



*The Law Library of Congress*

# REPORT FOR CONGRESS

December 2010

---

Global Legal Research Center  
LL File No. 2011-005074

## PRIVACY OF ELECTRONIC COMMUNICATIONS

*This report discusses the laws governing the privacy of electronic communications in Australia, Canada, China, France, Israel, Russia, and the United Kingdom.*

---

The Library of Congress  
James Madison Memorial Building, 101 Independence Avenue, S.E., Room LM-240  
Washington, DC 20540-3200  
(202) 707-6462 (phone), (866) 550-0442 (fax), [law@loc.gov](mailto:law@loc.gov) (email)  
<http://www.loc.gov/law>

**LAW LIBRARY OF CONGRESS**

**PRIVACY OF ELECTRONIC COMMUNICATIONS  
IN SELECTED FOREIGN COUNTRIES**

*Executive Summary*

*A survey of the laws of Australia, Canada, China, France, Israel, Russia, and the United Kingdom shows that all of the countries make provision for the privacy of electronic communications through constitutional or other legal protections, and all provide exceptions to allow law enforcement and security agencies to access and use such information. The majority of the countries require external authorization for the interception of electronic communications, and some place obligations on service providers to provide assistance and the technical capability needed to execute warrants or authorizations. In most countries, warrants or authorizations are only permitted for limited circumstances involving serious offenses and national interests, and there are rules relating to the use or disclosure of the information obtained, including its admissibility in court proceedings. In China and Russia, there are fewer restrictions on the ability of authorities to monitor Internet content and traffic for law enforcement and security purposes.*

The attached reports survey the laws of seven countries relating to the protection of the privacy of electronic communications. They set out the exceptions that apply and the rules that must be followed in order for there to be legal interception, access, surveillance, or use of communications, particularly by law enforcement and national security agencies.

The seven countries surveyed are Australia, Canada, China, France, Israel, Russia, and the United Kingdom. Due to privacy concerns, including constitutional rights to privacy or other legal protections of privacy, the laws of each of these countries contain general prohibitions that restrict the ability for electronic communications to be intercepted, accessed, or disclosed except in limited circumstances. Each country makes specific provision for electronic communications to be obtained by government agencies for law enforcement and national security purposes, although differing levels of restrictions and requirements apply in terms of the issuance of authorizations. Detailed rules relating to the justifications needed for warrants to be issued, conditions on their execution, and restrictions on the use of any information obtained, are found in the laws of Australia, Canada, France, Israel, and the United Kingdom. Russia and China have fewer restrictions, and warrants are either not needed or authorizations are subject only to internal procedural rules.

Australia, France, Israel, and the United Kingdom make specific provision for interception warrants or authorizations to be issued to security or intelligence agencies by a member of the executive branch (such as the Prime Minister or Attorney-General) where interception is necessary for the purposes of national security or other national interests.

In the United Kingdom, the Secretary of State issues warrants for both national security and law enforcement purposes, although in urgent circumstances a warrant may be issued by a senior official.

Australia, Canada, France, and Israel provide for interception to be authorized by a judge or similar judicial officer for law enforcement purposes. Australian law also includes specific rules relating to warrants for accessing communications stored by service providers. The general approach in all of these countries is that warrants can only be issued for the prevention, detection, or investigation of serious crimes.

A number of requirements must be met in terms of the contents of applications and the elements of warrants or authorizations, and these requirements may be different depending on the type of warrant involved. The maximum period of time for which interception may be authorized differs in each country, and provision is often made for warrants to be renewed or extended. There are also reporting and oversight mechanisms that relevant agencies must comply with in connection with the different types of warrants.

In China, public security and law enforcement agencies are allowed to inspect the content of telecommunications for the purposes of state security or investigating criminal offenses. There are no strict rules requiring the agencies to prove the involvement of state security issues, and criminal investigations are not limited by the type of crime involved. Approval procedures relating to the interception of communications have not been found in the laws and are likely to be contained in the internal documents of the agencies concerned. Approval to seize emails can be obtained from a police officer in charge of a public security organ at the county level or above.

In Russia, the Criminal Procedure Code requires that the monitoring of information transferred via or stored in electronic resources for the purposes of investigating illegal acts or acts that threaten national security must be conducted according to a court permit. However, the Federal Security Service has been authorized to install special equipment to enable remote access to and monitoring of communications transmitted via the Internet. The system allows secret police to monitor all Internet traffic, credit card transactions, and email exchanges in real time and without applying for a warrant. There are no requirements to inform individual users of such monitoring.

There is some provision in other countries for interceptions or access to information to be permitted in limited circumstances without external authorization. Following are some examples:

- In Australia, the Director-General of Security can issue a warrant under his or her own hand in urgent situations where a request has been made to the Attorney-General but a warrant has not yet been issued.
- In Canada, interception without judicial authorization is allowed in exceptional circumstances where a peace officer believes that the urgency of the situation is such that authorization could not be obtained in time to prevent an unlawful act that would cause serious harm to any person or property.

- In France, a 2006 law relating to the fight against terrorism empowers police officers to require the disclosure of certain data from service providers without any authorization from the Public Prosecutor.
- In Israel, prosecutors or chief investigators may review or use information derived from unauthorized secret monitoring as long as this is done for the purpose of preventing or investigating serious crimes or any crimes involving special reasons, or based on the public interest.

The use of data surveillance devices by agencies to record or monitor the input of information into a computer is specifically permitted by law in Australia, with agencies able to obtain warrants for limited purposes. A draft law in France that is currently before the National Assembly would also provide for similar data surveillance activities to be conducted by police for the purposes of fighting organized crime.

Interceptions of electronic communications by entities other than law enforcement and security agencies are expressly permitted in limited circumstances in Australia, Canada, France, Israel, and the United Kingdom. This is likely to include interception where there has been consent from the sender and recipient of the communication, and circumstances associated with the operation of the telecommunications service or network by the service provider.

Communications that may be subject to the rules relating to interception, access, and use appear to be broadly defined in the legislation of Australia, Canada, China, France, Israel, and the United Kingdom. Russia does not define the relevant terms in detail in this particular context.

Many of the countries place obligations on service providers in relation to the protection of data, maintenance of interception capabilities, and provision of assistance to law enforcement or security agencies. Following are some examples:

- In Australia, service providers must ensure that it is possible to execute a warrant for the interception of electronic communications. The relevant Minister may make a determination regarding the interception capabilities required of different types of telecommunications service, which must then be developed, installed, and maintained. Service providers must also have “interception capability plans” that comply with the requirements in the legislation.
- In China, service providers are required to assist the government in monitoring Internet communications. This includes recording the time emails were sent, as well as the email and IP addresses of senders and receivers, maintaining such records for sixty days, and providing the record to the relevant State agency on request.
- In the United Kingdom, service providers must comply with a notice that requires them to undertake steps necessary for having the practical capability to provide assistance in relation to interception warrants.

- In France, service providers, as well as Internet cafes, hotels, restaurants, and other organizations providing Internet access, may be required by police officers to keep certain telecommunications data for a year where it is needed for investigations.
- In France and the United Kingdom, entities may be required to give agencies the keys that allow for encrypted data to be deciphered.
- In Russia, federal legislation must set out the procedures under which service providers will provide information to law enforcement authorities, maintain the confidentiality of ongoing investigative activities, and install equipment at the request of law enforcement authorities for the purposes of conducting investigations and monitoring national security issues.

There have been several unsuccessful attempts in Canada to enact legislation that would require service providers to preserve and produce data pursuant to an order, maintain certain capabilities to facilitate the lawful interception of communications, and introduce enhanced investigative powers for police. Two new bills were introduced in the House of Commons in October 2010 and are currently going through the legislative process.

Unauthorized or unlawful interception of electronic communications is an offense in all of the countries surveyed. In Australia and the United Kingdom, the penalty is two years' imprisonment. In France, the penalties are three years' imprisonment and a fine of €45,000. In Israel and Canada, violation of the prohibition is punishable by five years' imprisonment. In Russia, the recommended penalties for unauthorized access to computer information include fines, correctional labor, detention, a ban on certain types of professional activities, and up to five years' imprisonment. Unlawful interception of personal emails and other electronic data has been criminalized in China by a decision issued by the Standing Committee of the National People's Congress.

There are also prohibitions and offenses relating to the unlawful use or disclosure of electronic communications in many of the countries. Specific exceptions may exist to enable information to be used in court proceedings. The admissibility of such evidence is governed by the different criminal procedure rules of each jurisdiction and any provisions of the relevant statutes. In cases where it is claimed that electronic communications have been obtained in breach of the rules relating to warrants or other authorizations, different approaches are taken, as follows:

- In Australia, the question of whether or not there has been a breach is determined on the balance of probabilities. Evidence may be admitted where a defect or irregularity in the warrant is not substantial and the court is satisfied that, but for the irregularity, the interception or access would not have constituted a breach of the prohibitions.
- In France, serious breaches of the rules governing the gathering of evidence may render the operation null and void. The court must look at whether the rule is sufficiently important to justify nullity for its breach and whether the breach has harmed the interest of the party challenging its breach.

- In Israel, information obtained through unauthorized secret monitoring may be admissible if, in a proceeding for a serious crime, the court orders that it is admissible after having been convinced, for special reasons that must be cited, that in the circumstances the need to reach the truth is greater than the need to protect privacy.
- In Russia, while there is a requirement for information on a person's Internet activities to be obtained by legal means, it appears that the courts accept evidence received by law enforcement and state security in accordance with existing executive regulations.
- In the United Kingdom, no evidence can be adduced, questions asked, or disclosure made in any legal proceedings of an authorized interception of a communication and the product of that interception. The Court of Appeal has stated that there would have to be highly unusual and material circumstances for a court to depart from this prohibition.

Prepared by Kelly Buchanan  
Foreign Law Specialist  
December 2010

**LAW LIBRARY OF CONGRESS**

**AUSTRALIA**

**PRIVACY OF ELECTRONIC COMMUNICATIONS**

*Executive Summary*

*The interception of electronic communications and access to stored communications is generally prohibited under Australian law. A range of exceptions apply, including for law enforcement, security, and intelligence gathering purposes, with detailed rules established for obtaining warrants. Carriers are required to provide assistance and to ensure that interception capability has been installed in relation to the network or system. There are also restrictions and exceptions relating to the disclosure of intercepted or stored information. Separate legislation applies to the use of surveillance devices, including the ability to obtain warrants for the use of data surveillance devices.*

**I. Introduction**

The Australian Privacy Act 1988 (Cth) sets out Information Privacy Principles<sup>1</sup> that apply to Australian federal government agencies, and National Privacy Principles<sup>2</sup> that apply to private sector organizations. The Privacy Act covers federal law enforcements agencies, but intelligence-gathering and national security agencies are exempt.<sup>3</sup> The principles set out responsibilities and requirements relating to the collection, storage, use, disclosure, and access to personal information held by the different entities. The Telecommunications Act 1997 (Cth) contains rules dealing specifically with information and communications held by telecommunications carriers and carriage service providers.<sup>4</sup>

The Telecommunications (Interception and Access) Act 1979 (Cth)<sup>5</sup> (TIA Act) regulates the ability of federal and state law enforcement agencies and the Australian Security Intelligence

---

<sup>1</sup> Privacy Act 1988 (Cth) s 14, available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/882D5E09F7C447CCCA2577CA0008B199/\\$file/Privacy1988\\_WD02HYP.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/882D5E09F7C447CCCA2577CA0008B199/$file/Privacy1988_WD02HYP.pdf).

<sup>2</sup> *Id.* sch 3.

<sup>3</sup> *See id.* s 7(1A). *See also* *Law Enforcement and National Security*, OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, <http://www.privacy.gov.au/topics/lawenforcement> (last visited Dec. 9, 2010).

<sup>4</sup> *Telecommunications Act 1997* (Cth) pt 6 and 13, available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/06D0D5A09A0C04E6CA2577CA007BDF01/\\$file/Tele1997\\_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/06D0D5A09A0C04E6CA2577CA007BDF01/$file/Tele1997_WD02.pdf).

<sup>5</sup> *Telecommunications (Interception and Access) Act 1979* (Cth), available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/F106D44BEEE5431ACA2577EB0005DF81/\\$file/TelecommIntAccess1979\\_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/F106D44BEEE5431ACA2577EB0005DF81/$file/TelecommIntAccess1979_WD02.pdf).

Organisation (ASIO) to obtain warrants to intercept communications passing over a telecommunications system, including the Internet, or to access communications that are stored by service providers.<sup>6</sup> It contains detailed rules and restrictions relating to obtaining warrants, obligations on carriers, the use and disclosure of information, offenses, and the admissibility of evidence. This report focuses on the rules contained in this legislation. Other relevant legislation referred to includes the Telecommunications Act 1997 (Cth), the Surveillance Devices Act 2004 (Cth),<sup>7</sup> the Cybercrime Act 2001 (Cth),<sup>8</sup> and the Australian Security Intelligence Organisation Act 1979 (Cth).<sup>9</sup>

State laws may also further regulate the interception of and access to electronic communication by state agencies. These must not be inconsistent with the federal legislation. State laws are not covered in this report.

In addition to the legislation referred to above, there are a range of government and Internet industry initiatives relating to cybersecurity, including consideration of privacy issues. For example, an Internet Service Provider (ISP) cybersecurity voluntary code of practice came into effect on December 1, 2010.<sup>10</sup> The government also released its Cyber Security Strategy in 2009,<sup>11</sup> and has established a computer emergency response team (CERT), which is the “primary source of cyber security information for the Australian community and the point of contact for Australia’s international cyber security counterparts.”<sup>12</sup>

---

<sup>6</sup> While the legislation does not specifically refer to Internet service providers or Internet access providers, the *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth) apply because such providers fall into the category of “carriage service providers.” See Internet Service Providers and Law Enforcement and National Security Fact Sheet, Australian Communications and Media Authority (ACMA), [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_100072](http://www.acma.gov.au/WEB/STANDARD/pc=PC_100072) (last visited Dec. 7, 2010) (note that it appears that this Fact Sheet is currently being updated, see Fact Sheets A-Z, ACMA, [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_310076](http://www.acma.gov.au/WEB/STANDARD/pc=PC_310076) (last visited Dec. 7, 2010).) See also Eugene Clark, George Cho, Arthur Hoyle & Paul Hynes, *Cyber Law in Australia* 359 (2010) (stating that “Internet service providers (ISPs) are carriage service providers, while anyone operating a website is arguably a content service providers. The Broadcasting Services Amendment (Online Services) Act 1999 (Cth) uses the same definitions, likewise regarding ISPs as carriage service providers.”).

<sup>7</sup> *Surveillance Devices Act 2004* (Cth), available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/D2FEAB3D2D45584CCA25773C00045369/\\$file/SurveillDevices2004.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/D2FEAB3D2D45584CCA25773C00045369/$file/SurveillDevices2004.pdf).

<sup>8</sup> *Cybercrime Act 2001* (Cth), available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/78F3C45ABCF46F42CA256F7100560110/\\$file/Cybercrime2001.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/78F3C45ABCF46F42CA256F7100560110/$file/Cybercrime2001.pdf).

<sup>9</sup> *Australian Security Intelligence Organisation Act 1979* (Cth), available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/BDB9F76626CD1EF8CA25773C0014FD09/\\$file/ASIO1979\\_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/BDB9F76626CD1EF8CA25773C0014FD09/$file/ASIO1979_WD02.pdf).

<sup>10</sup> *ISP Cyber Security Code of Practice Comes into Effect*, STAY SMART ONLINE, [http://www.staysmartonline.gov.au/news/news\\_articles/regular/isp\\_cyber\\_security\\_code\\_of\\_practice\\_comes\\_into\\_effect](http://www.staysmartonline.gov.au/news/news_articles/regular/isp_cyber_security_code_of_practice_comes_into_effect) (last visited Dec. 9, 2010). The Code of Practice is available at <http://iia.net.au/images/resources/pdf/icode-v1.pdf>.

<sup>11</sup> *Cyber Security Strategy* (Attorney-General’s Department, Commonwealth of Australia, 2009), available at [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA8653D%29~AG+Cyber+Security+Strategy+-+for+website.pdf/\\$file/AG+Cyber+Security+Strategy+-+for+website.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%284CA02151F94FFB778ADAEC2E6EA8653D%29~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf).

<sup>12</sup> See Press Release, Hon. Robert McClelland MP, Strengthening Australia’s Cyber Security Capability (Nov. 12, 2010), [http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/page/MediaReleases2010\\_FourthQuarter\\_12November2010-StrengtheningAustraliacybersecuritycapability](http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/page/MediaReleases2010_FourthQuarter_12November2010-StrengtheningAustraliacybersecuritycapability).

## II. Interception of Electronic Communications

Under the Telecommunications Act 1997 (Cth), ISPs are prohibited from disclosing the contents or substance of any communication or any information relating to the affairs or personal particulars of any person.<sup>13</sup> The legislation sets out a number of exceptions, including where the disclosure is required or otherwise authorized under a warrant or under law.<sup>14</sup>

Section 7 of the TIA Act prohibits the interception of telecommunications except in specified circumstances, including interception pursuant to a warrant.<sup>15</sup> Telecommunications interception warrants are issued under Chapter 2 of the TIA Act. The types of interception warrants are:

- Telecommunications service warrants and named person warrants issued by the Attorney-General to the ASIO in relation to security matters and for the collection of foreign intelligence (Part 2-2 warrants); and
- Telecommunications service warrants and named person warrants issued by a judge in relation to investigations of serious offenses by law enforcement agencies (Part 2-5 warrants).

Part 2-6 sets out the rules relating to dealing with intercepted information obtained using interception warrants. This includes provisions relating to employees of carriers, sharing of information by agencies, giving information in evidence in criminal and civil proceedings, and the destruction of records. Section 63 contains a general prohibition on communicating, using, making a record of, or giving in evidence in a proceeding, any intercepted information (whether lawfully or unlawfully intercepted) or any interception warrant information, unless this is done in accordance with the provisions in the Part.<sup>16</sup>

In addition to warrants, Part 2-4 of the TIA Act includes provisions relating to authorizations to intercept communications for the purposes of developing and testing interception capabilities.

### A. Part 2-2 Warrants

The Attorney-General may issue telecommunications service interception warrants upon the receipt of a request from the Director-General of Security where the telecommunications

---

<sup>13</sup> *Telecommunications Act 1997* (Cth) pt 13, s 270 (Simplified Outline). See also ACMA, *supra* note 6.

<sup>14</sup> *Id.* s 280. See below for information about exceptions to the prohibition.

<sup>15</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 7. See below for information about exceptions to the prohibition.

<sup>16</sup> See below for information about the exceptions in Part 2-6.

service is being, or is likely to be, used by a person engaged in, reasonably suspected to be engaged in, or likely to engage in, “activities prejudicial to security.”<sup>17</sup>

Where the warrant relates to the telecommunications service used by a person who is not the target of the investigation, but who is communicating with a person who is,<sup>18</sup> the Attorney-General must be satisfied that the ASIO has “exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the other person,” or that the interception from the telecommunications service used by that person would not otherwise be possible.<sup>19</sup> Such warrants may only remain in force for a period of three months, as compared to a maximum of six months for other Part 2-2 warrants.<sup>20</sup>

The Attorney-General may also issue warrants for named persons, rather than for a specific telecommunications service.<sup>21</sup> Named person warrants cover communications made to or from any telecommunications services used, or likely to be used, by the person, or communications made by means of particular telecommunications devices used by the person. In terms of warrants for the interception of communications made by means of a device, the Attorney-General must be satisfied that there are no other practicable methods available to the ASIO to identify the particular telecommunications service used, or that interception would not otherwise be practicable.<sup>22</sup>

In terms of emergency situations, provision is made for the Director-General of Security to authorize interception “by a warrant under his or her hand” prior to the issuing of a warrant by the Attorney-General. The Director-General must have forwarded a request to the Attorney-General, and must be satisfied that the facts of the case would justify the issuance of a warrant, and that if the interception does not commence before a warrant is issued by the Attorney-General “security will be, or is likely to be, seriously prejudiced.”<sup>23</sup> Such warrants are only to remain in force for a maximum period of forty-eight hours, and may be revoked by the Attorney-General at any time before the expiration of the period.<sup>24</sup> The Director-General must provide the Attorney-General with a copy of the warrant and a statement of the grounds on which it was issued.<sup>25</sup>

---

<sup>17</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 9(1)(a)(i). “Security” is defined in the *Australian Security Intelligence Organisation Act 1979* (Cth).

