

## **Chapter 2**

# **The Legal Situation: Prevention and Enforcement in the Information Age**

In this chapter, we will examine the development of the legal framework internationally, in the United States, in the European Union, and in selected other countries in relation to the issues outlined in Chapter 1. An examination of some of the laws that have evolved in these countries will offer insight into the delicate balance that modern nations strive for between the need for security and the preservation of civil rights. The law is changing rapidly in this regard, with updates that might suggest an on-line book and not a printed one. What is current today, may be history tomorrow.

Nevertheless, the principles and processes for addressing these fundamental issues are rooted in what we present here. The terrorist is ever more sophisticated, and so too must be the law. Grappling with the difficult balancing act between security needs, the legal rights of the individual and the ever evolving developments of technology is a daunting challenge for mankind.

The means of prevention and enforcement operated by government authorities are guided, at least on the face of it, by regulations and principles of public law, three of which are discussed below. First, state authorities are subject to constitutional law and basic rights of the normative framework, wherein all activities should be balanced with respect to human rights.

Second, the authorities are subject to the principles of administrative law, which delineate a framework of action in pursuing the principle of legality. The authorities must function within legal parameters. Furthermore, the existence of their power is not sufficient. The authorities must act reasonably and fairly and at the same time must take into account human rights considerations.

Third, the actions of the authorities are subject to the constant possibility of judicial control. More accurately, judicial control is possible at

all stages, both before implementation of the means of prevention and enforcement, such as when applying for required warrants, and afterwards, such as in the aftermath of a direct or indirect attack.

## 2.1 The International Scene

### *2.1.1 Protection of the Right to Privacy*

Modern treatment of the right to privacy at the international level is found in the Universal Declaration of Human Rights of 1948.<sup>1</sup> The guiding principle underlying the Declaration's approach is delineated in § 12, which states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." A large number of general international treaties expressly recognize the right to privacy, including the International Covenant on Civil and Political Rights (ICCPR)<sup>2</sup> and various UN treaties. The ICCPR explicitly states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, home or correspondence, nor to unlawful attacks on his honour and reputation." It goes on to affirm that "everybody has the right to the protection of the law against such interference or attacks." At the regional level, there are conventions that have made the right to privacy a legally enforceable right, such as the European Convention of Human Rights and Fundamental Freedoms of 1950.<sup>3</sup> Using similar language to earlier declarations of rights, Article 8 of the Convention states that "everybody has the right to respect for his private and family life, his home and his correspondence." It goes on to say that "there shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the rights and freedoms of others." Following this convention, the European Human Rights Commission, the European Human Rights Court, and the Charter

---

<sup>1</sup> Universal Declaration of Human Rights (1948). <http://www.hrweb.org/legal/udhr.html>

<sup>2</sup> International Covenant on Civil and Political Rights (1966), Art. 17. <http://www.hrweb.org/legal/cpr.html>

<sup>3</sup> European Convention of Human Rights & Fundamental Freedoms (1950), Art. 8.

of Fundamental Rights of the European Community were established, all of which aim to protect privacy and personal information.<sup>4</sup>

The recognition of the right to privacy in international law provides a foundation for the right to privacy as a basic human right. Most Western countries recognize the right to privacy at the level of national law as a constitutional right. More recent constitutions deal specifically with the right to privacy and the right to control personal information. Forty out of the fifty countries (including Israel) reviewed in the report of the Organization for Protection of Privacy (2000) demonstrated awareness and maintained clear rights regarding access to public documentation.<sup>5</sup> The protection granted at the international level and the recognition of the right to privacy in the national law of many countries indicate the importance of the right to privacy. This national and international awareness of the right to privacy is likely to have a direct influence on the checks and balances required in every situation in which this right may be compromised, particularly in the political climate created after the events of September 11 and in light of new technologies allowing unprecedented invasion of privacy.

### ***2.1.2 International Regulation for Protection of Personal Data***

The right to privacy also applies in specific cases concerning the right of the individual to prevent collection and processing of personal data concerning him. International protection of electronic data concerning the individual was established in the 1990 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.<sup>6</sup> This convention discusses personal data files and processing of data in the public sector and the private sector. It stipulates that the obtaining, processing, and storage of data must be conducted in accordance with the purposes for which it was collected. The data must be proper and relevant and must

---

<sup>4</sup> See: Charter of Fundamental Rights of the European Union, OJC 364.

