicable.[3]

The notice must be in writing, describe the protected information to which it relates, specify the position of the person giving the notice, specify the position of the person who granted permission for the notice, and establish a time limit for compliance with the notice. The notice must also describe the disclosure that is required and the way that the disclosure should be made.[4] The penalty for failing to comply with a disclosure notice is up to two years' imprisonment for regular cases or five years' imprisonment in national security cases, upon conviction.[5] This term of imprisonment has been criticized as being insufficient on the grounds that, if an individual's device contains encrypted information that could be used as evidence to convict him or her of a serious criminal offense, refusing to provide the encryption key in response to a notice carries a lesser sentence than the individual might otherwise receive.[6]

Redacted information in a report by the Intelligence and Security Committee of Parliament indicates that Government Communications Headquarters (GCHQ) has a program of work dedicated to unlocking encrypted communications, which requires no ministerial authorization.[7]

---

[1] Regulation of Investigatory Powers Act 2000, c. 23, § 49 & sched. 2, http://www.legislation.gov.uk/ukpga/2000/23, *archived at* https://perma.cc/B53E-4RJ7.

[2] DAVID ANDERSON Q.C., A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW ¶ 8.30 (June 2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf, *archived at* https://perma.cc/N4UN-UE7F.

[3] Regulation of Investigatory Powers Act 2000, c. 23, § 49.

[4] *Id.*

[5] *Id.* § 53.

[6] ANDERSON, *supra* note 2, ¶ 8.31.

[7] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK, 2014–15, H.C. 1075, ¶¶ 179–180, http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf, *archived at* https://perma.cc/6NDK-FCKH.

The program is provided for under the general power given to the GCHQ under section 3(1)(a) of the Intelligence Services Act, which states that the GCHQ may "monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and … obtain and provide information derived from or related to such emissions or equipment and from encrypted material."[8]

The Intelligence Services and Police may interfere with equipment (also known as "computer network exploitation") to obtain communications, equipment data, and other information from equipment. The use of computer network exploitation varies from using someone's login information to remotely and covertly installing software on a device.[9] The security and intelligence agencies may apply to the Secretary of State to obtain a warrant to use equipment interference if it is necessary in the interests of national security or the economic well-being of the UK, or to prevent and detect serious crime.[10]

II. Pending Investigatory Powers Bill

A draft Investigatory Powers Bill was published in the autumn of 2015 and consolidates and expands provisions relating to law enforcement's access to encrypted information.[11]

A. Equipment Interference

The Bill would introduce specific procedures for law enforcement and intelligence services to undertake equipment interference to access individuals' devices and computers to obtain data, such as communications via texts and email, and geolocation. Equipment interference could also be used to obtain otherwise encrypted data.[12] Clauses 88–90 of the Bill would provide law enforcement with the ability to apply for warrants for two equipment interference purposes:

- Targeted equipment interference. This would authorize law enforcement to interfere with equipment to obtain communications, private information, or equipment data, as well as to disclose, monitor, and examine this material.
- Targeted examination warrants. This would authorize the individual named in the warrant to examine material obtained under a bulk equipment interference warrant. Bulk equipment interference warrants are provided for in clauses 119–137 of the Bill and would apply only to individuals outside the UK.

[8] Intelligence Services Act 1994, c. 13, § 3(1)(a), http://www.legislation.gov.uk/ukpga/1994/13, *archived at* https://perma.cc/FK2X-9ARJ.

[9] *Id.* §§ 5 & 7; Police Act 1997, c. 50, § 93, http://www.legislation.gov.uk/ukpga/1997/50, *archived at* https://perma.cc/ 2QW2-LZTX.

[10] Intelligence Services Act 1994, § 3(2).

[11] Draft Investigatory Powers Bill 2015, 2015–16 Cm. 9152, *available at* https://www.gov.uk/government/publications/draft-investigatory-powers-bill, *archived at* https://perma.cc/9P94-FTYA.

[12] HOUSE OF COMMONS LIBRARY, INVESTIGATORY POWERS BILL, Mar. 11, 2016, Briefing Paper No. 7518, http://researchbriefings.files.parliament.uk/documents/CBP-7518/CBP-7518.pdf, *archived at* https://perma.cc/LP5A-964S.

Clauses 84–91 would authorize a senior law enforcement officer, with approval from a Judicial Commissioner, or the Secretary of State upon application from the intelligence services, to issue a warrant for equipment interference. Clause 84 provides that, for the intelligence services to obtain a warrant for equipment interference from the Secretary of State, the applicant would need to show that it is necessary

- on the grounds of national security,
- to prevent or detect serious crime, or
- that it is in the interests of the economic well-being of the UK, and
- that the warrant is proportionate.

Clause 89 of the Bill would authorize senior law enforcement officers to apply for a warrant to authorize equipment interference if necessary

- for the purposes of preventing and detecting serious crime; or
- to prevent death, injury, or damage to a person's physical or mental health; and
- that is a proportionate response.

The Bill would allow warrants to be granted to intercept equipment in cases where the targeted equipment interference is to obtain information subject to a legal privilege. There must be exceptional and compelling circumstances to justify the interception of such materials, however, and additional handling arrangements must be in place.[13] An individual who has a warrant would be able to serve a copy of it on anyone who may be able to assist him/her, including individuals outside the UK.[14] Clause 111 would "[place] a duty on telecommunications providers to assist with the implementation of equipment interference warrants."[15]

Because of the sensitive nature of such warrants, the Bill would create a duty not to make unauthorized disclosures about the existence or details of both the warrant and any materials obtained under it, and clause 116 sets out a specific offense of the unauthorized disclosure of such information.

B. Notices Requiring Communication Service Providers to Facilitate Assistance

Clause 214 of the Bill would authorize the Secretary of State to introduce measures to facilitate compliance with the Bill in areas that include decryption of communications. Clause 217 would enable the Secretary of State to impose obligations on communication service providers through regulations, in the form of technical capability notices to facilitate assistance to warrants issued under specified parts of the Investigatory Powers Bill. Clause 213 provides that communication service providers would receive a contribution towards any costs they incurred to comply with

[13] Draft Investigatory Powers Bill 2015, cl. 100.

[14] *Id.* cls. 109–110.

[15] HOUSE OF COMMONS LIBRARY, *supra* note 12, at 43.

the measure. Clause 189 provides that such obligations would include the removal of electronic protection applied by an operator, or any third party acting on their behalf, to any data or communications. When making these notices, the Secretary of State would be required to take into account the technical feasibility and cost of compliance.

C. Opposition to the Bill

These provisions have met considerable resistance both within the government and in private industry, who are concerned not only with the ability to access the communications that it appears the Bill requires, but also at the negative impact it could have on the UK's technology industry. Recommendations from the committee reviewing the Bill notes that the government should make it explicit that, if the Bill is adopted, providers of "end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide copies of those communications if it not practicable for them to do so."[16] Concerns have been raised that the language used in this clause would result in the prohibition of end-to-end encryption in the UK, and review committees are urging the government to clarify the nature of the obligations that would be required under the Bill. The government has responded that a Code of Practice will contain further details as to the necessity and proportionality of imposing these requirements on communication service providers.[17]

The Bill is currently in draft form, which means it will be reviewed and subject to consultations before being formally introduced in the House of Commons. As the Bill contains some controversial provisions, it is uncertain when it will be formally introduced, or if introduced whether it will be enacted.

[16] *Id.* at 71.

[17] *Id.* at 42.