<sup>18</sup> See *Telecommunications (Interception and Access) Act 1979* (Cth) s 9(1)(a)(ia), which allows for such warrants to be issued.

<sup>19</sup> *Id.* s 9(3).

<sup>20</sup> *Id.* s 9B(3A).

<sup>21</sup> *Id.* s 9A.

<sup>22</sup> *Id.* s 9A(3).

<sup>23</sup> *Id.* s 10(1)(d).

<sup>24</sup> *Id.* s 10(3).

<sup>25</sup> *Id.* s 10(4).

The Attorney-General may also issue telecommunications service warrants and named person warrants (including in relation to named foreign organizations) for the collection of foreign intelligence where he or she is satisfied, on the basis of advice from the Minister for Defence or the Minister for Foreign Affairs, that the collection relates to a matter that is in the interests of “Australia’s national security, Australia’s foreign relations or Australia’s national economic wellbeing.”<sup>26</sup> In order for named person warrants to be issued in such cases the Attorney-General must be satisfied that relying on a telecommunications service warrant to obtain the intelligence would be ineffective.<sup>27</sup> The restrictions relating to warrants for devices stated above also apply.<sup>28</sup>

A third type of warrant for the collection of foreign evidence relates to the interception of foreign communications. In addition to being satisfied that this is in Australia’s interests mentioned above, the Attorney-General must be satisfied that it is necessary to intercept foreign communications in order to collect the intelligence, and that relying on a telecommunications service or named person warrant would be ineffective.<sup>29</sup> A warrant issued under this provision can only authorize the interception of foreign communications.<sup>30</sup> Where the Director-General considers that any communication intercepted under such a warrant is “not relevant to the purposes specified in the warrant,” he or she must “cause any record or copy of the communication to be destroyed.”<sup>31</sup>

Foreign intelligence warrants may remain in force for a period of up to six months.<sup>32</sup> These warrants cannot be issued for the purpose of collecting information concerning an Australian citizen or permanent resident.<sup>33</sup>

Provisions relating to how Part 2-2 warrants are to be dealt with include the processes for informing the relevant carrier, recording of decisions on warrants, keeping of records, and requirements relating to descriptions of services and devices to which warrants apply.<sup>34</sup> The Director-General is required to provide reports on the results of interceptions to the Attorney-General in relation to all Part 2-2 warrants.<sup>35</sup> The TIA Act also requires that, where the Director-General is satisfied that a record or copy of a communication intercepted under a Part 2-2

---

<sup>26</sup> *Id.* ss 11A(1) (telecommunications service warrant), s 11B(1) (named person warrant).

<sup>27</sup> *Id.* s 11B(b)(i). Additional requirements for named person warrants issued under ss 9A or 11B are set out in s 16.

<sup>28</sup> *Id.* s 11B(3).

<sup>29</sup> *Id.* s 11C(1).

<sup>30</sup> *Id.* s 11C(2).

<sup>31</sup> *Id.* s 11C(5).

<sup>32</sup> *Id.* s 11D(2).

<sup>33</sup> *Id.* s 11D(5).

<sup>34</sup> *Id.* ss 15-16.

<sup>35</sup> *Id.* s 17.

warrant is not required, and is not likely to be required, in connection with the ASIO's functions and powers, such a record or copy must be destroyed.<sup>36</sup>

## B. Part 2-5 Warrants

Agencies<sup>37</sup> may apply for telecommunications interception warrants where information that would likely be obtained under the warrant “would be likely to assist in connection with the investigation of a serious offence, or serious offences.”<sup>38</sup> Such warrants may be issued by a judge or a nominated member of the Administrative Appeals Tribunal (AAT).<sup>39</sup> Applications for warrants are to be in writing, but provision is made for the chief officer of an agency to make an application by telephone if he or she thinks it is necessary because of urgent circumstances.<sup>40</sup> Written applications must be accompanied by an affidavit that sets out the facts and other grounds on which the application is based and a number of other details.<sup>41</sup> Similar information is required for telephone applications.<sup>42</sup>

Telecommunications service warrants may be issued where there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the telecommunications service.<sup>43</sup> The judge or AAT member must have regard to:

- “How much the privacy of any person or persons would be likely to be interfered with by interception under a warrant communications made to or from the service;”<sup>44</sup>
- The gravity of the conduct constituting the offense or offenses being investigated;<sup>45</sup>
- How much the information would be likely to assist the investigation;<sup>46</sup>
- To what extent methods of investigating the offence that do not involve intercepting communications have been used by, or are available to, the agency, and how much

---

<sup>36</sup> *Id.* s 14.

<sup>37</sup> In addition to the Australian Federal Police and other federal agencies such as the Office of Police Integrity and the Independent Commission Against Corruption, the relevant Minister may, by legislative instrument, declare an eligible state authority—such as a police force—to be an agency for the purposes of the Act. *Id.* ss 34-38.

<sup>38</sup> *Id.* ss 46(1)(d) (telecommunications service warrant), s 46A(1)(d) (named person warrant). “Serious offence” is defined in detail in s 5D and includes murder, kidnapping, conduct involving an act of terrorism, specified offenses under the *Criminal Code* and other legislation, and offenses punishable by imprisonment for life or for a period of at least seven years.

<sup>39</sup> *See id.* s 6DB.

<sup>40</sup> *Id.* s 40.

<sup>41</sup> *Id.* s 42.

<sup>42</sup> *Id.* s 43.

<sup>43</sup> *Id.* s 46(1)(c).

<sup>44</sup> *Id.* s 46(2)(a).

<sup>45</sup> *Id.* s 46(2)(b).

<sup>46</sup> *Id.* s 46(2)(c).

the use of such methods would be likely to assist or prejudice the investigation (for example, because of delay).<sup>47</sup>

Similar to the requirements relating to Part 2-2 warrants, a warrant in respect of a person not being investigated, but with whom a particular person suspected of being involved in a serious offense may communicate using the service, cannot be issued unless the agency has exhausted all other practicable methods of identifying the telecommunications services used by the person being investigated, or interception made to or from those services would not otherwise be possible.<sup>48</sup> Such warrants can only be issued for a maximum of forty-five days, whereas other Part 2-5 warrants can be issued for up to ninety days.<sup>49</sup>

Where a person being investigated may be using more than one telecommunications service, a named person warrant may be issued in respect of any service that person is using, or is likely to use, or to intercept communications made by means of a particular telecommunications device.<sup>50</sup> The list of considerations set out above also applies in such cases.<sup>51</sup> In addition, warrants relating to devices must not be issued unless there are not other practicable means to identify the telecommunications services used, or interception made to or from a telecommunications service would not otherwise be practicable.<sup>52</sup>

Provisions in Part 2-6 require the destruction of records obtained by means of an interception where they are not likely to be required for a permitted purpose.<sup>53</sup> Part 2-7 sets out the rules for the keeping and inspection of interception records relating to Part 2-5 warrants, including the powers of the Ombudsman to inspect records. Part 2-8 sets out the requirements relating to annual reports to the relevant Minister about warrant and interception activities.

### III. Surveillance

In addition to the provisions in the TIA Act, the Surveillance Devices Act 2004 (Cth) enables law enforcement agencies to install surveillance devices under surveillance device warrants,<sup>54</sup> including data surveillance devices, listening devices, and tracking devices.<sup>55</sup> “Data surveillance device” is defined as “any device or program capable of being used to record or monitor the input of information into, or the output of information from, a computer, but does

---

<sup>47</sup> *Id.* s 46(2)(d)-(f).

<sup>48</sup> *Id.* s 46(3).

<sup>49</sup> *Id.* s 49(3).

<sup>50</sup> *Id.* s 46A(1).

<sup>51</sup> *Id.* s 46A(2).

<sup>52</sup> *Id.* s 46A(3).

<sup>53</sup> *Id.* ss 79, 79A.

<sup>54</sup> *Surveillance Devices Act 2004* (Cth), s 10 (stating that a warrant may be issued in respect of more than one kind of surveillance device).

<sup>55</sup> *Id.* s 6 (definition of surveillance device).

not include an optical surveillance device.”<sup>56</sup> “Tracking device” means “any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.”<sup>57</sup>

A law enforcement officer may apply for a surveillance device warrant if he or she suspects on reasonable grounds that:

- (a) one or more relevant offences have been, are being, are about to be, or are likely to be, committed; and
- (b) an investigation into those offences is being, will be, or is likely to be, conducted; and
- (c) the use of a surveillance device is necessary in the course of that investigation for the purpose of enabling evidence to be obtained of the commission of the relevant offences or the identity or location of the offenders.<sup>58</sup>

Surveillance device warrants may be issued by a judge or nominated AAT member.<sup>59</sup> In determining whether a warrant should be issued, regard must be given to a list of factors, including the nature and gravity of the alleged offense, the extent to which the privacy of any person is likely to be affected, the existence of alternative means of obtaining the information sought, and the likely evidentiary value of any evidence or information sought.<sup>60</sup> Emergency authorizations can be issued in situations where there is an imminent risk of “serious violence to a person or substantial damage to property,”<sup>61</sup> or where particular crimes are being investigated and the use of a surveillance device is immediately necessary to prevent the loss of evidence.<sup>62</sup>

The Surveillance Devices Act 2004 contains provisions relating to dealing with information obtained using surveillance devices,<sup>63</sup> reporting requirements,<sup>64</sup> recordkeeping,<sup>65</sup> and the oversight functions of the Ombudsman.<sup>66</sup>

The use of surveillance devices by the ASIO, including tracking and listening devices, are governed by the Australian Security Intelligence Organisation Act 1979 (Cth).<sup>67</sup>

---

<sup>56</sup> *Id.* s 6 (definition of data surveillance device).

<sup>57</sup> *Id.* s 6 (definition of tracking device).

<sup>58</sup> *Id.* s 14. “Relevant offence” is defined in s 6 as an offence under federal or state law that is punishable by a maximum term of imprisonment of more than three years, as well as specified offences under the *Financial Transaction Reports Act 1988*, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, the *Fisheries Management Act 1991*, and the *Torres Strait Fisheries Act 1984*.

<sup>59</sup> *Id.* ss 11-13.

<sup>60</sup> *Id.* s 16(2).

<sup>61</sup> *Id.* s 28.

<sup>62</sup> *Id.* s 30.

<sup>63</sup> *Id.* ss 46-48.

<sup>64</sup> *Id.* ss 49-50.

<sup>65</sup> *Id.* ss 51-53.

<sup>66</sup> *Id.* ss 54-61.

#### IV. Access to Stored Communications

It is an offense to access stored communications unless access is permitted by a warrant or some other exception applies.<sup>68</sup> A separate stored communications warrant is not required where a Part 2-2 warrant has been issued to the ASIO. Part 3-2 of the TIA Act states that such warrants also authorize a person to access a stored communication if “the warrant would have authorised interception of the communication if it were still passing over a telecommunications system.”<sup>69</sup> In addition, computer access warrants may be issued under the Australian Security Intelligence Organisation Act 1979 (Cth).<sup>70</sup> Such warrants may include using a computer, telecommunications facility, or any other electronic equipment or data storage device for the purposes of obtaining data that is relevant to a security matter.<sup>71</sup>

Law enforcement agencies may apply for stored communications warrants in respect of a person under Part 3-3 of the TIA Act. There must be reasonable grounds for suspecting that a particular carrier holds stored communications that the person has made, or that another person has made and for which the person is the intended recipient.<sup>72</sup> The information that would likely be obtained under a warrant must be likely to assist an investigation of a “serious contravention” in which the person is involved.<sup>73</sup> As with interception warrants issued under Part 2-5, the Act lists a number of matters that must be taken into account, including how much the privacy of any person or persons would likely to be interfered with.<sup>74</sup>

Stored communications warrants may be issued by an “issuing authority,” which includes judges, federal magistrates, magistrates, and members of the AAT who have been nominated by the relevant Minister.<sup>75</sup> The Act makes provision for such warrants to be issued on a telephone application.<sup>76</sup> A stored communications warrant remains in force until it is first executed, or for five days after the day on which it was issued, whichever occurs sooner.<sup>77</sup>

Part 3-4 sets out the rules relating to dealing with accessed information in similar terms to the provisions that apply with respect to interception warrants. This includes the destruction of information obtained by accessing a stored communication if the chief officer of the agency

---

<sup>67</sup> *Australian Security Intelligence Organisation Act 1979* (Cth) ss 26-26C.

<sup>68</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 108. See below for information on exceptions to the prohibition on accessing stored communications.

<sup>69</sup> *Id.* s 109.

<sup>70</sup> *Australian Security Intelligence Organisation Act 1979* (Cth) s 25A.

<sup>71</sup> *Id.* s 25A(4).

<sup>72</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 116(1)(c).

<sup>73</sup> *Id.* § 116(1)(d). “Serious contravention” is defined in s 5E and includes “serious offenses” (defined in s 5D), and offenses punishable by at least three years’ imprisonment or particular fine levels.

<sup>74</sup> *Id.* s 116(2).

<sup>75</sup> See *id.* ss 6DA, 6DB.

<sup>76</sup> *Id.* s 120.

<sup>77</sup> *Id.* s 119.

determines that it is not likely to be required for a permitted purpose.<sup>78</sup> Part 3-5 contains the recordkeeping requirements and the Ombudsman's functions with respect to inspections of those records. Part 3-6 covers the requirements for annual reports to be produced regarding stored communications warrant activities.

## V. Types of Communication Covered

The TIA Act defines “communication” as including

conversation and a message, and any part of a conversation or message, whether:

- (a) in the form of:
  - (i) speech, music or other sounds;
  - (ii) data;
  - (iii) text;
  - (iv) visual images, whether or not animated; or
  - (v) signals; or
- (b) in any other form or in any combination of forms.<sup>79</sup>

Further relevant definitions are similarly broad in scope. For example, definitions are provided for “stored communication” (a communication that is not passing over a telecommunications system and that is held on equipment operated by, and in the possession of, a carrier), “telecommunications device” (a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system), and “telecommunications network” and “telecommunications service” (systems and services for carrying communications “by means of guided or unguided electromagnetic energy or both,” but excluding systems and services that carry communications solely by means of radiocommunication).<sup>80</sup>

The legislation covers telecommunications networks that are within, or partly within, Australia, but only to the extent that the network is within Australia,<sup>81</sup> “whether or not the communications originated in Australia, and whether or not the final destination of the communications is within Australia.”<sup>82</sup>

---

<sup>78</sup> *Id.* s 150.

<sup>79</sup> *Id.* s 5. See also *Telecommunications Act 1997* (Cth) s 5 (definition of “communications”).

<sup>80</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 5. See also *Telecommunications Act 1997* (Cth) s 5 (definition of “telecommunications network”).

<sup>81</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 5. See also s 5(5), which clarifies when a telecommunications network shall be taken to be within Australia. This includes networks used for the purpose of carrying communications over an earth-based facility within Australia, between an earth-based facility within Australia and a satellite-based facility, and over or between satellite-based facilities to the extent that the last or next earth-based facility for the communication is in Australia.

<sup>82</sup> *Id.* s 5(5).

## VI. Exceptions

The telecommunications legislation contains exemptions from the application of the provisions. In particular, radiocommunication systems are exempt by virtue of the definitions of “telecommunications network” and “telecommunications system,” as noted above. The Telecommunications Act 1997 also states that entities will be exempt from the definition of a “carriage service provider” (which is included in the definition of a “carrier” under the TIA Act) where:

- The supplier of the service manages a business or activity on particular premises, and all of its customers are physically present on those premises;<sup>83</sup>
- The sole or principal use of the service is by a defense organization to carry communications for defense purposes;<sup>84</sup>
- The service is wholly or principally used by the ASIO or the Australian Secret Intelligence Service;<sup>85</sup>
- The service is wholly or principally used by transport authorities to carry communications for the workings of aviation, train, bus, or tram services;<sup>86</sup>
- The sole or principal use of the service is to carry communications that are necessary for the supply of broadcasting services to the public;<sup>87</sup>
- The sole or principal use of the service is use by an electrical supply body to carry communications necessary for managing the generation, transmission, distribution, or supply of electricity;<sup>88</sup> or
- The relevant Minister has made a determination, by written instrument, that the definition will not apply to a particular person or specified carriage service.<sup>89</sup>

There are also exceptions to the application of the prohibitions against intercepting, disclosing, using, or recording communications and information, as set out below.

### A. Exceptions to the Prohibition on Intercepting Communications

The prohibition on the interception of communications in section 7 of the TIA Act is subject to the following exceptions:

---

<sup>83</sup> *Telecommunications Act 1997* (Cth) s 89.

<sup>84</sup> *Id.* s 90.

<sup>85</sup> *Id.* s 91.

<sup>86</sup> *Id.* s 92.

<sup>87</sup> *Id.* s 93.

<sup>88</sup> *Id.* s 94.

<sup>89</sup> *Id.* s 95.

- An act done by an employee of a carrier in the course of his or her duties relating to: the installation of any line or equipment used in connection with a telecommunications service; the operation or maintenance of a telecommunications system; or the identifying or tracing of any person who has contravened particular provisions of the Criminal Code.<sup>90</sup>
- Interception by a person lawfully engaged in duties relating to the installation, connection, or maintenance of equipment or a line, where the interception is reasonably necessary in order to perform those duties effectively.<sup>91</sup>
- Interception by a person who has been authorized, in writing, by a responsible person for a computer network to engage in network protection duties, and the interception is reasonably necessary in order to perform those duties effectively.<sup>92</sup>
- Interception by a person lawfully engaged in duties relating to the installation, connection, or maintenance of equipment used for the interception of communications under warrants.<sup>93</sup>
- Interception that results from, or is incidental to, action taken by an ASIO officer, in the lawful performance of his or her duties, for the purpose of discovering whether a listening device is being used at a particular place or determining the location of a listening device.<sup>94</sup>
- Interception of a communication under a warrant.<sup>95</sup>
- Interception pursuant to an emergency request or authorization made under the TIA Act.<sup>96</sup>
- Acts done by an officer of an agency if the officer or another officer of the agency is a party to the communication and there are reasonable grounds for suspecting that another party to the communication has done, or threatened to do, certain acts involving harm to themselves or others, where it is not practicable to make an application for a Part 2-5 warrant due to the urgency of the situation.<sup>97</sup>
- Acts done by an officer of an agency where the person to whom the communication is directed has consented to the act and there are reasonable grounds for believing that he or she is likely to receive communication from a person who has done, or threatened to do, certain acts involving harm to themselves or others, where it is not

---

<sup>90</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 7(2)(a).

<sup>91</sup> *Id.* s 7(2)(aa).

<sup>92</sup> *Id.* s 7(2)(aaa).

<sup>93</sup> *Id.* s 7(2)(ab).

<sup>94</sup> *Id.* s 7(2)(ac).

<sup>95</sup> *Id.* s 7(2)(b).

<sup>96</sup> *Id.* s 7(2)(c), (d).

<sup>97</sup> *Id.* s 7(4). Note that for this exception, and for that set out in s 7(5), an officer must make an application for a Part 2-5 warrant unless that action has ceased before it is practicable for such an application to be made. *Id.* ss 7(6), 7(6A).

practicable to make an application for a Part 2-5 warrant due to the urgency of the situation.<sup>98</sup>

## **B. Exceptions to the Prohibition on Disclosing Information**

In terms of dealing with intercepted information, Part 2-6 of the TIA Act sets out a number of exceptions to the general prohibition contained in section 63, including:

- Communicating, making a record of, or making use of interception warrant information, or giving such information in evidence in a proceeding, for the purposes of Parts 2-2, 2-5, 2-7, or 2-8.<sup>99</sup>
- Exceptions relating to employees of a carrier communicating information in the performance of their duties, including in relation to the operation or maintenance of a telecommunications network, the supply of services, and where the communication of interception warrant information is reasonably necessary to enable the interception of a communication under the warrant.<sup>100</sup>
- Communicating or making use of lawfully intercepted information in performing duties relating to network protection.<sup>101</sup>
- Where a person is engaged in network protection duties in relation to a network operated by a government agency, the person may communicate or make use of lawfully intercepted information for the purpose determining whether disciplinary action should be taken in relation to use of the network by an employee of the agency.<sup>102</sup>
- A person with responsibility for a computer network may communicate information that has been intercepted lawfully if he or she suspects that it is relevant to determining whether another person committed an offense.<sup>103</sup>
- Communicating, making use of, or making a record of, lawfully intercepted information (other than foreign intelligence information) in connection with the performance by the ASIO of its function.<sup>104</sup> Only employees of the ASIO may communicate foreign intelligence information, unless there is approval in writing by the Attorney-General.<sup>105</sup>

---

<sup>98</sup> *Id.* s 7(5).

<sup>99</sup> *Id.* s 63AA.

<sup>100</sup> *Id.* s 63B.

<sup>101</sup> *Id.* s 63C.

<sup>102</sup> *Id.* s 63D.

<sup>103</sup> *Id.* s 63E.

<sup>104</sup> *Id.* s 64(1).

<sup>105</sup> *Id.* ss 64(2), 65.

- An employee of a carrier may communicate lawfully intercepted information (other than foreign intelligence information) to an officer of an agency for a purpose connected with the investigation of a serious offense.<sup>106</sup>
- A person who has intercepted information under a warrant may also communicate the information obtained to the relevant agency.<sup>107</sup>
- An officer of an agency may communicate, make use of, or make a record of lawfully intercepted information (other than foreign intelligence information) for a permitted purpose.<sup>108</sup>
- The Chief Officer of the agency may communicate lawfully intercepted information to other agencies in a range of listed situations.<sup>109</sup>
- A member of a police force may communicate to another member, or to any other person whose assistance may be required in dealing with an emergency, information obtained by an interception under Part 2-3.<sup>110</sup>
- Where a person suspects that information obtained by intercepting communication may establish that an offense has been committed under section 7 or section 63 of the TIA Act, this information may be communicated to, for example, the Attorney General, Integrity Commissioner, or Commissioner of Police.<sup>111</sup>
- A person may give lawfully intercepted information (other than foreign intelligence information) in evidence in an exempt proceeding.<sup>112</sup>

The Surveillance Devices Act 2004 also sets out exceptions to the prohibition on the use, recording, communication or publication of information obtained under or associated with the use of a surveillance device, including:

- Where information has been disclosed in open court.<sup>113</sup>
- Where a person believes that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property.<sup>114</sup>

---

<sup>106</sup> *Id.* s 65A.

<sup>107</sup> *Id.* s 66.

<sup>108</sup> *Id.* s 67. “Permitted purpose” is defined in s 5 and includes purposes connected with investigating prescribed offenses, making decisions relating to proceedings, relevant proceedings, the exercise of particular powers by the chief officer, and the keeping of records under Part 2-7. It also includes a range of activities such as disciplinary actions and decisions relating to appointments, retirements, and terminations of agency employees, and the exercise of functions by different bodies.

<sup>109</sup> *Id.* s 68.

<sup>110</sup> *Id.* s 70. Part 2-3 warrants relate to the interception of emergency calls.

<sup>111</sup> *Id.* s 71.

<sup>112</sup> *Id.* s 74. “Exempt proceeding” is defined in s 5B and refers to proceedings by way of a prosecution for a prescribed offense, and proceedings relating to the provisions in a number of other statutes and actions.

<sup>113</sup> *Surveillance Devices Act 2004* (Cth) s 45(4)(a).

- Communication to the ASIO or another agency with functions under the Intelligence Services Act 2001, and use, recording, or communication of the information by an officer of such an agency in the performance of his or her functions.<sup>115</sup>
- Communication to a foreign country in accordance with the Mutual Assistance in Criminal Matters Act 1987.<sup>116</sup>
- Where it is necessary for the investigation of a relevant offense, the making of a decision regarding prosecution of a relevant offense, or a relevant proceeding.<sup>117</sup>
- Where it is necessary to the investigation of a complaint about the conduct of a public officer, any subsequent prosecution of the officer, or for making a decision in relation to the appointment, termination, or retirement of the officer.<sup>118</sup>
- The keeping of records as required by the Act and inspections by the Ombudsman.<sup>119</sup>
- Where it is necessary for the performance of any function of public interest monitors under certain legislation.<sup>120</sup>
- Where it is necessary for the investigation under the Privacy Act 1988 or any other Commonwealth law concerning the privacy of personal information, and any subsequent prosecution of a relevant offense arising from that investigation.<sup>121</sup>

The Telecommunications Act 1997 also prohibits the disclosure of information held by service providers, including personal information and location information.<sup>122</sup> Disclosure or use of protected information is authorized in limited circumstances, including disclosure or use:

- By an employee or contractor of a service provider in the performance of his or her duties.<sup>123</sup>
- In connection with the operation of an enforcement agency where the disclosure or use is required or authorized under a warrant, or otherwise where it is required or authorized by or under law.<sup>124</sup>

---

<sup>114</sup> *Id.* s 45(4)(b).

<sup>115</sup> *Id.* s 45(4)(c)-(e).

<sup>116</sup> *Id.* s 45(4)(f).

<sup>117</sup> *Id.* s 45(5)(a)-(c).

<sup>118</sup> *Id.* s 45(5)(d)-(e).

<sup>119</sup> *Id.* s 45(5)(f)-(g).

<sup>120</sup> *Id.* s 45(5)(h).

<sup>121</sup> *Id.* s 45(5)(i).

<sup>122</sup> *Telecommunications Act 1997 (Cth)* pt 13.

<sup>123</sup> *Id.* s 279.

<sup>124</sup> *Id.* s 280.

- By a person who is summoned as a witness to give evidence or produce documents.<sup>125</sup>
- To assist the Australian Communications and Media Authority, the Australian Competition and Consumer Commission, or the Telecommunications Industry Ombudsman.<sup>126</sup>
- Where a person believes that disclosure or use is reasonably necessary to prevent or lessen a serious or imminent threat to the life or health of a person.<sup>127</sup>
- Where the person that the information relates to “is reasonably likely to have been aware or made aware that information or a document of that kind is usually disclosed, or used, as the case requires, in the circumstances concerned,” or “has consented to the disclosure, or use, as the case requires, in the circumstances concerned.”<sup>128</sup>
- Where the information relates to a communication by another person, and “it might reasonably be expected that the sender and the recipient of the communication would have consented to the disclosure or use, if they had been aware of the disclosure or use.”<sup>129</sup>
- Where the disclosure or use is made for the purpose of, or is connected to, another service provider carrying on its business.<sup>130</sup>

### C. Exceptions to the Prohibition on Accessing Stored Communications

In terms of accessing stored communications, the TIA Act sets out a number of exceptions to the general prohibition, including:

- Access pursuant to a warrant.<sup>131</sup>
- An act done by an employee of a carrier in the course of his or her duties relating to the installation of any line, the operation or maintenance of a telecommunications system, or the identification or tracing of any person who is suspected of contravening certain provisions of the Criminal Code.<sup>132</sup>
- Access by a person lawfully engaged in duties relating to installing or maintaining systems for accessing stored communications under warrants.<sup>133</sup>

---

<sup>125</sup> *Id.* s 281.

<sup>126</sup> *Id.* s 284.

<sup>127</sup> *Id.* s 287.

<sup>128</sup> *Id.* s 289.

<sup>129</sup> *Id.* s 290.

<sup>130</sup> *Id.* s 291.

<sup>131</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 108(2)(a)-(c).

<sup>132</sup> *Id.* s 108(2)(d)-(e).

<sup>133</sup> *Id.* s 108(2)(f).

- Access that results from, or is incidental to, an action taken by an officer of the ASIO in performing his or her duties relating to discovering and determining the location of listening devices.<sup>134</sup>
- Access by the Australian Communications and Media Authority engaged in duties relating to the enforcement of the Spam Act 2003.<sup>135</sup>

## VII. Obligations on Service Providers

Under the Telecommunications Act 1997, carriers and carriage service providers must ensure that it is possible to execute a warrant under the Telecommunications (Interception and Access) Act 1979.<sup>136</sup> Such entities must prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offenses,<sup>137</sup> and must give officers and authorities of the Commonwealth and States such help as is reasonably necessary for enforcing criminal laws and laws imposing pecuniary penalties, protecting the public revenue, and safeguarding national security.<sup>138</sup>

Part 5-3 of the TIA Act sets out the obligations on carriers with respect to interception capability. Under this Part, the relevant Minister may make determinations relating to “interception capabilities applicable to a specified kind of telecommunications service that involves, or will involve, the use of a telecommunications system.”<sup>139</sup> A carrier must then ensure that the capability is developed, installed, and maintained.<sup>140</sup> Where a carrier is not covered by a determination, it must still ensure that the system has the capability to enable a communication passing over the system to be intercepted.<sup>141</sup> Carriers must also have delivery capabilities<sup>142</sup> and “interception capability plans” that comply with the requirements in the TIA Act.<sup>143</sup> The legislation sets out provisions relating to the allocation of costs between carriers and interception agencies in relation to the development, installation, and maintenance of interception and delivery capabilities.<sup>144</sup>

---

<sup>134</sup> *Id.* s 108(2)(g).

<sup>135</sup> *Id.* s 108(2)(h).

<sup>136</sup> *Telecommunications Act 1997* (Cth) pt 14 (national interest matters). *See also* Internet Service Providers Interception Obligations Fact Sheet, ACMA, [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_100073](http://www.acma.gov.au/WEB/STANDARD/pc=PC_100073) (last visited Dec. 7, 2010). Note that this Fact Sheet is in the process of being updated. *See* Fact Sheets A-Z, ACMA, [http://www.acma.gov.au/WEB/STANDARD/pc=PC\\_310076](http://www.acma.gov.au/WEB/STANDARD/pc=PC_310076) (last visited Dec. 7, 2010).

<sup>137</sup> *Id.* ss 313(1), (2).

<sup>138</sup> *Id.* s 313(3), (4).

<sup>139</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 189(1).

<sup>140</sup> *Id.* s 190(2).

<sup>141</sup> *Id.* s 191(1).

<sup>142</sup> *Id.* pt 5-5.

<sup>143</sup> *Id.* pt 5-4.

<sup>144</sup> *Id.* pt 5-6.

## VIII. Offenses and Penalties

### A. Unlawful Interception of Communications

Contravention of section 7 of the TIA Act is an offense punishable by up to two years' imprisonment.<sup>145</sup> Part 2-10 of the TIA Act contains provisions relating to civil remedies for unlawful interception.

### B. Unlawful Use or Disclosure of Information

A breach of section 63 of the TIA Act is an offense punishable by up to two years' imprisonment.<sup>146</sup> Part 2-10 contains provisions relating to civil remedies for unlawful communication of intercepted information.

Under the Telecommunications Act 1997, unlawful disclosure of information by an employee (or former employee) of a service provider carries a penalty of up to two years' imprisonment.<sup>147</sup>

The Surveillance Devices Act 2004 provides that it is an offense to use, record, communicate, or publish any protected information, where this is not permitted by the provisions in the Act.<sup>148</sup> The penalty is up to two years' imprisonment, or up to ten years if the action endangers the health or safety of any person or prejudices the effective conduct of an investigation.<sup>149</sup>

### C. Unlawful Access to Stored Communications

Unlawful access to stored communication carries a penalty of up to two years' imprisonment or a fine, or both.<sup>150</sup> Part 3-7 of the TIA Act sets out civil remedies for unlawful access to or disclosure of stored communications.

### D. Procedural Offenses

It is an offense, punishable by imprisonment of up to six months, for a person to obstruct a person acting under a warrant.<sup>151</sup> There are also offenses relating to obstructing or hindering Ombudsman inspections that carry a penalty of imprisonment for up to six months.<sup>152</sup>

---

<sup>145</sup> *Id.* s 105.

<sup>146</sup> *Id.*

<sup>147</sup> *Telecommunications Act 1997* (Cth) s 276.

<sup>148</sup> *Surveillance Devices Act 2004* (Cth) s 45.

<sup>149</sup> *Id.* s 45(2).

<sup>150</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) s 108.

<sup>151</sup> *Id.* s 106.

<sup>152</sup> *Id.* s 107.

## E. Cybercrime Legislation

In addition to the above offenses, Australia has enacted the Cybercrime Act 2001 (Cth), which includes the following offenses:

- Unauthorized access or modification of data held on a computer, or impairment of electronic communications, with knowledge that such an action is unauthorized, where the person intends to commit, or facilitate the commission of, a serious offense against a law of the Commonwealth, State, or Territory.<sup>153</sup> This offense is punishable by a penalty “not exceeding the penalty applicable to the serious offence.”<sup>154</sup>
- Unauthorized modification of data held in a computer to cause impairment, with knowledge that the modification is unauthorized and being reckless as to whether it will impair access to the data or the reliability of the data. This offense relates to data held in Commonwealth computers as well as modification of data that impairs the operation of a telecommunications service. The penalty is up to ten years’ imprisonment.<sup>155</sup>
- Unauthorized impairment of electronic communication, where the person knows that the impairment is unauthorized and either the communication is sent by means of a telecommunications service or to or from a Commonwealth computer. The penalty is up to ten years’ imprisonment.<sup>156</sup>
- Unauthorized access to, or modification of, restricted data, with intent and with knowledge that the access or modification is unauthorized, where the restricted data is held in a Commonwealth computer, or on behalf of the Commonwealth, or where the access or modification is caused by means of a telecommunications service. The penalty is up to two years’ imprisonment.<sup>157</sup>
- Unauthorized impairment of data held on a computer disk, credit card, or another device used to store data, where the person intends to cause the impairment, and knows that the impairment is unauthorized, and the device is owned by a Commonwealth entity. The penalty is up to two years’ imprisonment.<sup>158</sup>
- Possession or control of data with intent to commit a computer offense carries a penalty of up to three years’ imprisonment.<sup>159</sup>

---

<sup>153</sup> *Cybercrime Act 2001* (Cth) s 477.1.

<sup>154</sup> *Id.* s 477.1(6).

<sup>155</sup> *Id.* s 477.2.

<sup>156</sup> *Id.* s 477.3.

<sup>157</sup> *Id.* s 478.1.

<sup>158</sup> *Id.* s 478.2.

<sup>159</sup> *Id.* s 478.3.

- Producing, supplying, or obtaining data with the intent that it be used by another person in committing a computer offense carries a penalty of up to three years' imprisonment.<sup>160</sup>

## IX. Defenses

The different statutes include the elements that must be satisfied in order for a person to be convicted of an offense, but do not list specific defenses in relation to each offense. The exceptions to the prohibitions on intercepting, accessing, or disclosing communications or personal information listed above could be raised as a defense where a person is charged with an offense under those provisions. The Criminal Code contains general provisions regarding the requirements for different elements of offenses and the available defenses that may apply depending on the type and wording of the offense.<sup>161</sup>

## X. Admissibility of Evidence

The TIA Act states that intercepted and accessed material and warrant information is inadmissible except as provided in the Act.<sup>162</sup> In particular, a person may lawfully give information in evidence in proceedings specified in the legislation ("exempt proceedings"), with the question of whether or not a communication was obtained in contravention of the prohibitions against interception and access to be determined on the balance of probabilities.<sup>163</sup>

The TIA Act makes provision for a court to allow a person to give information in evidence where there was a non-substantial defect or irregularity in the relevant warrant. The court must be satisfied that, but for the irregularity, the interception or access would not have constituted a breach of the prohibitions, and considering all the circumstances the irregularity should be disregarded.<sup>164</sup> This does not apply in the case of foreign intelligence warrants.

A certifying officer of an agency may issue a written certificate setting out relevant facts relating to anything done in relation to the execution of a warrant or in connection with communicating, making use of, making a record of, the custody of, or the giving in evidence of information obtained under the warrant. Such a certificate "is to be received in evidence in an exempt proceeding without further proof and is, in an exempt proceeding, prima facie evidence of the matters stated in the document."<sup>165</sup> A certified copy of a warrant shall also be received in evidence as if it were the original warrant.<sup>166</sup>

---

<sup>160</sup> *Id.* s 478.4.

<sup>161</sup> See *Criminal Code Act 1995* (Cth) ch 2 (general principles of criminal responsibility), available at [http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/97F3AA96A75C181BCA2577EA001ABF49/\\$file/CriminalCode1995\\_WD02.pdf](http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/97F3AA96A75C181BCA2577EA001ABF49/$file/CriminalCode1995_WD02.pdf).

<sup>162</sup> *Telecommunications (Interception and Access) Act 1979* (Cth) ss 77, 147.

<sup>163</sup> *Id.* ss 74, 143.

<sup>164</sup> *Id.* ss 75, 144.

<sup>165</sup> *Id.* s 61(4). See also s 130.

<sup>166</sup> *Id.* ss 61A, 131.

Prepared by Kelly Buchanan  
Foreign Law Specialist  
December 2010

## LAW LIBRARY OF CONGRESS

### CANADA

## PRIVACY OF ELECTRONIC COMMUNICATIONS

### *Executive Summary*

*Canada's Criminal Code contains extensive rules regarding the interception of private communications by law enforcement officials. Judicial orders for wiretapping, surveillance, and the production of data can be obtained. However, Canadian law does not currently impose obligations on service providers. In October of 2010, the Government introduced two bills to address this situation.*

*Violation of the Criminal Code's provisions respecting the interception of private communications is a criminal offense that can result in imprisonment, awards of damages, and the exclusion of evidence in legal proceedings against a person accused of a criminal offense.*

### **I. Interception**

Section 184(1) of Canada's Criminal Code, an Act of Parliament that applies throughout the country, provides that anyone who uses an "electro-magnetic, acoustic, mechanical or other device" to willfully intercept a private communication is guilty of an indictable offense and is liable to imprisonment for a term not exceeding five years.<sup>1</sup> There are a number of exceptions to this general rule, however, including cases in which

- (1) one party consents to the interception;
- (2) the interception is authorized;
- (3) the interceptor is a provider of public communication service who is randomly monitoring the service or is acting to protect the service's rights or property; and
- (4) the interception is carried out by a person in possession or control of a computer system and is reasonably necessary to manage the service's quality with respect to performance, prevent the unauthorized use of a computer, or prevent such malicious acts as destroying or altering data, rendering data meaningless, obstructing the

---

<sup>1</sup> Criminal Code, R.S.C. 1985, c. C-46, § 184(1), *as amended*, <http://laws-lois.justice.gc.ca/eng/C-46/page-5.html>. Canada does not have a separate Code of Criminal Procedure. Most procedural issues are addressed in the Criminal Code itself.

lawful use of data, or denying any person access to data to which he or she is entitled.<sup>2</sup>

Private communications lawfully intercepted by a provider or other non-official party can only be retained if retention is essential to identify, isolate, or prevent harm to a computer system or the communications are to be used in court proceedings.<sup>3</sup>

Section 184.1 of the Criminal Code allows an agent of the state to use the types of devices described above to intercept private communications if either the originator or intended recipient consents, the agent believes on reasonable grounds that there is a risk of bodily harm to the person who consented to the interception, and the purpose of the interception is to prevent bodily harm. Evidence so obtained is only admissible in proceedings in which actual or threatened bodily harm is alleged. Recordings so obtained must be destroyed as soon as is practicable if they do not support such a charge.<sup>4</sup>

Intercepting a private communication with the consent of one party requires judicial authorization. To obtain such an authorization, a law enforcement official must file an affidavit stating that there are reasonable grounds for believing that an offense will be committed. A judge may grant such an application if he agrees that there are reasonable grounds to believe that information concerning the offense that law enforcement is investigating will be obtained through interception.<sup>5</sup> A judicial authorization must state the following:

- (1) The offense being investigated;
- (2) The type of private communication that may be intercepted;
- (3) The identity of the parties, if known;
- (4) The place of interception, if possible;
- (5) The general manner in which the product of interception may be used; and
- (6) Any terms and conditions the judge considers advisable.<sup>6</sup>

Authorization to intercept with consent may be given for up to sixty days.<sup>7</sup> Applications for authorization to intercept private communications may be made by means of a

---

<sup>2</sup> *Id.* § 184(2).

<sup>3</sup> *Id.* § 184(3).

<sup>4</sup> *Id.* § 184.1.

<sup>5</sup> *Id.* § 184.2(1)-(3).

<sup>6</sup> *Id.* § 184.2(4)(a)-(d).

<sup>7</sup> *Id.* § 184.2(4)(e).

telecommunications device if it would be “impracticable” for the law enforcement official to appear personally before a judge.<sup>8</sup>

Interception without judicial authorization is allowed in exceptional circumstances where a peace officer reasonably believes that the urgency of a situation is such that authorization could not be obtained in time to prevent an unlawful act that would cause serious harm to any person or property and the target of the interception is one who would either commit the offense or suffer harm caused by its commission.<sup>9</sup>

The rules pertaining to the interception of private communications where neither the originator nor the expected recipient has consented are more detailed than they are when consent has been obtained. In these cases, the application must be filed by the Attorney General for a province, the Deputy Attorney General, or the Minister for Public Safety and Emergency Preparedness, depending upon certain circumstances. The affidavit must include the same information required for an authorization with the consent of a party, plus such facts as

- (1) the occupations of the parties;
- (2) the number of applications that have been filed in connection with an offense and the dates thereof; and
- (3) whether other investigative procedures have been tried, why they are unlikely to be successful, and why other measures would be impractical.<sup>10</sup>

However, information on other investigative procedures does not have to be included in applications for authorizations to investigate criminal organizations or terrorism offenses.<sup>11</sup> In these cases, the authorization may be for a period of up to one year, as opposed to the usual limit of sixty days.<sup>12</sup>

## II. Surveillance

Under section 186(5.1) of the Criminal Code, “an authorization that permits interception by means of an electro-magnetic, acoustic, mechanical or other device includes the authority to install, maintain or remove the device covertly.”<sup>13</sup>

The Criminal Code does not contain special provisions for the surveillance of Internet communications. There are provisions for other types of surveillance. The adoption of these provisions was required by a major court decision. In 1990, the Supreme Court of Canada held that a warrantless video surveillance by government authorities in circumstances where the

---

<sup>8</sup> *Id.* § 184.3.

<sup>9</sup> *Id.* § 184.4.

<sup>10</sup> *Id.* § 185(1).

<sup>11</sup> *Id.* § 185(1.1).

<sup>12</sup> *Id.* § 186.1.

<sup>13</sup> *Id.* § 186(5.2).

subject has a reasonable expectation of privacy is a violation of section 8 of the Canadian Charter of Rights and Freedoms.<sup>14</sup> Section 8 of the Charter states that “everyone has the right to be secure against unreasonable search or seizure.”<sup>15</sup> Parliament responded to this decision by adding a new provision to the Criminal Code authorizing judges to issue warrants authorizing a peace officer to “use any device or investigative technique or procedure or do any thing described in the warrant” that would otherwise violate the Charter, subject to certain exceptions.<sup>16</sup>

In the case of video surveillance in circumstances where the target has a reasonable expectation of privacy, “general” or section 487.01 warrants can only be issued where there are reasonable grounds to believe the target has or is committing a Criminal Code offense listed in section 183 of the Code. To obtain a warrant, the police must meet the same tests they are required to meet to obtain a warrant to intercept private communications.<sup>17</sup>

### III. Access to Stored Communications

Section 487 of the Criminal Code allows law enforcement authorities to apply for search warrants to enter a building, receptacle, or place where there are reasonable grounds to believe that it has been used in the commission of an offense or holds evidence of the commission of an offense or the intention to commit an offense. Section 487(2.1) states as follows:

(2.1) A person authorized under this section to search a computer system in a building or place for data may

- (a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;
- (b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;
- (c) seize the print-out or other output for examination or copying; and
- (d) use or cause to be used any copying equipment at the place to make copies of the data.

Section 487.012 of the Criminal Code authorizes judges to order persons to produce data, or documents based upon data, to law enforcement officials. Before making such an order, a judge must be satisfied that there are reasonable grounds to believe that a criminal offense has been committed, the data will afford evidence of the offense, and the person who is the subject of the order has possession or control of the data. The order may contain any terms and conditions that the judge considers advisable in the circumstances, “including terms and conditions to protect a privileged communication between a lawyers and their client.”<sup>18</sup> In the event that the

---

<sup>14</sup> R. v. Wong, [1990] 3 S.C.R. 36, 60.

<sup>15</sup> Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, § 8, being Schedule B to the Canada Act, 1982, ch. 11 (U.K.), [http://laws-lois.justice.gc.ca/eng/charter/1.html#anchorbo-ga:l\\_I](http://laws-lois.justice.gc.ca/eng/charter/1.html#anchorbo-ga:l_I).

<sup>16</sup> Criminal Code, R.S.C. 1985, c. C-46, § 487.01, <http://laws-lois.justice.gc.ca/eng/C-46/page-10.html>.

<sup>17</sup> *Id.*

<sup>18</sup> *Id.* § 487.012(4).

target of the production order is a media outlet, the judge must employ a balancing test to weigh the importance of freedom of the press in a democratic society against the interests of justice.<sup>19</sup>

#### IV. Obligations on Service Providers

Despite several attempts by the last two Canadian governments to enact appropriate legislation, Canada still does not have laws imposing obligations on service providers. Previous attempts to enact such legislation were not approved by Parliament before it was either dissolved by a call for a general election or a session was closed. On October 29, 2010, the Minister of Justice introduced two new bills in the House of Commons that are designed to give law enforcement greater access to Internet data. The first of these, Bill C-51, would add the Investigative Powers for the 21st Century Act to the Criminal Code. That proposed Act provides for, among other matters,

- (1) new powers for judges and the police to make preservation demands and issue orders to compel providers to preserve electronic evidence;
- (2) new production orders to compel providers to produce data relating to the transmission of communications and the location of transactions, individuals, or things; and
- (3) the issuance of warrants “that will enable the tracking of transactions, individuals and things and that are subject to legal thresholds appropriate to the interests at stake.”<sup>20</sup>

The proposed Investigative Powers for the 21st Century Act would provide law enforcement agencies with specialized investigative powers that are designed to be particularly, but not exclusively, helpful in combating child sexual exploitation, organized crime, and terrorism. The Homeland Security Newswire (HSNW) states that the Act would assist in these activities because of the following:

- enabling police to identify all the network nodes and jurisdictions involved in the transmission of data and trace the communications back to a suspect. Judicial authorizations would be required to obtain transmission data, which provides information on the routing but does not include the content of a private communication;
- requiring a telecommunications service provider to temporarily keep data so that it is not lost or deleted in the time it takes law enforcement agencies to return with a search warrant or production order to obtain it;
- making it illegal to possess a computer virus for the purposes of committing an offence of mischief; and
- enhancing international cooperation to help in investigating and prosecuting crime that goes beyond Canada’s borders.<sup>21</sup>

---

<sup>19</sup> Canadian Broadcasting Corp. v. Manitoba (Attorney General), (2009) 1 W.W.R. 389 (Man. C.A.).

<sup>20</sup> Bill C-51, Summary, 40th Parl. 3d Sess., <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4745885&Language=e&Mode=1&File=27>.

The second bill would add the Investigating and Preventing Criminal Electronic Communications Act to the Criminal Code. The summary of Bill C-52 states as follows:

This enactment requires telecommunications service providers to put in place and maintain certain capabilities that facilitate the lawful interception of information transmitted by telecommunications and to provide basic information about their subscribers to the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Commissioner of Competition and any police service constituted under the laws of a province.<sup>22</sup>

The Homeland Security Newswire states as follows:

The Canadian government says that the Investigating and Preventing Criminal Electronic Communications Act would address challenges posed by today's technologies that did not exist when the legal framework for interception was updated nearly forty years ago. The Act would require service providers to include interception capability in their networks, thereby allowing law enforcement and national security agencies to execute authorizations for interception in a more timely and efficient manner with a warrant.<sup>23</sup>

Bills C-51 and C-52 have only received a first reading in the House of Commons. Before they can be signed into law, they will have to go through the normal legislative process of being read and approved three times in both the House of Commons and the Senate, as well as being studied by the appropriate committees, which usually recommend some changes to complex legislation. Concerns the government can expect to hear are whether the new laws would impose an undue burden on service providers and those related to privacy. Because the current Conservative government is a minority government, it will need the support of some opposition members to enact Bills C-51 and C-52.<sup>24</sup>

## V. Offenses, Penalties, and Defenses

Section 193 of the Criminal Code provides that everyone who willfully discloses an intercepted private communication without the express consent of the originator or of the person intended by the originator to receive it is guilty of an indictable offense and is liable to a term of imprisonment of up to two years.<sup>25</sup> There are a number of exceptions to this provision, including ones relating to

---

<sup>21</sup> *Canada Introduces Legislation to Fight Crime in Today's High-Tech World*, HSNW (Dec. 15, 2010), <http://homelandsecuritynewswire.net/canada-introduces-legislation-fight-crime-todays-high-tech-world>.

<sup>22</sup> Bill C-52, 40<sup>th</sup> Parl. 3d Sess. Summary, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4753163&Language=e&Mode=1&File=19>

<sup>23</sup> *Canada Introduces Legislation to Fight Crime in Today's High-Tech World*, *supra* note 21.

<sup>24</sup> *Privacy Advocates Concerned About Potential Internet Wiretapping Law*, CBC NEWS (Feb. 13, 2010), <http://www.cbc.ca/technology/story/2009/02/12/privacy-wiretap.html>.

<sup>25</sup> Criminal Code, R.S.C. 1985, c. C-46, § 193(1), *as amended*, <http://laws-lois.justice.gc.ca/eng/C-46/page-5.html>.

- (1) the giving of evidence in civil or criminal proceedings;
- (2) investigations where the interception was lawful;
- (3) the giving of notice to produce intercepted communications in legal proceedings;
- (4) disclosure by telecommunications operators for the purpose of protecting a computer system;
- (5) disclosures to peace officers made in the interests of the administration of justice in Canada or elsewhere; and
- (6) disclosures to the Canadian Security Intelligence Service for the purpose of enabling the Service to perform its duties combating terrorism and certain other activities against a state.<sup>26</sup>

There is also an exception for communications that have already been lawfully disclosed in the course of giving evidence.<sup>27</sup>

In addition to criminal penalties, a person who illegally discloses an intercepted private communication can be fined by a judge who convicts him or her. Section 194 of the Criminal Code states that a judge can impose an amount not exceeding Can\$5,000 (approximately US\$4,955) as punitive damages.<sup>28</sup>

## VI. Admissibility

Section 196 of the Criminal Code provides that a person whose private communications have been lawfully intercepted must be notified that he has been the target of an interception. Generally, the notification must be given within ninety days or by the end of the period allowed by the authorization unless another period is set by the court. The notice must be in writing, but details concerning the intercepted communication do not have to be divulged. Certification that notice has been given has to be filed with the court.

Section 196 allows judges to extend the notice period for up to three years before it has started to run; thereafter, it may be further extended by three-year periods. In order to grant such an extension, a judge must be satisfied that an investigation is continuing and the interests of justice warrant the extension. In cases involving investigations into criminal organizations or terrorism activities, a judge must only be satisfied that an extension would be in the interests of justice.<sup>29</sup>

---

<sup>26</sup> *Id.* § 193(2).

<sup>27</sup> *Id.* § 193(4).

<sup>28</sup> *Id.* § 194.

<sup>29</sup> *Id.* § 196.

Section 189 of the Criminal Code states that an intercepted private communication cannot be introduced into evidence against a person accused of an offense unless he or she has been given reasonable notice of that intention along with a transcript or statement setting out full particulars, and a statement respecting the time, place, and date of the private communication as well as the involved parties, if they are known.<sup>30</sup>

Prior to 1993, Canada had an automatic exclusionary rule for unlawfully intercepted private communications. However, in that year, the automatic exclusionary rule was repealed by an amendment, which did not create an alternative rule.<sup>31</sup> The result is that in deciding whether an illegally intercepted communication may be admitted in legal proceedings, a judge must rely on section 24(2) of the Canadian Charter of Rights and Freedoms and the jurisprudence that has developed under it. Section 24(2) of the Charter states as follows:

Where, in proceedings [to exclude evidence], a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.<sup>32</sup>

As has already been mentioned, section 8 of the Charter states that “everyone has the right to be secure against unreasonable search or seizure.”<sup>33</sup> It has been stated that “where private communications have been unlawfully intercepted then there will likely be a violation of s. 8 of the Charter.”<sup>34</sup> Thus, a section 24(2) analysis would likely be required in such cases. Generally, the courts have found that administrative or inadvertent errors will not bring the administration of justice into disrepute.<sup>35</sup> However, a willful violation of the authorization rules respecting the interception of private communications may well be viewed as a criminal invasion of the right to privacy. In such a case, the offense the accused is charged with committing might well have to be of a very serious or heinous nature in order for a judge to allow the illegally-obtained evidence to be admitted over his or her objection.

## VII. Conclusion

Although law enforcement can obtain authorizations to intercept private conversations in Canada where there are reasonable grounds to believe that they will provide evidence of the commission of a criminal offense, service providers are not under strict obligations to have the means for preserving data or to preserve data prior to being served with a production order. The

---

<sup>30</sup> *Id.* § 189(5).

<sup>31</sup> *Id.*, c. C-46, as amended by Criminal Law Amendment Act, 1993 S.C. ch. 40, § 10, <http://laws-lois.justice.gc.ca/eng/C-46/page-5.html>.

<sup>32</sup> Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, § 24(2), being Schedule B to the Canada Act, 1982, ch. 11 (U.K.), [http://laws-lois.justice.gc.ca/eng/charter/Charter\\_index.html](http://laws-lois.justice.gc.ca/eng/charter/Charter_index.html).

<sup>33</sup> *Id.* § 8.

<sup>34</sup> EDWARD GREENSPAN, MARTIN’S CRIMINAL CODE 2011 § 189 annots., at 380.

<sup>35</sup> *See id.*, § 24 annots., at 1797-1806.

government is trying to address this situation through Bills C-51 and C-52, which have both received a first reading in the House of Commons.

The failure to obtain judicial authorization for the interception of private communications is, except in limited circumstances, a criminal offense that is punishable with up to five years' imprisonment. Aggrieved parties can be awarded damages. The unauthorized disclosure of intercepted private communications are, again except in certain circumstances, a criminal offense and punishable with up to two years' imprisonment. Evidence obtained through the unlawful interception of a private communication can be excluded by a judge if he or she is of the opinion that its admission would bring the administration of justice into disrepute.

Prepared by Stephen F. Clarke  
Senior Foreign Law Specialist  
December 2010

**LAW LIBRARY OF CONGRESS**

**CHINA**

**PRIVACY OF ELECTRONIC COMMUNICATIONS**

*Executive Summary*

*Under Chinese law, freedom and privacy of correspondence is a constitutional right. The infringement of the freedom and privacy of others' correspondence, including emails, may be subject to criminal punishment, administrative penalties, and civil liability.*

*Government law enforcement organs, however, are generally exempted by these laws when censoring electronic communications in criminal investigations or for the needs of national security. Effective rules protecting individuals from unauthorized government access to their Internet communications are hard to find under Chinese law.*

**I. Introduction**

China does not have legislation protecting privacy in electronic communications similar to the Electronic Communications Privacy Act in the United States; nor has China provided clear rules on wiretapping or passed a comprehensive cybersecurity law. The legal system regulating the Internet is still developing. Furthermore, privacy—or to be more specific, an individual's personal privacy—is not an independent civil right clearly under the protection of Chinese civil law.

Provisions protecting Internet communications, and emails in particular, can be found in a number of laws and regulations. These provisions are primarily rooted in the constitutional right to freedom and privacy of correspondence. Government law enforcement organs, however, are generally exempted by these laws when censoring correspondence in criminal investigations and for the needs of national security.

**II. Freedom and Privacy of Correspondence in the Constitution**

The Chinese Constitution protects the “freedom and privacy of correspondence of citizens of the People's Republic of China.”<sup>1</sup> Article 40 of the Constitution states:

---

<sup>1</sup> XIANFA art. 40 (1982, last amended Mar. 14, 2004), available in English translation in 2004 LAWS OF PEOPLE'S REPUBLIC OF CHINA 59, 70 (Legislative Affairs Commission of the Standing Committee of the National People's Congress (NPC); Beijing, 2005) (hereafter LAWS OF CHINA).

The freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of state security or for investigation into criminal offences, public security or procuratorial organs<sup>2</sup> are permitted to censor correspondence in accordance with procedures prescribed by law.<sup>3</sup>

Thus, although the Constitution says that no organization or individual may on any ground infringe upon citizens' freedom and privacy of correspondence, it makes an exception for the public security and procuratorial organs, which may censor correspondence in accordance with the procedures prescribed by law for the needs of state security and for criminal investigations.

### III. Freedom and Privacy of Correspondence in Internet Communications

#### A. Criminal Law

To protect the constitutional right to freedom and privacy of correspondence, the Criminal Law criminalizes concealing, destroying, or unlawfully opening others' letters, which may result in up to one year of imprisonment.<sup>4</sup> If committed by postal office employees, such violations may result in up to two years' imprisonment.<sup>5</sup> Email and other Internet communications, however, are not clearly covered by these provisions.

The unlawful interception of personal emails and other electronic data is criminalized by a decision issued by the Standing Committee of the National People's Congress (NPC, China's top legislative body). On December 28, 2000, the NPC Standing Committee issued the *Decision of the NPC Standing Committee on Maintaining Internet Security*, which provides that "illegal interception, modification, and deletion of emails or other electronic data of others, infringing the freedom and secrets of communication of citizens thereby" are subject to criminal punishments.<sup>6</sup> The decision also subjects to criminal punishment the illegal interruption of a computer network or communications service without authorization, where the interruption causes a breakdown or malfunction of the computer network or communication system.<sup>7</sup> In addition, the decision states that the violators may also be subject to administrative punishment, or be liable under civil law.<sup>8</sup>

---

<sup>2</sup> "Procuratorial organs" refers to the Supreme People's Procuratorate and the local people's procuratorates. They are responsible for both prosecution and investigation in China.

<sup>3</sup> *Id.*

<sup>4</sup> Criminal Law art. 252, 1997 LAWS OF CHINA at 95.

<sup>5</sup> *Id.* art. 253.

<sup>6</sup> Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Weihu Hulianwang Anquan de Jueding [Decision of the Standing Committee of the National People's Congress (NPC) on Maintaining Internet Security] art. 4(2) (Dec. 28, 2000), 1 GAZETTE OF THE NPC STANDING COMMITTEE (2001) 18-19.

<sup>7</sup> *Id.* art. 1(3).

<sup>8</sup> *Id.* art. 6.

## B. Regulations on Telecommunication

The Regulations on Telecommunication promulgated by the State Council (China's cabinet) protects the freedom and privacy of using telecommunications services.<sup>9</sup> The Regulations prohibit telecommunications business operators and their staffs from providing user content transported by telecommunications networks to others without approval.<sup>10</sup> As in the Constitution, the public security public and procuratorial organs are expressly allowed to inspect telecommunications content as long as it is “for the purposes of state security or investigating criminal offenses according to proceedings as provided by laws.”<sup>11</sup>

“Telecommunication” under the Regulations refers to all activities of transmitting, transporting, or receiving sound, words, data, image, and other information through a wireless or cable electromagnetic system or photoelectric system.<sup>12</sup>

- *Measures for the Administration of Internet E-Mail Services*

Based on the authorization of the Regulations on Telecommunication, the Ministry of Information Industry (currently the Ministry of Industry and Information Technology, MIIT) issued *The Measures for the Administration of Internet Email Services*, which took effect on March 30, 2006.<sup>13</sup> The Measures specified the obligations of email service providers with regard to the rights of users, including:

- a. *Providing contents and rules of use:* The provider of Internet email services must clearly inform users of the contents of services and rules of use when providing services to users.<sup>14</sup>
- b. *Keeping confidential the personal registration information and Internet email address of users:* No provider of Internet email services or his employees may illegally use any users' personal registration information or Internet email address, or disclose any user's personal registration information or Internet email address, without the consent of the user, unless otherwise provided by law and administrative regulations.<sup>15</sup>

---

<sup>9</sup> Dianxin Tiaoli [Regulations of the People's Republic of China on Telecommunications] (promulgated by the State Council on Sept. 25, 2000), 2000 ZHONGHUA RENMIN GONGHEGUO FALU FAGUI HUIBIAN (FAGUI HUIBIAN) 799-819.

<sup>10</sup> *Id.* art. 66.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.* art. 2.

<sup>13</sup> Hulianwang Dianzi Youjian Fuwu Guanli Banfa [The Measures for the Administration of Internet Email Services] (issued by the Ministry of Information Industry on Feb. 20, 2006, effective Mar. 30, 2006), 2006 FAGUI HUIBIAN 814-17.

<sup>14</sup> *Id.* art. 8.

<sup>15</sup> *Id.* art. 9.

Email service providers who fail in meeting these obligations—in particular, by disclosing the users’ registration information and email address—are subject to administrative penalties of up to a RMB30,000 fine (about US\$4,500).<sup>16</sup>

### C. Regulations on Internet Security

In 1994, the State Council promulgated the thirty-one-article *Regulations on the Protection of the Security of the Computer Information System*. The Regulations gave the authority of protecting Internet security to the Ministry of Public Security (MPS).<sup>17</sup> The Ministry of State Security, the State Administration for the Protection of State Secrets, and other departments under the State Council may also be responsible for cybersecurity within their areas of responsibility.

The MPS then issued orders with regard to protecting Internet security, including the 1997 *Measures for Security Protection Administration of the International Networking of Computer Information Networks* (1997 Order). Although most of the 1997 Order’s provisions focus on censoring Internet content, it contains one provision on the protection of freedom and privacy of correspondence in Internet communications, prohibiting “any use of the Internet to infringe users’ freedom of communication and communication privacy.”<sup>18</sup> The 1997 Order also prohibits any use of the Internet to “endanger state security, divulge state secrets, infringe on national, social and collective interests and the legitimate rights and interests of citizens,” and “any other illegal and criminal activities.”<sup>19</sup>

The following activities are specifically prohibited by the 1997 Order as endangering Internet security:

- a. Access to computer information networks or the use of computer information network resources without permission;
- b. Deletion, revision, or addition of computer information network functions without permission;
- c. Deletion, revision, or addition of the data and applied procedures stored, processed, or transmitted on computer information networks without permission; and
- d. The deliberate production and spread of computer viruses and other disruptive programs.<sup>20</sup>

---

<sup>16</sup> *Id.* art. 22.

<sup>17</sup> Jisuanji Xinxi Xitong Anquan Baohu Tiaoli [Regulations on the Protection of the Security of the Computer Information System] (promulgated by the State Council on Feb. 18, 1994, effective on the same day), art. 6, 1994 FAGUI HUIBIAN 263-68.

<sup>18</sup> Jisuanji Xinxi Wangluo Guoji Lianwang Anquan Baohu Guanli Banfa [Measures for Security Protection Administration of the International Networking of Computer Information Networks] (issued by the Ministry of Public Security on Dec. 16, 1997, effective Dec. 20, 1997), art. 7, 1997 FAGUI HUIBIAN 389-95.

<sup>19</sup> *Id.* art. 4.

<sup>20</sup> *Id.* art. 6.

### III. Government Access to Private Internet Communications

While the law claims to protect Internet communications from private interference, effective rules protecting individuals from unauthorized government access to their electronic communications are hard to find. As discussed above, the law generally exempts law enforcement authorities, including the public security organs, the state security administration, and the procuratorial organs, from restrictions when they are censoring personal communications, including Internet communications, “for the needs of state security and criminal investigations.”<sup>21</sup> Since there are no strict rules requiring law enforcement personnel to prove the involvement of state security in a given case, and because criminal investigations are not limited by the type of the underlying crime(s), the exemption may inevitably be used arbitrarily by the law enforcement organs.

Furthermore, Internet rules even require service providers to assist the government in monitoring Internet communications. For example, *The Measures for the Administration of Internet Email Services* requires the provider of Internet email services to record the sending and receiving time of Internet emails sent or received via its email server, as well as the Internet email addresses and IP addresses of the senders and receivers. It also requires the record to be kept for sixty days and to be provided to the “relevant State organ” upon request, according to law.<sup>22</sup>

#### A. Wiretapping

Only a few general rules are available under Chinese law relevant to wiretapping, which allow the state security organs and public security organs to use “technological means of reconnaissance” “after going through strict approval procedures.”<sup>23</sup> Such “strict approval procedures,” however, have not been found in the procedure laws. They are very likely to be internal procedures; namely, upon the approval of certain higher ranking officers within the public security organs, procuratorial organs, and state security administration, wiretapping may be applied in an investigation without obtaining any search warrant from the court.

#### B. Seizure of Emails

The law does make it clear that in order to seize mail, telegraphs, and even emails in criminal investigations, investigators need only an approval from a public security organ or a procuratorate.

The Criminal Procedure Law, which was last amended in 1996 and does not mention email, provides that if the police deem it necessary to seize the mail or telegraph of a criminal

---

<sup>21</sup> XIANFA art. 40 (1982, last amended Mar. 14, 2004), 2007 LAWS OF CHINA 59, 70.

<sup>22</sup> *The Measures for the Administration of Internet Email Services*, *supra* note 13, art. 10.

<sup>23</sup> Baoshou Guojia Mimi Fa [State Security Law] (adopted by the NPC Standing Committee on Feb. 22, 1993, effective on the same day), art. 10, 1993 LAWS OF CHINA 43, 47. Renmin Jingcha Fa [People’s Police Law] (adopted by the NPC Standing Committee on Feb. 28, 1995, effective on the same day), art. 16, 1995 LAWS OF CHINA 101, 105.

suspect, they may, upon approval of a public security organ or a procuratorate, notify the post and telecommunications offices to check and hand over the relevant mail and telegrams.<sup>24</sup>

A set of MPS procedural rules clearly expands the coverage to the seizure of emails. *The Procedural Requirements of the Public Security Organs in Handling Criminal Cases* provides that the seizure of any mail, emails, or telegraphs of criminal suspects must be approved by a police officer in charge of a public security organ at the county level or above.<sup>25</sup>

Prepared by Laney Zhang  
Senior Foreign Law Specialist  
December 2010

---

<sup>24</sup> Xingshi Susong Fa [Criminal Procedure Law] (adopted by the NPC on July 1, 1979, amended Mar. 17, 1996), art. 116 (1), 1996 LAWS OF CHINA 63, 88.

<sup>25</sup> Gonggan Jiguan Banli Xingshi Anjian Chengxu Guiding [The Procedural Requirements of the Public Security Organs in Handling Criminal Cases] (passed by the MPS on Apr. 20, 1998, amendment effective Dec. 1, 2007), art. 215, MPS official website, <http://www.mps.gov.cn/n16/n1996048/n1996090/n1996180/2247345.html> (in Chinese; last visited Dec. 10, 2010).

**LAW LIBRARY OF CONGRESS**

**FRANCE**

**PRIVACY OF ELECTRONIC COMMUNICATIONS**

*Executive Summary*

*French law guarantees the confidentiality of electronic communications but allows for the interception of communications in specific cases. In matters of public security, interceptions are authorized in exceptional circumstances and for the purpose of gathering information concerning national security, protecting France's essential scientific and economic information, preventing terrorism or organized crime, or ending the reconstitution or maintenance of unlawful paramilitary groups. These interceptions are authorized by the Prime Minister. Judicial interceptions are allowed during a criminal investigation when the penalties to be incurred are equal to or greater than two years of imprisonment, for researching cause of death or suspicious disappearances and researching fugitives and organized crime. As a general rule service providers must erase or render anonymous any data relative to electronic communications traffic. There are several exceptions to the rule for purposes of the investigation and prosecution of criminal offenses, and to ensure the security of networks. Service providers are also required to give assistance and to ensure that interception capability has been installed.*

**I. General Overview**

Law No. 91-646 of July 10, 1991, on the Secrecy of Electronic Communications, as amended, guarantees the confidentiality of electronic communications but allows for the interception of communications for public security reasons or for the detection and investigation of crimes.<sup>1</sup> The term “electronic communications” is defined broadly to include a very wide range of transmissions through modern technologies, including telephone, facsimile, telex, and computer, and concerns all modes of interception.<sup>2</sup>

The conditions for interception differ depending on whether it is authorized for security reasons (administrative interception), in the course of a criminal investigation (judicial interception), or for other reasons. Provisions regarding judicial interceptions have been

---

<sup>1</sup> Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques modifiée par la Loi 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle [Law No. 91-646 of July 10, 1991, relating to the Secrecy of Electronic Communications as amended by Law 2004-669 of July 2004, on Electronic Communications], LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les textes législatifs et réglementaires) (consolidated version).

<sup>2</sup> Pascal Dourneau-Josette, *Ecoutes téléphoniques judiciaires*, in III RÉPERTOIRE DE DROIT PÉNAL ET DE PROCÉDURE PÉNALE §§ 30–32 (Daloz 2010).

incorporated into the Code of Criminal Procedure. Below is a chart that summarizes the different types of interceptions. Each of them is reviewed in detail in the discussion which follows.

Type of Interceptions	Authority	Grounds	Duration	Renewal
Security (administrative)	Prime Minister (Law No. 91-646 of July 10, 1991, art. 3)	Prevention: - Terrorism - Organized crime - National security - Economic Protection - Reconstitution of banned militia or paramilitary groups	4 months	No limitation
Judicial	Investigation judge (C. PR. PÉN. art 100)	Offenses punishable by at least two years' imprisonment	4 months	No limitation
	Investigation judge (C. PR. PÉN. art. 80-4)	Research of cause of death or suspicious disappearances	2 months	No limitation
	Prosecutor under the authority of the Judge of Liberty and Detention (C. PR. PÉN. arts. 74-2, 695-36, and 696-21)	Research of fugitives	2 months	Renewable three times for <i>délits</i> (serious offenses) and without limitation for <i>crimes</i> (most serious offenses such as murder)
	Prosecutor under the authority of the Judge of Liberty and Detention (C. PR. PÉN. art. 706-95)	Organized crime	15 days	Renewable once
Others	Penitentiary administration under the supervision of the Public Prosecutor (C. PR. PÉN. art 727-1)	Prevention of escape and prison security	Duration of detention	Not applicable

## II. Administrative Interceptions

In matters of public security, the law provides that interception of electronic communications is allowed only in exceptional circumstances and for the purpose of gathering information concerning national security, protecting France's essential scientific and economic information, preventing terrorism or organized crime, or ending the reconstitution or maintenance of unlawful paramilitary groups or militia.<sup>3</sup>

An interception is authorized by a written decision of the Prime Minister or the Minister's representatives at the request of the Defense Minister, the Interior Minister, the Minister in charge of customs, or any of these Ministers' representatives.<sup>4</sup> The number of interceptions susceptible to take place simultaneously is also decided by the Prime Minister.<sup>5</sup>

The Prime Minister's decision must specify the grounds for the authorization. The interception may last for a maximum of four months. It can be renewed under the same conditions and procedure.<sup>6</sup> Only obtained information that relates to the security objectives can be transcribed. The recording is destroyed within ten days,<sup>7</sup> while the transcripts must be destroyed as soon as they are dispensable.<sup>8</sup> A written report of the destruction must be drafted.<sup>9</sup>

An independent national commission, the National Commission for the Monitoring of Security Interceptions (*Commission nationale de contrôle des interceptions de sécurité*), monitors the application of these rules.<sup>10</sup> The Commission is chaired by a person appointed for six years by the President of the Republic. In addition, it comprises one member of the Senate and one member of the National Assembly.<sup>11</sup>

The Commission must be notified of the Prime Minister's decision to intercept electronic communications within forty-eight hours. If the president of the Commission estimates that the decision is unlawful, he convenes the Commission, which must rule within seven days.<sup>12</sup> The Commission may, on its own initiative, check on any security interceptions.<sup>13</sup> If the interception is found to be unlawful the Commission recommends its immediate termination.<sup>14</sup> The

---

<sup>3</sup> Law No. 91-646 of July 10, 1991, art. 3.

<sup>4</sup> *Id.* art. 4.

<sup>5</sup> *Id.* art. 5.

<sup>6</sup> *Id.* art. 6.

<sup>7</sup> *Id.* art. 9.

<sup>8</sup> *Id.* art. 12.

<sup>9</sup> *Id.*

<sup>10</sup> *Id.* art. 13.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.* art. 14.

<sup>13</sup> *Id.* art. 15.

<sup>14</sup> *Id.*

Commission will verify the grounds and justifications of the interception request. It ensures that it respects the principle of proportionality between the goal to be achieved and the measure to be taken.<sup>15</sup>

The Minister in charge of electronic communications ensures that service providers of such communications comply with the Prime Minister's interception requests.<sup>16</sup> These providers are required to provide any information or documents that are necessary to the implementation and exploitation of the authorized interception.<sup>17</sup> Individuals or legal entities providing cryptology services to ensure the confidentiality of information are required to give authorized agents the keys permitting the encoded data to be deciphered.<sup>18</sup> Finally, a decree provides for the remuneration of electronic communication providers that were asked to implement interceptions for public security reasons.<sup>19</sup>

The 2009 report prepared by the Commission shows that 5,117 requests for interception based on security were issued in 2009 (3,176 new requests and 1,941 renewals).<sup>20</sup> The Commission gave negative opinions for 88 of the new requests. The Prime Minister followed the Commission's recommendation in 87 of the cases. Fifty-nine percent of the new requests concerned the prevention of crimes and organized crime, 22.5 percent terrorism, and 17.5 percent national security.

### III. Judicial Interception

#### A. Offenses Punishable By a Minimum of Two Years' Imprisonment

Interception, recording, and transcription of electronic communications may be allowed during a criminal investigation when the penalties to be incurred are equal to or greater than two years of imprisonment.<sup>21</sup> The Investigating Judge in charge of the case may authorize such interception. He directs the entire investigation, overseeing the legality of the evidence and requesting the services of the police where needed.<sup>22</sup> The authorization must be in writing and

---

<sup>15</sup> Commission nationale de contrôle des interceptions de sécurité, 18<sup>th</sup> Activity Report, 2009, at 16, LA DOCUMENTATION FRANÇAISE, <http://www.ladocumentationfrancaise.fr/rapports-publics/104000489/index.shtml>.

<sup>16</sup> Law No. 91-646 of July 10, 1991, art. 21, *as amended*, LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les textes législatifs et réglementaires).

<sup>17</sup> *Id.* art. 22.

<sup>18</sup> *Id.* art. 11-1.

<sup>19</sup> Décret 2007-1519 du 22 octobre 2007 portant modification du code des postes et des communications électroniques et relatif à la tarification des interceptions de communications électroniques [Decree 2007-1519 on remuneration of electronic communication interceptions], LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les textes législatifs et réglementaires).

<sup>20</sup> Commission nationale de contrôle des interceptions de sécurité, *supra* note 15, at 17.

<sup>21</sup> CODE DE PROCEDURE PENALE [C. PR. PÉN.] art. 100 (Daloz 2011).

<sup>22</sup> *Id.* art. 100.

cannot be appealed. The decision must include all elements relating to the communication to be intercepted, the offense that warrants the interception, and its duration.<sup>23</sup>

Authorized interceptions can last for a maximum of four months. The authorization can be renewed for an additional four months under the same procedure and conditions.<sup>24</sup> Only the information useful to the investigation can be transcribed. It is destroyed at the expiration of the statute of limitations on the order of the Public Prosecutor.<sup>25</sup>

The Investigating Judge may requisition any agent placed under the authority of the Minister in charge of telecommunication or any qualified agent of a provider of telecommunications services to set up the interception device or system.<sup>26</sup>

Interception of an attorney's communications taking place in his office or residence cannot be conducted without first informing the local bar president. It can be done only if there is an indication that the attorney is participating in the commission of a criminal offense.<sup>27</sup> Communications of an attorney relating to the right of the defense cannot be transcribed. No interception of communication of a senator or deputy can be made without first notifying the respective presidents of these chambers.<sup>28</sup> Finally, the communications of a journalist revealing the identity of his/her sources cannot be transcribed.<sup>29</sup>

## **B. Research of Cause of Death or Suspicious Disappearances**

Interceptions of electronic communications are ordered by the Investigating Judge during the course of an investigation under the same procedure and conditions described in the previous section, to research the cause of death of an individual or to try to locate a missing person who disappeared under suspicious circumstances.<sup>30</sup> The initial length of the interception is two months and it is renewable. If the person who disappeared is found, his/her address may only be disclosed to his/her family after that person agrees. The Investigating Judge needs to agree to the release of that information if the person is a minor.<sup>31</sup>

## **C. Research of Fugitives**

The persons concerned are those against whom an arrest warrant has been issued. In such cases and for the necessity of the inquiry related to researching such persons, the Public

---

<sup>23</sup> *Id.* art. 100-1

<sup>24</sup> *Id.* art. 100-2.

<sup>25</sup> *Id.* art. 100-6.

<sup>26</sup> *Id.* art. 100-3.

<sup>27</sup> *Id.* art. 100-7.

<sup>28</sup> *Id.*

<sup>29</sup> *Id.* art. 100-5.

<sup>30</sup> *Id.* art. 80-4.

<sup>31</sup> *Id.*

Prosecutor may ask the Judge of Liberty and Detention to authorize interception, recording, and transcription of electronic communications. The initial maximum duration is two months, renewable three times for *délits* (serious offenses) and without limitation for *crimes* (most serious offenses such as murder).<sup>32</sup>

#### D. Organized Crime

Where the offenses committed relate to organized crime, the Judge of Liberty and Detention may order the interception at the stage of the police preliminary investigation. The initial maximum duration is two weeks and it may be extended once.<sup>33</sup>

#### E. Admissibility of Evidence

According to French criminal procedure, offenses may be proven by any mode of evidence and the judge determines culpability according to his/her inner conviction.<sup>34</sup> Respect for the specific procedures for obtaining electronic communications and for the prescribed conditions of their storage is usually sufficient to establish the criminal activities.<sup>35</sup>

If unlawfully obtained, the evidence may be nullified.<sup>36</sup> France deals with the issue of illegally or improperly obtained evidence under the rubric *nullités de procédure*. The French theory is that the rules governing the gathering of evidence are procedural rules, and certain serious breaches of these rules render the operation null and void.<sup>37</sup> Nullity of a police act, for example, may arise either from a statute expressly stating that breach of the rule in question will result in rendering the act null and void, or, where the statute is silent as to the consequences of its infringement, from a court decision.<sup>38</sup> The court must look at whether the rule is sufficiently important to justify nullity for its breach and whether the breach has harmed the interest of the party challenging its breach.<sup>39</sup>

---

<sup>32</sup> *Id.* art. 74-2.

<sup>33</sup> *Id.* art. 706-95.

<sup>34</sup> *Id.* art. 427.

<sup>35</sup> David Chilstein, *Législation sur la cybercriminalité en France*, REVUE INTERNATIONALE DE DROIT COMPARÉ, RIDC, 2010-2, at 589.

<sup>36</sup> Muriel Guerin, *Nullités de Procédure*, in RÉPERTOIRE DE DROIT PÉNAL ET DE PROCÉDURE PÉNALE §§ 31–33 (Dalloz 2010).

<sup>37</sup> MIREILLE DELMAS-MARTY & J. R. SPENCER, EUROPEAN CRIMINAL PROCEDURES 605 (Cambridge University Press, 2002).

<sup>38</sup> *Id.* at 606.

<sup>39</sup> C. PR. PÉN. art. 802. Article 802 provides:

In case of the disregard of formalities prescribed by law under penalty of nullity or of nonobservance of substantial formalities, any court, the Court of Cassation included, which has to rule on an application for annulment, or which raises such an irregularity on its own motion, may pronounce the nullity only where this has had the effect of harming the interests of the party concerned. (Translation by the author, N.A.)

#### IV. Obligations on Service Providers

The general principle is that service providers of electronic communications must erase or render anonymous any data relative to the traffic of these communications. There are several exceptions to the rule for the purpose of investigating and prosecuting criminal offenses, and to ensure the security of networks.<sup>40</sup> Data may be retained for up to a year where needed for criminal investigations and for three months for network security purposes.<sup>41</sup>

Law 2006-64 of January 23, 2006, on the fight against terrorism, specifically empowered police officers to require the communication of certain data from Internet providers without any authorization from the Public Prosecutor. This provision was incorporated in the Postal and Electronic Communication Code.<sup>42</sup> Internet providers may also be required by these police officers to keep the data for one year.<sup>43</sup> The police officers must state the grounds for their requests in writing. These requests are reviewed by a qualified person appointed for three years by the National Commission for the Monitoring of Security Interceptions. This Commission may verify the officer's requests at any time and notify the Ministry of Interior of any violation of individuals' rights and liberties.<sup>44</sup>

The Law has further extended the scope of telecommunications data retention, as the obligation to retain data, when it comes to Internet providers, now also applies to Internet cafes, hotels, restaurants, and, more generally, to any person or organization providing Internet access as a main or side activity.<sup>45</sup>

The list of the types of data that must be retained was published in an implementing decree.<sup>46</sup> Relevant data identifies the user and his or her terminal equipment; the recipient of the communication; the date, time, and duration of the communication; the additional services used and the suppliers; and, for telephone services, the origin and location of the communication.<sup>47</sup>

A 2009 report prepared by the National Commission for the Monitoring of Security Interceptions shows that in 2009, police officers presented 43,559 requests to the qualified

---

<sup>40</sup> *Id.*

<sup>41</sup> CODE DES POSTES ET DES TELECOMMUNICATIONS ÉLECTRONIQUES art. L.34-1-1, LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les Codes).

<sup>42</sup> Loi 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers [Law 2006-64 on Combating Terrorism and on Various Provisions Concerning Security and Borders Controls] art. 7, LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les textes législatifs et réglementaires).

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.* arts. 5, 6.

<sup>46</sup> Décret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques [Decree 2006-358 of Mar. 24, 2006 on the Retention of Telecommunication Data], LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les textes législatifs et réglementaires).

<sup>47</sup> *Id.* art. 1.

person appointed by the Commission. Of those requests, 39,070 were deemed valid, 30 were refused, and 4,459 were sent back to the requesting services for additional information.<sup>48</sup>

## V. Offenses and Penalties

### A. Violation of Confidentiality of Correspondence

The Penal Code provides:

Except where provided otherwise by law, the ordering, committing or facilitating of the misappropriation, suppression or opening of correspondence, and the disclosure of the contents of such correspondence, by a person holding public authority or charged with a public service mission acting in the course of or on the occasion of his office or duty, is punished by three years of imprisonment and a fine of €45,000.

The same penalties apply to the persons referred to under the previous paragraph, or to employees of an electronic communication network open to the public, or to employees of a provider of telecommunications services, who, acting in the performance of their functions, order, commit, or facilitate, except where provided for by law, any interception or misappropriation of correspondence sent, transmitted, or received by a means of telecommunication, or the use or the disclosure of its contents.<sup>49</sup>

### B. Revealing the Existence of a Lawful Interception

Any person who participates in the implementation of a decision ordering the interception of electronic communications and who reveals the existence of such interception is punishable for violating professional confidentiality, for a maximum of one year's imprisonment and a €15,000 fine.<sup>50</sup>

### C. Service Providers

A service provider's violation of its obligation to either erase or render anonymous data relative to electronic communications traffic or to conserve certain data as required by law is punishable by one year of imprisonment and a €75,000 fine.<sup>51</sup>

A service provider's refusal to provide any information or documents necessary to the implementation and exploitation of an authorized interception, or providing erroneous information, is punishable by six month's imprisonment and a €7500 fine.<sup>52</sup>

---

<sup>48</sup> Commission nationale de contrôle des interceptions de sécurité, *supra* note 15, at 31.

<sup>49</sup> CODE PÉNAL art. 432-9 (translation by the author, N.A.). Currently, €1 is equal to US\$1.32.

<sup>50</sup> Law No. 91-646 of July 10, 1991, art. 26, *as amended*, LEGIFRANCE, <http://www.legifrance.gouv.fr/> (File: Les textes législatifs et réglementaires).

<sup>51</sup> CODE DES POSTES ET DES TELECOMMUNICATIONS ÉLECTRONIQUES art. L39-3.

<sup>52</sup> *Id.* art. 22.

The refusal to provide cryptology keys to an empowered authority in order to allow it to proceed with a lawful interception is punishable by two years of imprisonment and a €30,000 fine.<sup>53</sup>

## VI. Pending Legislation

The Draft Law for the Programming and Performance of Internal Security would allow police investigators to see and record in real time, from a distance, the data that appears on a computer screen, even when the data is not stored. If passed, the law would allow the state to install software that can observe, collect, record, save, and transmit keystrokes from the computers on which it is installed. The measure could only be done upon authorization by an Investigating Judge and after consultation with the Public Prosecutor. It could only be ordered to fight organized crime. The duration of the measure would be four months. The Investigating Judge could renew it once for an additional four months.<sup>54</sup>

The National Assembly adopted the draft law on a first reading on February 16, 2010. The Senate adopted a different version on September 10, 2010, and sent it back to the National Assembly on September 13, 2010. Both versions need to be reconciled. The version adopted by the National Assembly will prevail if no reconciliation can be reached.

Prepared by Nicole Atwill  
Senior Foreign Law Specialist  
December 2010

---

<sup>53</sup> *Id.* art. 11-1.

<sup>54</sup> Assemblée Nationale, *Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure*, art. 22, available at <http://www.assemblee-nationale.fr/13/ta/ta0417.asp>.

## LAW LIBRARY OF CONGRESS

### ISRAEL

## PRIVACY OF ELECTRONIC COMMUNICATIONS

### *Executive Summary*

*Infringement of a person's privacy by intercepting, surveilling, or using his electronically stored communications without his consent is prohibited in Israel in the absence of specific permits granted in accordance with the law. Permits may be granted by the president of a district court or his designated deputy to law enforcement officers for crime prevention and identification of offenders, as well as to special intelligence unit officers in the Israel Defense Forces and the General Security Service for reasons of state security. The release of telecommunications data by service providers is regulated by law and requires similar justifications for a judicial order. Data retrieved from service providers must be limited to location, information regarding subscribers, and traffic; it does not extend to the content of communications. Such data may be maintained in the police database for identification of telecommunications and is available to designated police officers.*

### **I. Electronic Communications Privacy and Access to Stored Communications**

The Privacy Protection Law, 5741-1981,<sup>1</sup> as amended, prohibits infringement of a person's privacy by copying or using the content of any writing without the permission of either the author or the addressee. This prohibition applies to electronic and non-electronic writings alike, unless the writing is of historic value or fifteen years have passed since it was made.<sup>2</sup> For the purpose of privacy protection, an electronic message is defined as “[i]nformation created, sent, received or deleted by electronic or optic means, when it is viewed, read, heard or retrieved by such means.”<sup>3</sup>

The Law also extends privacy protection to information preserved in databases relating to sensitive information, information regarding persons that was collected without their knowledge or consent, or a group exceeding 10,000 persons.<sup>4</sup> Privacy protection similarly applies to databases held by governmental, local, and other bodies by law or by a Minister of Justice decree approved by the Knesset's Constitution, Law and Justice Committee.<sup>5</sup>

---

<sup>1</sup> Privacy Protection Law, 5741-1981, 35 LAWS OF THE STATE OF ISRAEL [LSI] 5741 (1980/81).

<sup>2</sup> *Id.* § 2(5).

<sup>3</sup> *Id.* (applying the definition provided by the Electronic Signature Law, 5761-2001, SEFER HAHUKIM [SH] 5761 No. 1785 p. 210).

<sup>4</sup> *Id.* § 8.

<sup>5</sup> See Freedom of Information Act 5758-1998, §§ 1, 2, 9(3), SH 5759 No. 1667 p. 226, *as amended*.

The Law exempts from criminal and civil liability privacy violations caused by persons engaged in actions authorized by law, or by persons acting on behalf of the Israel Police, Israel Defense Forces (IDF) Intelligence Division, the General Security Service, the *Mossad* (Israel's intelligence agency), and the Witness Protection Agency, as long as the violation occurred in a reasonable manner and in the course and for the furtherance of their duties.<sup>6</sup> Special rules also apply to the transfer of information, including digital information, between public agencies.<sup>7</sup>

## II. Monitoring of Electronic Communications

### A. Offenses and Penalties

The Secret Monitoring Law, 5739-1979, as amended, prohibits unauthorized secret monitoring of electronic communications.<sup>8</sup> A “secret monitoring” is defined as “monitoring without the consent of either party to the conversation.”<sup>9</sup>

The law prohibits an unauthorized installation of secret monitoring devices, unauthorized secret monitoring, and the use of any information derived from such monitoring. Violation of any of these prohibitions is punishable by five years' imprisonment.<sup>10</sup> Private investigators who are convicted of any of these offenses may, in addition, lose their license to maintain an office for private investigation for a period of up to seven years.<sup>11</sup>

### B. Types of Communications Interception Requiring Permits

The protection against secret monitoring under the Secret Monitoring Law, 5739-1979, as amended, applies to “a conversation” and includes “communication among computers.”<sup>12</sup> It also applies to data derived from databases held by licensed telecommunications service providers concerning location, subscribers, and traffic information, but excluding the subject content of communications.<sup>13</sup>

### C. Authorized Exceptions

The following exceptions from the Secret Monitoring Law may be authorized:

---

<sup>6</sup> Privacy Protection Law § 19.

<sup>7</sup> *Id.* ch. D.

<sup>8</sup> Secret Monitoring Law, 5739-1979, 33 LSI 141 (5739-1978/79).

<sup>9</sup> *Id.* § 1.

<sup>10</sup> *Id.* § 2.

<sup>11</sup> *Id.* § 2A.

<sup>12</sup> Secret Monitoring Law § 1.

<sup>13</sup> *Id.* § 9C (referring to the Criminal Procedure (Enforcement Authorities-Telecommunications Data) Law 5768-2007, SH 5758 No. 2122 p. 72).

- Exceptions for Law Enforcement

The law authorizes high-ranking police officers to review information derived from unauthorized secret monitoring for the purpose of enforcement of the Secret Monitoring Law, to the extent not exceeding what is necessary.<sup>14</sup> The law further authorizes prosecutors or chief investigators to review or use such information, as long as this is done for the purpose of preventing or investigating serious crimes or any crimes involving special reasons, or based on the public interest.<sup>15</sup> This authorization will not apply to secret monitoring performed unlawfully by a person who was authorized to obtain a permit, unless it was done in good-faith error and pursuant to what was perceived as legal authority.<sup>16</sup>

- Exceptions for State Security

The law authorizes the Prime Minister or the Minister of Defense, upon a written request by the IDF Intelligence Division or the General Security Service (hereafter Head of a Security Agency), to authorize secret monitoring after considering the extent of harm to privacy and determining that monitoring is necessary for state security. Authorization for this purpose must be in writing and must include specific identifying information concerning the subject, location, and methods of monitoring. The authorization is valid for a period not exceeding three months and may be extended periodically.<sup>17</sup>

The grant or extension of authorization for secret monitoring for state security reasons must be immediately reported by the Minister of Defense to the Prime Minister, and by both on an annual basis to the joint Knesset (Parliament) Constitution, Law and Justice, and Foreign Affairs and Defense Committees, who then conduct hearings on this issue behind closed doors.<sup>18</sup>

The law further authorizes the Prime Minister or the Minister of Defense, upon a request by the Head of a Security Agency to authorize the secret monitoring of the conversations of a defense authorities employee in order to identify or prevent the leaking of security information that may cause serious harm to state security. This type of authorization is to be provided in writing for a period not to exceed fifteen days, which may be extended, and must be carried out in accordance with the rules determined by the Minister of Defense after consultation with the Minister of Justice.<sup>19</sup>

The Head of a Defense Agency is also authorized, in urgent situations, to issue proactive and retrospective authorization for secret monitoring for a period not to exceed forty-eight hours.

---

<sup>14</sup> Secret Monitoring Law § 2B(a).

<sup>15</sup> *Id.* § 2B(b).

<sup>16</sup> *Id.* § 2B(d).

<sup>17</sup> *Id.* ch. B, § 4.

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* § 4A.

Such authorization must be in writing and must be immediately reported to the Prime Minister or the Minister of Defense.<sup>20</sup>

- Exceptions for Prevention of Offenses and Identification of Offenders

The president of a district court or his designated deputy may issue a decree authorizing secret monitoring if he is convinced, after having evaluated the level of harm to privacy, that it is necessary for the disclosure, investigation, or prevention of serious crimes; the disclosure or arrest of the perpetrators; or for forfeiture of property related to such crimes. Authorization granted under these conditions may not exceed three months and may be periodically extended.<sup>21</sup>

The General Chief of Police must provide a monthly report to the Attorney General on the number of permits granted that authorize secret monitoring. The Minister of Police must provide an annual report on the number of requests and permits granted under these conditions to the Knesset's Constitution, Law and Justice Committee.<sup>22</sup>

Similarly to permits granted based on state security, permits and retroactive authorizations for crime prevention and the identification of offenders may be granted on an expedited basis under similar conditions.<sup>23</sup>

Special rules apply to conversations legally intercepted for the purpose of crime prevention and the identification of offenders that involve Knesset members (KMs). Monitoring must stop immediately upon recognizing that the conversation involves a KM, and the information already retrieved must be transferred for review by the judge who authorized the monitoring, for a determination of whether the need for disclosure exceeds the possible harm to the ability of the KM to perform his job, and for a decision concerning the methods for dealing with the information retrieved by the monitoring.

- Other Exceptions

The monitoring of conversations in the “public domain” does not require a permit if it is done:

- (1) by the Head of a Security Agency for reasons of state security;
- (2) by a person authorized by an authorized police officer for preventing offenses or identifying offenders; or
- (3) by chance and in good faith, in the process of open recording that was designed for public publication or research.<sup>24</sup>

---

<sup>20</sup> *Id.* § 5.

<sup>21</sup> *Id.* § 6.

<sup>22</sup> *Id.*

<sup>23</sup> *Id.* § 7.

<sup>24</sup> *Id.* § 8(1).

For the purpose of this exception, “public domain” includes a place where a reasonable person could anticipate that his conversations may be heard without his consent, as well as a place where a prisoner or a detainee is held.<sup>25</sup>

Additional exceptions from permit requirements apply to the monitoring of international conversations for military censorship, the monitoring of conversations that utilize telecommunications systems used by the IDF or Israel Police, the monitoring of service by employees of the Ministry of Telecommunication or license holders, and monitoring within radio and public broadcasts.<sup>26</sup>

#### **D. Privileged Conversations**

Privileged conversations cannot be monitored unless permitted by a decree issued by the president of a district court or his designated deputy, and are only allowed if the district court president or his designee is convinced that there is a basis to suspect that an attorney, a physician, a psychologist, a social worker, or a religious leader was involved in an offense and the following conditions are met:

- (1) A request for monitoring was made in writing by the Head of a Security Agency, when the offense is classified as crime that may harm state security and secret monitoring is necessary for reasons of state security;
- (2) A request for monitoring was made in writing by an authorized police officer, when the offense is murder, manslaughter, an offense endangering state security, a drug offense, or conspiracy to commit any of these offenses, and secret monitoring is necessary for the prevention and investigation of the offense.<sup>27</sup>

A request for secret monitoring of privileged conversation must be submitted for the approval of the Attorney General or the State Attorney. The law provides special arrangements for the recording and review of information retrieved in connection with monitoring requested by an authorized police officer.<sup>28</sup>

### **III. Admissibility of Information Retrieved from Unauthorized Secret Monitoring**

The law provides that information retrieved by secret monitoring in violation of the provisions of the Secret Monitoring Law or in violation of KMs’ parliamentary immunity is not admissible in court, except:

- (1) In a criminal process for an offense under the Secret Monitoring Law; or
- (2) In a criminal process for a serious crime, if the court has ordered that it would be admissible after having been convinced, for special reasons that must be cited, that

---

<sup>25</sup> *Id.*

<sup>26</sup> *Id.* § 8(2)-(5).

<sup>27</sup> *Id.* § 9A.

<sup>28</sup> *Id.*

in the circumstances of the matter the need to reach the truth is greater than the need to protect privacy.<sup>29</sup>

Secret monitoring performed unlawfully by a person who is authorized to obtain a permit for it is not admissible, unless conducted as the result of a good-faith error in the course of using what appeared to be a legal authorization.

The law contains specific rules on the procedure and criteria for the evaluation of requests for determinations of admissibility of such evidence.<sup>30</sup>

#### **IV. Release of Telecommunications Data by Service Providers and Access to Police Databases**

##### **A. Conditions for Granting Release Orders**

Licensed telecommunications service providers may be ordered to release telecommunications data pursuant to an order issued by a circuit court decree if the court was convinced that the disclosure is necessary for the following objectives, as long as it does not harm a person's privacy in a way that exceeds what is necessary:

- (1) Saving or protecting human life;
- (2) Disclosure, investigation, or prevention of offenses;
- (3) Identification and prosecution of offenders; and
- (4) Forfeiture of property by law.<sup>31</sup>

Based on the above, the release of telecommunications data may only be ordered in the context of a criminal investigation, or for crime prevention and property forfeiture, and not for the purpose of civil lawsuits. In a leading decision rendered in March 2010 the Supreme Court rejected a request to force the respondent, an Internet service provider, to reveal the Internet protocol (IP) address that accompanied anonymous talk-back messages published in an Internet forum in order to enable the plaintiff to identify the authors for the purpose of a civil action for slander.<sup>32</sup>

The Court held that the right to anonymity was based on the fundamental rights of freedom of expression and privacy. The Court further recognized that anonymity in the Internet era enjoys double importance by constituting a clear democratic means for promoting the principle of equality. The Court also recognized the right of a person to his dignity and to be

---

<sup>29</sup> *Id.* § 13.

<sup>30</sup> *Id.*

<sup>31</sup> Criminal Procedure (Enforcement Authorities-Telecommunications Data) Law 5768-2007, § 3(A), SH 5758 No. 2122 p. 72.

<sup>32</sup> Request for Civil Appeal 4447/07 Mor v. Barak, <http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.pdf> (in Hebrew; last visited Dec. 7, 2010).

protected from slander. The Court held, however, that although Israel's criminal law provides easy and quick ways to verify information regarding anonymous surfers, it did not provide any legislative remedy in civil proceedings and the Court was not willing to recognize any such remedies. In view of the serious constitutional implications of harming surfers' anonymity, the Court called for the legislature to regulate this area.<sup>33</sup>

In a published comment analyzing the decision, an Israeli cyberlaw expert noted that the Electronic Trade Law Bill was introduced a few years ago and that this bill included a process for the disclosure of data regarding persons responsible for torts. He opined, however, that the delay in legislative regulation of the disclosure of surfers' IP addresses in the context of civil lawsuits was due to policy disagreements regarding voluntary Internet surfing at the Ministry of Justice.<sup>34</sup>

### **B. Data Disclosures to Law Enforcement by Service Providers**

Telecommunications data disclosures that may be authorized by the circuit court are restricted to data concerning location, subscribers, and traffic, but does not extend to the content of communications.<sup>35</sup>

The law regulates the content of requests for disclosure, as well as for the transfer and preservation of data retrieved by such disclosure, in confidential databases maintained by the police.<sup>36</sup> The law further authorizes the reimbursement of telecommunications licensees for expenses incurred by the transfer of data files to authorities.<sup>37</sup>

### **C. Service Providers' Confidentiality Duties**

The law prohibits telecommunications service providers from disclosing to a subscriber or any other person information on the transfer of telecommunications data based on a request by the police or another investigative authority authorized by law, in the absence of permission to do as granted by a court.<sup>38</sup>

Reports on the number of requests, their objectives, offenses for which disclosure was requested, types of data requested, and other information must be submitted by the relevant Minister to the Knesset's Constitution, Law and Justice Committee on an annual basis.<sup>39</sup>

---

<sup>33</sup> *Id.*

<sup>34</sup> Haim Ravia, Adv., *Stopping and a Dangerous Opening*, LAW.CO.IL (Apr. 3, 2010), <http://www.law.co.il/articles/isp-liability/2010/04/03/anonymity-as-a-constitutional-right-in-mor-v-barak/> (in Hebrew).

<sup>35</sup> *Id.* § 9C (referring to the Criminal Procedure (Enforcement Authorities-Telecommunications Data) Law).

<sup>36</sup> Criminal Procedure (Enforcement Authorities-Telecommunications) (Database of Identification of Telecommunications) Regulations 5769-2008, KOVETZ HATAKANOT [KT] 5769 No. 6735 p. 270.

<sup>37</sup> Criminal Procedure (Enforcement Authorities-Telecommunications Data) Law § 10.

<sup>38</sup> *Id.* § 5.

<sup>39</sup> *Id.* § 14.

#### **D. Access to Police Maintained Database**

The Criminal Procedure (Enforcement Authorities-Telecommunications) (Database of Identification of Telecommunications) Regulations 5769-2008 regulate the usage, control, maintenance, and access to the police-controlled database for identification of telecommunications data.<sup>40</sup> According to the Regulations, access is available to subscribers who are included on a basic list composed of police officers with access to operational intelligence systems and those designated for this purpose by the head of the police section for investigation and intelligence, officers from secret monitoring units, and other designated police officers.<sup>41</sup>

Prepared by Ruth Levush  
Senior Foreign Law Specialist  
December 2010

---

<sup>40</sup> Criminal Procedure Regulations, *supra* note 36.

<sup>41</sup> *Id.* § 7.

**LAW LIBRARY OF CONGRESS**

**RUSSIAN FEDERATION**

**PRIVACY OF ELECTRONIC COMMUNICATIONS**

*Executive Summary*

*Russia does not have detailed Internet regulations. Issues of privacy protection are regulated according to existing civil and criminal procedural legislation, and its infringement is prosecuted. Personal data is recognized as confidential information and special rules for its collection, handling, usage, and distribution apply. While the Supreme Court rulings confirm judicial control requirements for online surveillance, the interception of electronic messages and access to information retrieved from databases by law enforcement and national security authorities rely on executive regulations that are less strict in comparison to judicial control. Nearly unrestricted government control over personal Internet communications was introduced in 1998 with the purpose of ensuring investigative activities. Amendments providing for more Internet freedom are currently under parliamentary deliberation.*

**I. Introduction**

Russia does not have a universal law that would regulate all legal issues related to the use of the Internet and there are no established legal definitions for such terms as “Internet,” “virtual space,” “global network,” “website,” “global information exchange,” and “online media.” As stated by the Deputy Chairman of the State Duma Committee for Information Policy, Boris Reznik, “the Internet has become an integral part of many people’s lives, but it has no legal framework. Current Russian legislation does not even define what the Internet is.”<sup>1</sup> Specific Internet-related aspects are regulated by general legislation. The use of personal information, including online use, is regulated by the Federal Law on Protection of Personal Data; the business responsibilities of Internet service providers are defined by the Federal Law on Information, Informatization, and Information Protection; and provisions of the Federal Law on Consumer Protection apply to online trade operations and other financial activities. Existing legislation contains such definitions as “information,” “information technology,” “information exchange,” and other such definitions, but they are used in the context of general regulation of the communications sector.<sup>2</sup> General rules of criminal procedure apply to investigative activities

---

<sup>1</sup> Ekaterina Maksimova, *Dueling Internet Legislation*, RUSSIAN PRESS DIGEST, No. 709a, July 9, 2010, available at <http://dlib.eastview.com/browse/doc/22154055> (by subscription).

<sup>2</sup> ILIA RASSOLOV, PRAVO I KIBERPROSTRANSTVO [LAW AND CYBERSPACE] 60 (Moscow: Academia, 2008) (in Russian).

and the admissibility of evidence involving electronic communications; however, a number of government regulations allow for simplified access by the authorities to personal and business Internet traffic and more power over Internet control, including web content control, in the case of emergencies.

The main rule that applies to the legal regulation of Internet-related issues in Russia is the norm defined by article 15.3 of the Federal Law on Information, Informatization, and Information Protection, which states that the use of information or telecommunications networks for business or other activities cannot be a reason to establish additional requirements or restrictions to regulate this type of activity if it would be conducted without the use of such networks.<sup>3</sup> According to this provision, regulation of cyberspace in Russia is based on general principles of legal regulation in the public sphere.<sup>4</sup>

## II. Legal Guarantees for Privacy of Electronic Communications

Privacy is the constitutional right of every Russian individual. Article 23 of the Russian Federation Constitution provides for the inviolability of private life and the protection of personal and family secrecy. Constitutional protection is extended in particular to the secrecy of letter exchanges, telephone conversations, mail, telegraphs, and other messages. The Constitution states that this right can be restricted according to a judicial ruling only.<sup>5</sup> The Constitution also restricts the collection, storage, use, and distribution of information on one's private life. These are not allowed without one's consent.<sup>6</sup> The Constitution prohibits censorship and guarantees the freedom to exchange information, which is recognized as the search, receipt, transfer, production, and distribution of information by any legal means. It specifies, however, that this protection does not apply to information classified as a state secret.<sup>7</sup> In Russia, constitutional provisions apply directly and do not require the adoption of implementing legislation.<sup>8</sup> A report on privacy regulations prepared by the Russian nongovernmental organization *Pravozaschitnaia Set'* (Legal Defense Network) did not find any contradictions between these constitutional norms and related provisions included in the charters of Russia's constituent components.<sup>9</sup>

The violation of one's privacy rights is prosecuted in accordance with the Criminal Code of the Russian Federation. Article 137 prohibits the illegal intrusion into one's private life, and

---

<sup>3</sup> SOBRANIE ZAKONODATELSTVA ROSSIISKOI FEDERATSII [SZ RF] [COLLECTION OF RUSSIAN FEDERATION LEGISLATION (official gazette)] 1995, No. 8, Item 609.

<sup>4</sup> D.V. Gribanov, *K Voprosu o Pravovoi Teorii Kiberneticheskogo Prostranstva (On the Legal Theory of Cyberspace)*, GOSUDARSTVO I PRAVO, 2010, No. 4, at 58 (in Russian).

<sup>5</sup> CONSTITUTION OF THE RUSSIAN FEDERATION art. 23.2 (Constitution adopted by the all-nation referendum on Dec. 12, 1993 (Moscow: Yurizdat, 1993) (official publication)).

<sup>6</sup> *Id.* art. 24.1.

<sup>7</sup> *Id.* arts. 29.4, 29.5.

<sup>8</sup> *Id.* art. 15.1. See also, WILLIAM BUTLER, *RUSSIAN LAW* 94 (Oxford University Press, 2009).

<sup>9</sup> PRIVATNOST' V ROSSIISKOM INTERNETE [PRIVACY IN RUSSIAN INTERNET] 7 (S.A. Smirnov ed., Moscow: Prava Cheloveka, 2003) (in Russian).

article 138 establishes responsibility for the violation of communications secrecy. Unauthorized access to computer information is recognized as a crime under article 272 of the Code. Punishments in the form of fines, correctional labor, detentions, a ban on certain types of professional activities, and imprisonment for a term of up to five years are recommended for these crimes by the sentencing guidelines.<sup>10</sup> Personal and family secrecy are also protected by article 150 of the Civil Code.<sup>11</sup>

Constitutional norms on privacy protection are reiterated and sometimes developed in individual legislative acts. The most relevant are the 1995 Federal Law on Information, Informatization, and Information Protection (hereafter Information Law),<sup>12</sup> the 2003 Federal Law on Communications (hereafter Communications Law),<sup>13</sup> and the 2006 Federal Law on Personal Data.<sup>14</sup>

### III. Access to and Protection of Information

The Information Law requires that government information resources remain open and publicly accessible (art. 10). Regardless of who owns information, only that information classified as a state secret or confidential, which includes personal data, is exempt from this rule (art. 11.1). According to the Information Law, all users must have equal rights to access government resources and are not required to justify their requests for information. A refusal to provide information can be appealed to a court (art. 13). The law emphasizes that access of individuals and legal persons to information about them must be unrestricted, except for cases specified in legislation. Everyone is allowed to know what information about them is collected, insist on correcting or adding information, and find out who is using the information and for what purposes. Such information must be provided for free (art. 14). Information must be processed and handled in accordance with existing legal norms and the owner of information resources may be liable for a violation of such norms (art. 15). The owners of nongovernment information resources provide information to the users based on legislation, their bylaws, and agreements with the customers (art. 12). All information must be protected if its illegal use may entail harm to its owner, possessor, user, or another person. The protection regime is defined by the State Secrecy Law and Personal Data Law for state secrets and personal information respectively, and owners of information resources are responsible for the protection of confidential information (art. 21).

The secrecy of communications is protected by article 63 of the Communications Law. It obligates all communications providers to ensure communications secrecy and states that only senders and recipients of correspondence and their legal representatives may have access to their correspondence in any format forwarded through the existing legal channels of communications. Secrecy rights can be restricted in cases stipulated by law. Special provisions (art. 64) regulate

---

<sup>10</sup> SZ RF 1996, No. 25, Item 2954.

<sup>11</sup> SZ RF 1994, No. 32, Item 3301.

<sup>12</sup> SZ RF 1995, No. 8, Item 609.

<sup>13</sup> SZ RF 2003, No. 28, Item 2895.

<sup>14</sup> SZ RF 2006, No. 31, Item 3451.

the mechanism of sharing information between the provider of communications services and law enforcement authorities.

The Federal Law on Personal Data recognizes as personal all information concerning the facts, events, and circumstances of one's life that allow for identification of a person. The inclusion of this definition in the Law was based on the Russian President's Decree No. 188 of March 6, 1997, On Listing Information Considered Confidential. The Decree distinguished between personal and confidential information and provided that such facts as date of birth, place of residence, etc., are not protected as long as they do not disclose the circumstances of one's private life.<sup>15</sup> The Law on Personal Data entered into force in January 2007, and established that the processing of personal information must be made to conform with it as of 2011. The Law requires the licensing of all who perform business operations with personal information (hereafter "operators of information" or "operators"), the technical certification of equipment, and the performance of measures aimed at protecting the data collected. These measures include notifying an individual about the processing of his/her personal information, obtaining that individual's consent for processing, notifying the individual upon termination of processing, and destruction of the information collected. Notification and consent are not required if the operator of information and the individual in question have labor or other contractual relations (arts. 21, 22).

Reportedly, in 1999, more than 15 percent of all of the personal information collected by operators was used illegally in order to receive profit. In violation of legal requirements, the operators collected information, the possession of which was not justified by the original goals of collecting, as required by article 5 of the Law on Personal Data. It appears that the number of violations has now increased exponentially.<sup>16</sup>

#### **IV. Obligations on Service Providers Related to Personal Data Protection**

Russian legislation obligates Internet service providers to ensure that the requirements for communications secrecy are met. Those who violate rules for collecting, storing, using, and distributing information on individuals or inappropriately disclose restricted information are subject to substantial fines according to section 13 of the Code of Administrative Violations.<sup>17</sup> However, exemptions from this rule are allowed. Until the late 1990s, such exemptions could be granted by court rulings, and each case of government access to information stored by Internet providers required a warrant preliminarily sanctioned by a judge. Subsequent legislation substituted the requirement of judicial review with provisions allowing government regulatory agencies to define the cases and circumstances in which the monitoring of one's Internet activities would be justified.<sup>18</sup>

---

<sup>15</sup> SZ RF 1997, No. 10, Item 1127.

<sup>16</sup> O.I. Trofimov, *Nekotorye Aspekty Pravovogo Regulirovaniia Baz Dannykh* [On Legal Regulation of Databases], GOSUDARSTVO I PRAVO, 2008, No. 10, at 66 (in Russian).

<sup>17</sup> SZ RF 2002, No. 1(1), Item 1.

<sup>18</sup> Communications Law art. 63.4.

Because Russia does not have special Internet-related legislation, and because the existing criminal procedural norms were established before the development of the Internet and do not address electronic communications directly, the Russian leadership decided to regulate the activities of Internet service providers and other electronic communications operators in support of national security and investigative activities by executive regulations. Article 64 of the Communications Law, as amended in 2006, states that federal legislation must define the procedures under which Internet service providers will offer to law enforcement authorities information on their customers and services received by individual customers, terminate services for individual customers on the request of law enforcement authorities, remain silent about the ongoing investigative activities, and per the request of law enforcement authorities install special equipment, which would allow them to conduct investigations and monitor issues related to national security. A 2009 Ministry of Justice regulation requires the Internet domain registration authorities to report to the Federal Security Service information on individuals who registered an Internet domain name in the .RU and .RF zones.<sup>19</sup>

Since January 1, 2007, due to an amendment to the Communications Law, no telecom or Internet operator is allowed to terminate services provided to the government. The Law established that all operators must provide services to government institutions in order to ensure national defense, state security, and law enforcement. The provision of services can be terminated upon a government request only.<sup>20</sup>

## V. Interception and Surveillance

In 1998, the Federal Security Service of the Russian Federation started to install special equipment for remote control over information transmitted via the Internet. These activities were sanctioned by the Ministry of Communications and were called the System for Ensuring Investigative Activities (*Systema Operativno-Rozysknykh Meropriiatii*, SORM). The legal foundation for the system was article 64 of the Communications Law, which lists obligations of Internet providers in the field of national security. Government-approved Rules on Cooperation Between Internet Operators and Government Authorities Conducting Investigative Activities<sup>21</sup> defined the major principles of the government's monitoring of private Internet use.

The system consists of special devices placed in the office of an Internet provider, a monitoring station in the Federal Security Service office, and a specially designated high-speed communications channel. Based on the principle of keyword recognition, the system allows secret police to monitor all Internet traffic, credit card transactions, and email exchanges in real time and without applying for a warrant. Also, there is no requirement to inform the user that he/she is being watched.

---

<sup>19</sup> Rules for Domain Names Registration, Ministry of Justice Resolution No. 2010-15/97 of Oct. 11, 2010, available at [http://rf.reg.ru/docs/rfdomain/rf\\_rules.pdf](http://rf.reg.ru/docs/rfdomain/rf_rules.pdf) (last visited Dec. 9, 2010).

<sup>20</sup> Federal Law No. 153-FZ of July 27, 2006, ROSSIISKAIA GAZETA (official publication), July 31, 2006.

<sup>21</sup> Government Regulation No. 538 of August 27, 2005, accessible through the Consultant Plus legal database (by subscription only), at <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=80879>.

The Federal Security Service, through one of its service units, the Federal Agency for Government Communications and Information, which together with the Ministry of Communications is authorized to approve license requests of Internet providers, requires that all equipment needed to install and maintain SORM, which costs approximately US\$30,000 per provider, must be purchased by the Internet providers themselves and offered to the officers of the Federal Security Service for free use. If Internet providers do not meet SORM requirements, their license can be terminated.<sup>22</sup>

This practice became publicly known when one small firm that provides Internet and other cable services in the city of Volgograd in Central Russia refused to install such equipment and threatened to bring the issue to the court, justifying its refusal by arguing for the protection of the constitutional rights of its customers. According to the Federal Security Service, the firm did not have enough money to buy the equipment and wanted to use this situation for self-promotion. Rather than going to court over the matter, the Federal Security Service has simply chosen to conduct business with large telecom firms.<sup>23</sup>

In 2009, the Federal Security Service of the Russian Federation requested that Internet service and access providers block access to Skype service in Russia because this system could not be penetrated for interception and cannot be connected with SORM. This requirement was later revoked and the Federal Security Service has announced that it now has a technological solution to intercept Skype.<sup>24</sup>

Access to and the use of video surveillance materials is not regulated by legislation. There are no restrictions on the use of video surveillance equipment unless it is used for secret videotaping and is included in the list of special means used for police investigative activities. The importation and use of such equipment is subject to licensing, according to Government Regulation No. 214 of March 10, 2000.<sup>25</sup> Usually, employers inform employees if they conduct videotaping at work in order to avoid potential complaints; however, they are not obligated to do so by law.

## VI. Admissibility Rules

Information received through SORM is often used to initiate investigations and other procedural activities against members of the political opposition and those who, in the opinion of the law enforcement authorities, use electronic communication to propagate terrorism and extremist ideas. A large number of individuals have been prosecuted for statements in their

---

<sup>22</sup> Electronic Networks Requirements for Investigative Activities, Approved by Orders of the RF Ministry of Information and Communications No. 6 of Jan. 16, 2008; No. 73 of May 27, 2010; accessible through the Consultant Plus legal database (by subscription only), at <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=102523>.

<sup>23</sup> Julia Solovyova, *Russia Prepares to Police Internet*, MOSCOW TIMES, No. 1505, July 27, 1998.

<sup>24</sup> *Skype Might Be Banned in Russia*, BETAMART, <http://www.betamart.ru/2010/06/02/skype-mogut-zapretit-v-rf-on-meshaet-monopolistam-i-ne-poddaetsya-proslushke/> (in Russian; last visited Dec. 8, 2010).

<sup>25</sup> SZ RF 2000, No. 12, Item 1292.

blogs or comments placed on others' websites.<sup>26</sup> In 2006, amendments to varied legislative acts making Internet content and service providers responsible for the distribution of extremist materials were introduced in the Russian legislature. Pursuant to these amendments, the owners of Internet resources could to be held responsible for statements made by their customers or website visitors. Providers failing to monitor and correct content faced fines and warnings from authorities, which could potentially lead to the liquidation of a website or provider.<sup>27</sup> In June 2010, the Supreme Court of the Russian Federation made clear that Internet providers and website owners will be responsible for "commentaries of their readers left on web forums if freedom of information is abused." The Court ruled that the preliminary moderation of comments is not required but comments must be removed if the Federal Committee for Communications Monitoring submits a formal complaint.<sup>28</sup>

The monitoring of information transferred via or stored in electronic resources involves investigative activities and must be conducted according to a court permit if there is: information on the preparation or commitment of an illegal act that is actively being investigated; information that an individual is attempting or committing, or has committed, an illegal act that must be preliminarily investigated by law; and information on acts or activities that threaten the national, military, economic, or environmental security of the Russian Federation. Criminal procedural law requires that information on one's Internet activities submitted to the court shall be obtained by legal means.<sup>29</sup> Because the legality of these means is not defined with regard to materials received by secret access to electronic communications, it appears that courts accept evidence received by law enforcement and state security in accordance with existing executive regulations.<sup>30</sup>

## VII. Recent Legislative Developments

Two bills on the legislative regulation of Internet-related issues were introduced in the State Duma of the Russian Federation in the summer of 2010. One was drafted by a working group at the State Duma and the other by the Ministry of Communications and Mass Media. The bills provide for amendments to the Information Law concerning parameters for the government regulation of activities on the Internet and regulate the interaction of society and the government with the Internet. Apart from defining general terms, such as "global computer network" and "website operator," the bills would establish Russia's territorial jurisdiction and provide that if a server is located somewhere abroad but the authors and moderators of a website are in Russia,

---

<sup>26</sup> *Blogger Terentyev Poluchil God Uslovno Za Kommentarii v Zhivom Zhurnale* [Blogger Terentyev Was Sentenced to One Year of Imprisonment for Comments in Livejournal], NEWSRU.COM, (July 7, 2008), [http://www.newsru.com/russia/07jul2008/terya\\_jun\\_srok.html](http://www.newsru.com/russia/07jul2008/terya_jun_srok.html) (in Russian).

<sup>27</sup> Anastasia Matveyeva & Marat Khairullin, *Real Prison for Virtual Extremists*, GAZETA, 2006, No.13, at 4, English translation published in RUSSIAN PRESS DIGEST, 2006, No. 31.

<sup>28</sup> Russian Federation Supreme Court Ruling No. 16 of June 15, 2010, BIULLETEN VERKHOVNOGO SUDA ROSSIISKOI FEDERATSII [RF SUPREME COURT BULLETIN] 2010, No. 8, at 3 (official publication; in Russian).

<sup>29</sup> Criminal Procedural Code of the Russian Federation, art. 84, SZ RF 2001, No. 52(1), Item 4921.

<sup>30</sup> Ruling of the Russian Federation Supreme Court Plenary Meeting No. 1 of March 5, 2004, on Application of Select Provisions of the RF Criminal Procedural Code, BIULLETEN VERKHOVNOGO SUDA ROSSIISKOI FEDERATSII [RF SUPREME COURT BULLETIN] 2004, No. 5, at 8 (official publication; in Russian).

they must abide by Russian legislation. The two bills address the issue of Internet privacy differently. The State Duma Bill includes a direct ban on imposing out-of-court restrictions on citizens' and legal entities' rights and freedoms and states that a user's access to information may be restricted only by a court order. The bill drafted by the Communications and Mass Media Ministry envisages a stricter legal framework for virtual space. The bill gives broader authority to law enforcement agencies and requires access providers to suspend a domain on a substantiated request by a law enforcement agency and to restrict the user's access to information if requested by a public prosecutor. Both bills support the complete freedom of searching for information and establish the inviolability of property in the sphere of information technology.<sup>31</sup>

Prepared by Peter Roudik  
Chief, Eastern Law Division  
December 2010

---

<sup>31</sup> Ekaterina Maksimova, *Dueling Internet Legislation*, RUSSIAN PRESS DIGEST, No. 709a, July 9, 2010, available at <http://dlib.eastview.com/browse/doc/22154055> (by subscription).

**LAW LIBRARY OF CONGRESS**

**UNITED KINGDOM**

**PRIVACY OF ELECTRONIC COMMUNICATIONS**

*Executive Summary*

*The comprehensive Regulation of Investigatory Powers Act 2000 provides for a closely knit regulatory regime that initially creates criminal offenses for the unlawful interception of electronic communications, and also a tort of unlawful interception, but grants fairly extensive lawful authority for the interception of a wide range of electronic communications on specified grounds, including interests of national security, the prevention of serious crimes, and the economic well-being of the country. A stratified system of issuing interception warrants and authorizations are in place, but warrantless interceptions are permitted in specified cases. Obligations are placed on telecommunications services providers to comply with notices issued by investigatory authorities carrying out interception. Offenses are also created for the unauthorized disclosure of lawfully intercepted communications. A prohibition is in place against the fact of interception and its product being disclosed in court proceedings. Detailed Codes of Practices provide the procedures to be followed in intercepting and retaining data.*

**I. Interception**

**A. Legislation and Codes of Practice**

The United Kingdom's Regulation of Investigatory Powers Act 2000<sup>1</sup> [RIPA] takes similar measures to those in U.S. statutes, including the Wiretap Act (known as "Title III") and the law on Unlawful Access to Stored Communications.

Part 1, Chapter 1, of RIPA governs the interception of communications over private telecommunications systems.<sup>2</sup> As with its predecessor statute, the Interception of Communications Act 1985, RIPA creates offenses of unlawful interception, but creates an exception for interception carried out under lawful authority.

RIPA also authorizes the Secretary of State to issue Codes of Practice relating to the exercise and performance of the powers and duties under the Act.<sup>3</sup> Every draft of the Codes of

---

<sup>1</sup> Regulation of Investigatory Powers Act 2000 [RIPA], c. 23, <http://www.legislation.gov.uk/ukpga/2000/23/contents>

<sup>2</sup> RIPA §§ 1-20.

<sup>3</sup> RIPA § 71.

Practice is submitted to both Houses of Parliament. The Secretary of State is required to consider any representations made to him about the draft, and he may incorporate any modifications to the draft Codes.

### **B. Under a Warrant**

Section 5 of RIPA sets out a mechanism for the issuance by the Secretary of State of a warrant authorizing conduct, as described in the warrant, for the interception of communications transmitted by means of a postal service or telecommunications system.

In issuing a warrant, the Secretary of State must be of the belief that it is necessary on the following grounds: in the interests of national security; for the purpose of preventing or detecting serious crime; safeguarding the economic well-being of the United Kingdom; or, for giving effect to the provisions of any international mutual assistance agreement.<sup>4</sup> The Secretary of State must also believe that the conduct authorized by the warrant is proportionate to what is sought to be achieved by the conduct.<sup>5</sup> Matters to be taken into account by the Secretary of State in considering whether these requirements are satisfied must include whether the information sought to be obtained under the warrant could reasonably be obtained by other means.<sup>6</sup>

An interception warrant must be issued under the hand of the Secretary of State, except in two cases in which a senior official may issue a warrant: (1) in an urgent case (but the Secretary must expressly authorize it); and (2) in a case where the warrant is for the purposes of a request for assistance under an international mutual assistance agreement and the interception subject is outside the United Kingdom or the interception is in relation to premises outside the United Kingdom.<sup>7</sup>

The application for an interception warrant must be made by or on behalf of persons specified in the RIPA.<sup>8</sup> These include the Director-General of the Security Service, the Chief of the Secret Intelligence Service, the Chief of Defence Intelligence, the Commissioner of Police of the Metropolis, the chief constable of any police force, and others.

### **C. Types of Warrants**

A domestic interception warrant must name or describe one person as the subject of the interception or a single premises in relation to which the interception is to take place.<sup>9</sup> The warrant must describe the communications that are authorized to be intercepted and set out one

---

<sup>4</sup> RIPA § 5(3).

<sup>5</sup> RIPA § 5(2).

<sup>6</sup> RIPA § 5(4).

<sup>7</sup> RIPA § 7(2).

<sup>8</sup> RIPA § 6.

<sup>9</sup> RIPA § 8(1).

or more schedules of the addresses, numbers, apparatus, or other factors that are to be used for identifying the communications.<sup>10</sup>

A broader warrant (also referred to as a “certificated warrant”) may be issued without naming a subject, premises, or schedules if the warrant is confined to “external communications,” as defined, and the Secretary of State certifies the description of materials that are necessary to be intercepted in the interests of national security, for preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom.<sup>11</sup>

Provisions are made for the duration, renewal, modification, and cancellation of warrants.<sup>12</sup> Normally, interception warrants have effect for three months; those issued on the grounds of national security or the economic well-being of the country are renewed for six months at a time. A warrant issued by a senior official in urgent cases expires at the end of the fifth working day after issue.

#### **D. Without a Warrant**

An interception without a warrant is permitted under separate provisions in RIPA. Section 3 authorizes such interception if: (1) there are reasonable grounds to believe that both the sender and the recipient of the communication consent to the interception; (2) either the sender or the recipient consents and the interception has been authorized under the directed surveillance provisions of RIPA; or (3) the interception is connected with the operation of a telecommunications service for the purpose of enforcement provisions governing the use of the service and the interception is done by or on behalf of a person who provides the service.

Warrantless interceptions are also permitted if:

- The interception is for the communications of an overseas person relating to the use of a public telecommunications system in that country, and the law of the country requires the service provider to carry out the interception;
- A “legitimate business practice” in carrying on a business of monitoring or keeping a record of communications is authorized under regulations to intercept;<sup>13</sup> or
- An interception is carried out under legislation relating to high-security psychiatric hospitals.<sup>14</sup>

---

<sup>10</sup> RIPA § 8(2).

<sup>11</sup> RIPA § 8(4).

<sup>12</sup> RIPA § 9.

<sup>13</sup> Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, SI 2000/ 2699, <http://www.legislation.gov.uk/uksi/2000/2699/contents/made>.

<sup>14</sup> RIPA § 4.

## II. Surveillance

Directed surveillance, covert surveillance, and the use of covert human intelligence sources are regulated under Part II of RIPA.<sup>15</sup> Authorization procedures are provided for each type, but one scholar has noted that Part II “creates what is essentially a voluntary scheme for authorization . . . of surveillance.”<sup>16</sup> Oversight is provided by a Surveillance Commissioner, set up under separate legislation on the police, for authorizations for non-intelligence services.

“Surveillance” is defined to include monitoring, observing or listening to persons, and their movements; recording anything monitored in the course of surveillance; and surveillance by or with a surveillance device.<sup>17</sup> “Directed surveillance” is carried out for the purposes of a specific investigation. Surveillance is “covert” if it is calculated to ensure that the subject is unaware of it.<sup>18</sup> Covert surveillance carried out in relation to residential premises or private vehicles that involves the presence of an individual on the premises or in the vehicle or the use of a surveillance device is “intrusive surveillance,” subject to certain exceptions.<sup>19</sup>

Intrusive surveillance requires the authority of the Secretary of State upon application made by a member of the intelligence services, armed forces, or other designated authorities.<sup>20</sup> For applications made by a member of a police force, a customs official, or other crime authorities, the authorization can be given by a “senior authorizing officer.” Conditions of necessity and proportionality are needed for authorization of the surveillance. Necessity includes interests of national security, the economic well-being of the UK, or the purpose of preventing or detecting serious crime. The authorizing official must also consider whether the information could reasonably be obtained by other means. Authorizations given to police or customs officers must be approved in writing by a Surveillance Commissioner, except in cases of urgency.<sup>21</sup>

Directed surveillance may be authorized by a superintendent of police, or a higher rank, and those having equal seniority in the security and intelligence services, armed forces, and other public authorities that have power to undertake surveillance. Again, conditions of necessity and proportionality must be met. Conditions of necessity are: national security; preventing or detecting any crime or disorder; the economic well-being of the UK; interests of public safety; protecting public health; collection of taxes or duties, etc.; and a purpose specified in an order made by the Secretary of State.

---

<sup>15</sup> RIPA §§ 26-48.

<sup>16</sup> Victoria Williams, *Surveillance And Intelligence Law Handbook* 125 (Oxford, 2005).

<sup>17</sup> RIPA § 26(2), (3).

<sup>18</sup> RIPA § 26(9).

<sup>19</sup> RIPA § 26(3).

<sup>20</sup> RIPA § 32.

<sup>21</sup> RIPA § 36.

### III. Access to Intercepted Communications

RIPA places a duty on the Secretary of State to ensure that the number of persons to whom, and the extent to which, the intercepted data is disclosed and copies made is limited to the minimum necessary for the authorized purposes.<sup>22</sup> These requirements are satisfied if the arrangements made for securing the materials include an arrangement for ensuring that every copy is stored in a secured place.<sup>23</sup> Another requirement regarding copies made is that the material or data is destroyed as soon as there are no longer any grounds for retaining the information for any authorized purposes.<sup>24</sup>

Extra safeguards are imposed on certificated warrants requiring that intercepted material is looked at or listened to only to the extent that it has been certified as material of which examination is necessary.<sup>25</sup>

Interception in relation to any stored communication is allowed if it is in exercise of a statutory power granted under any other statute (e.g., relating to police investigations).<sup>26</sup>

### IV. Types of Communications Covered

#### A. Generally

The Act defines private telecommunications systems as including any system that is attached, directly or indirectly, to a public telecommunications system, and that has apparatus both located in the United Kingdom and is used for making the attachment to the public telecommunications system.<sup>27</sup> The Act applies to the interception of communications “in the course of their transmission”<sup>28</sup> and provides operational definitions at some length of the terms “interception,” “communication,” and “in the course of transmission.”<sup>29</sup>

RIPA excludes “traffic data,” as defined,<sup>30</sup> from the interception provisions, and subjects it to a different “watered down system.”<sup>31</sup> Section 21(4) of RIPA coins the term “communication data” and defines it to include:

---

<sup>22</sup> RIPA § 15(2).

<sup>23</sup> RIPA § 15(5).

<sup>24</sup> RIPA § 15(3).

<sup>25</sup> RIPA § 16.

<sup>26</sup> RIPA § 1(5); WILLIAMS, *supra* note 16, at 77.

<sup>27</sup> RIPA § 2(1).

<sup>28</sup> RIPA § 1(1).

<sup>29</sup> RIPA §§ 2(2), (3), (5), and 81(1).

<sup>30</sup> RIPA § 2(9). In simpler language, this is data that is attached to “the communication and which serves to identify its source, destination, sender or sending and receiving equipment and other message attributes. It can be seen as the operating information supplied by the system as opposed to the content of the message being sent.” WILLIAMS, *supra* note 16, at 71.

<sup>31</sup> David Feldman, *Civil Liberties and Human Rights in England and Wales* 667 (Oxford, 2002).

- Traffic data comprised in or attached to a communication of any postal service or telecommunications system;
- Any information that includes none of the contents of a communication and is about the use made by any person of a postal or telecommunications service; or
- Information in connection with the provision or use of any telecommunications service.

“Communications data” is therefore stated in one leading handbook to include “information such as numbers dialed, times of calls, details of callers and receivers, website addresses, email addresses, etc.”<sup>32</sup>

Communications data is more readily obtainable, and it is not subject to the restrictions on use placed on intercepted communications. Section 22 supplies wider grounds for access: in the interests of national security; for preventing or detecting crime or preventing disorder; in the interests of the economic well-being of the United Kingdom; in the interests of public safety; for the protection of public health; for assessing or collecting tax or duty; for preventing, in an emergency, death or injury or any damage to a person’s physical or mental health; or for any other purpose that is specified by an order made by the Secretary of State.

The public authorities that may access communications data include: a police force; the National Criminal Intelligence Service; the National Crimes Squad; Commissioners of Customs and Inland Revenue; any intelligence service; and any other public authority as may be specified by the Secretary of State.<sup>33</sup> Within each public authority, a “designated person” is responsible for receiving, approving, or rejecting applications to obtain communications data from service providers.<sup>34</sup>

## **B. Encrypted Data**

RIPA authorizes the serving of a notice for disclosure to a person who is believed to have the key to any protected information.<sup>35</sup> “Protected information” is defined as “electronic data which, without the key to the data – (a) cannot . . . be accessed, or (b) cannot . . . be put into an intelligible form”; a “key” is defined as any “code, password, algorithm” that allows access to the electronic data or renders it “into an intelligible form.”<sup>36</sup>

---

<sup>32</sup> WILLIAMS, *supra* note 16, at 111.

<sup>33</sup> RIPA § 25(1).

<sup>34</sup> RIPA § 22.

<sup>35</sup> RIPA § 49.

<sup>36</sup> RIPA § 56(1).

The notice to disclose a key to protected data may include a requirement that the person served must keep secret the giving of the notice, its contents, or anything done in pursuance of it.<sup>37</sup>

## **V. Obligations of Service Providers**

The Secretary of State is authorized to notify telecommunications service providers to undertake steps necessary for having the practical capability of providing assistance in relation to interception warrants.<sup>38</sup> It is the duty of service providers to comply with the notice, which notice is enforceable by civil proceedings for an injunction or specific performance.<sup>39</sup> The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002<sup>40</sup> provides the requirements that the Secretary of State may place on service providers.

RIPA sets up a Technical Advisory Board appointed by the Secretary of State, whose membership must include persons who are likely to effectively represent the interests of service providers on whom obligations to provide information are placed, and also to represent those on whose behalf applications for interception warrants are made.<sup>41</sup> The membership must be constituted so as to produce a balance between the representations of the two interests.

A service provider who has been served with a notice requiring it to comply with an obligation may refer the notice to the Technical Advisory Board within twenty-eight days. On referral to the Board, the obligation is suspended until the Board reports to the Secretary of State about the technical requirements and the costs to the service provider. RIPA also authorizes service providers to receive a fair contribution towards the costs incurred in complying with a notice.<sup>42</sup>

## **VI. Offenses, Penalties, and Defenses**

The principal offenses arising from unlawful interception of communications are:

- To intentionally intercept any communication in the course of its transmission by means of a public postal service or a public telecommunications system; and
- To intentionally intercept any communication in the course of its transmission by means of a private telecommunications system.<sup>43</sup>

---

<sup>37</sup> RIPA § 54(2).

<sup>38</sup> RIPA § 12(3).

<sup>39</sup> RIPA § 12(7).

<sup>40</sup> S.I. 2002/1931.

<sup>41</sup> RIPA § 13.

<sup>42</sup> RIPA § 14.

<sup>43</sup> RIPA § 1(1), (2).

A person guilty of these offenses is liable (a) on indictment to a term of imprisonment not exceeding two years, or to a fine, or both; and (b) on summary trial (a non-jury trial) to a fine not exceeding a specified statutory amount.<sup>44</sup>

RIPA also creates an action for a tort under which the sender or recipient of an unlawfully intercepted communication is granted an actionable right to bring suit.<sup>45</sup>

The unauthorized disclosure of information concerning interception warrants, the requirement to provide assistance in giving effect to warrants, and everything in the intercepted material, including related communications data, by a person who is required to keep them secret constitutes an offense and gives rise to liability (a) on conviction on indictment to a term not exceeding five years or a fine, or both; and (b) on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or both.<sup>46</sup> The persons who have the duty of secrecy are public, police, and intelligence officials, and postal and telecommunications personnel that have involvement with the lawful interception of communications.<sup>47</sup>

It is a defense for a person accused of the offense of unauthorized disclosure to show that he could not reasonably have been expected, after becoming aware of the matter disclosed, to take steps to prevent the disclosure.<sup>48</sup> It is also a defense for that person to show that (a) the disclosure was made by or to a professional legal adviser in connection with the giving of legal advice about the effect of the provisions of Chapter I of RIPA; and (b) the person to or by whom the disclosure was made was the client or representative of the client.<sup>49</sup> It is also a defense to show that the disclosure was made by a legal adviser (a) in contemplation or connection with any legal proceedings; and (b) for the purpose of those proceedings.<sup>50</sup> These defenses are not available in the case of a disclosure made with a view to furthering any criminal purpose.<sup>51</sup> It is also a defense for that person to show that the disclosure was confined to one that was made to the Interception of Communications Commissioner or authorized (a) by that Commissioner; (b) by the warrant or the person to whom the warrant is or was addressed; (c) by the terms of the requirement to provide assistance; or (d) by section 11(9) of RIPA.<sup>52</sup>

With regard to the notice served on a person who has the key to protected information (*see* Part IV, above), it is an offense to knowingly fail to make the disclosure required by the

---

<sup>44</sup> RIPA § 1(7).

<sup>45</sup> RIPA § 1(3).

<sup>46</sup> RIPA § 19(1), (2), (3), (4).

<sup>47</sup> RIPA § 19(2).

<sup>48</sup> RIPA § 19(5).

<sup>49</sup> RIPA § 19(6).

<sup>50</sup> RIPA § 19(7).

<sup>51</sup> RIPA § 19(8).

<sup>52</sup> RIPA § 19(9).

notice.<sup>53</sup> A person found guilty of this offense is liable on conviction on indictment to a term of imprisonment not exceeding two years or to a fine, or to both; and on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both. It is a defense for a person to show that it was not reasonably practicable to make the disclosure within the time by which the notice required the information, but that he made the disclosure as soon after that time as was reasonably practicable.<sup>54</sup>

Concerning the requirement of secrecy in a notice served for the disclosure of a key to protected data, any breach will result in an offense of tipping-off.<sup>55</sup> A person committing the offense is liable on conviction under indictment for a term of imprisonment not exceeding five years or to a fine, or both; and on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both. It is a defense for the person charged with tipping-off to show that the disclosure was effected entirely by the operation of software designed to indicate when a key to protected information has ceased to be secure and that he could not reasonably have been expected to take steps to prevent the disclosure. Other defenses relating to seeking the advice of a professional legal adviser are also allowed.<sup>56</sup>

A right of civil action is also granted to any person who incurs loss or damage resulting from a disclosure relating to protected information.<sup>57</sup>

When an offense under any provision of RIPA, other than under Part III (sections 49-56) is committed by a corporate body and is proved to have been committed with the consent or connivance of a corporate official, the official as well as the body corporate shall be guilty of the offense and liable to be proceeded against and punished accordingly.<sup>58</sup>

## **VII. Admissibility**

No evidence can be adduced, questions asked, or disclosure made in any legal proceedings of an authorized interception of a communication and the product of that interception.<sup>59</sup> However, such disclosure may be made to a prosecutor to allow him to

determine what is required of him by his duty to secure the fairness of the prosecution. . . . It may also require disclosure to the judge so that the judge may sum up the case in a particular way, give appropriate directions to the jury or require admissions of fact from the prosecution.<sup>60</sup>

---

<sup>53</sup> RIPA § 53.

<sup>54</sup> RIPA § 53(4).

<sup>55</sup> RIPA § 54.

<sup>56</sup> RIPA § 54(9), (10).

<sup>57</sup> RIPA § 55(4)–(7).

<sup>58</sup> RIPA § 79.

<sup>59</sup> RIPA §§ 17, 18.

<sup>60</sup> BLACKSTONE'S CRIMINAL PRACTICE 2010 at 1446 (commenting on RIPA § 18).

The Attorney-General has issued “Section 18 RIPA: Prosecutor’s Guidelines,”<sup>61</sup> which notes that it is long-standing policy that the fact of the interception of communications should remain secret and not be disclosed to the subject.

In its decision in *Khyam*,<sup>62</sup> the Court of Appeal stated that there would have to be highly unusual and material circumstances for a court to depart from the prohibition placed in RIPA.

### VIII. Codes of Practice

Several Codes of Practice have been issued under the authority of the 2000 Act.

- The *Code of practice on the interception of communications*<sup>63</sup> provides guidance on the procedures to be followed. It also is admissible as evidence in criminal and civil proceedings, and a court or a tribunal must take into account any provision of the Code that appears relevant to the proceedings.
- The *Code of practice for the acquisition and disclosure of communications data*<sup>64</sup> relates to RIPA provisions in Chapter II of Part I.
- The *Code of practice for covert surveillance and property interference*<sup>65</sup> provides guidance on a use by public authorities of Part II of RIPA that is likely to result in obtaining private information about a person.
- The *Code of practice for the use of human intelligence sources*<sup>66</sup>
- The *Code of practice on investigation of protected electronic sources*<sup>67</sup> relates to encrypted data.

Prepared by Kersi B. Shroff  
Co-Director of Legal Research  
Global Legal Research Center  
December 2010

---

<sup>61</sup> *Id.*, App. 2, at 2805-07.

<sup>62</sup> [2009] Cr App R (S) 455.

<sup>63</sup> Available at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/interception-comms-code-practice>.

<sup>64</sup> Available at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary>.

<sup>65</sup> Available at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert>.

<sup>66</sup> Available at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-human-intel>.

<sup>67</sup> Available at <http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-electronic-info?view=Binary>.