<sup>5</sup> This is a survey conducted by the Center for Electronic Privacy in Washington and the International Center for Privacy in London. The report reviews the status of the right to privacy in some fifty countries by examining various areas of privacy, including data protection, wiretapping, data banks, identification systems, and freedom of information. <http://www.privacyinternational.org/survey/phr2000/>

<sup>6</sup> Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (ETS No. 108, Strasbourg, 1981). At: <http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm> (Report #108);

not deviate from those purposes. The holder of the data must guarantee its exactness, including the possibility of periodic correction and updating. However, at the same time, he must implement appropriate means of protection in order to safeguard the data from unauthorized access or modification. According to the convention, the means of protection of a person's privacy must be verified. Therefore, individuals whose details are included in the data must receive access to the information in such a way as to be able to determine the existence of the data file, its purpose, and the identity of the agency controlling the data. The individual must also have the possibility of receiving confirmation that the personal data is indeed stored, as well as confirmation of corrections or deletions. However, the convention recognizes exceptions that may be anchored in the national legislation of a country for purposes of protecting state security, public security, and the financial affairs of the State or for purposes of enforcing criminal law or defending the rights of others.<sup>7</sup>

This regulation, even though it is at the level of guidelines only and does not constitute normative law, is found in the United Nations Guidelines Concerning Computerized Personal Data Files.<sup>8</sup> This document only provides an outline, leaving the actual implementation of the regulation on automated personal data to each country's discretion. The following list of guidelines defines a series of principles in relation to a minimum standard of privacy at the national level:

- **Principle of lawfulness and fairness** – Information about persons should not be collected or processed in unfair or unlawful ways.
- **Accuracy** – Persons responsible for keeping the data have an obligation to conduct regular checks on the accuracy and relevance of the data recorded.
- **Purpose-specification** – The purpose for which the data is collected must be specified, legitimate and known, so that it will be possible to limit the storage to the area, time and capacity of use.
- **Access** – Anyone who offers proof of identity has the right to know whether information concerning him is being collected.
- **Non-discrimination** – Subject to cases of exceptions, data likely to give rise to discrimination, including information on racial or ethnic origin, color, sexual orientation, political opinions, religious,

---

<sup>7</sup> Yehonatan Bar-Sadeh, *Ha-Internet Vehamishpat Hamishari Hamekuvan*, The Internet and On-line Commercial Law 184–86 (Tel Aviv: Perlstein-Genosar, 1996).

<sup>8</sup> See: United Nations Guidelines Concerning Computerized Personal Data Files, adopted by the General Assembly on December 14, 1990.

philosophical and other beliefs, as well as membership in an association or trade union, should not be compiled.

- **Power to make exceptions** – Deviations from these guidelines may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as the rights of others, provided that such deviations are expressly specified in a law and that their limits are expressly stated. With regard to the prohibition of discrimination and related data, additional safeguards are required within the limits prescribed by the International Bill of Human Rights.
- **Security** – Appropriate measures should be taken to protect data files against accidental loss or destruction or intentional tampering.
- **Supervision and sanctions** – The law of every country shall designate the authority that is to be responsible for supervising observance of the principles set forth above. In the event of a violation, criminal or other penalties should be sanctioned and appropriate remedies provided.
- **Trans-border data flows** – When the legislation of two or more countries concerned by a trans-border data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as within each of the territories concerned.
- **Application** – The principles should also be extended to data that is not stored by computerized means. The principles also apply to the data files in the possession of government agencies, subject to appropriate adjustments.<sup>9</sup>

Another international regulation on electronic data, although it has lesser importance, consists of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Recommendation of the Council.<sup>10</sup> These guidelines set down the basic principles regarding collection, use, and disclosure of personal data and information. The guidelines recommend the following:<sup>11</sup>

- a restriction in local law to be imposed on collection of personal data;
- transparency with regard to the purposes of collection of the information and the intended uses of the information;
- disclosure of personal data only with the owner's consent;

---

<sup>9</sup> See: [http://europa.eu.int/comm/internal\\_market/privacy/index\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/index_en.htm)

<sup>10</sup> OECD, "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981: [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1,00.html)

<sup>11</sup> Bar-Sadeh, *supra* note 7, at 186–87.

- development of protections anchored in law;
- adoption of a policy of openness regarding personal data and safeguarding of the right of the individual to receive confirmation that data concerning him was collected, as well as the right to study the data, to verify that it is correct, and to protest data that is erroneous.

### ***2.1.3 International Regulation of Encryption Products***

On the international scene, we note a clear trend toward limiting (or even abolishing) control over encryption products and services.<sup>12</sup> In most countries of the Western world, it is now possible to freely create, use, and sell encryption products and encryption services. In line with the international report on encryption,<sup>13</sup> we can identify two policymaking bodies as the key players in rejecting limitations on encryption and developing a competitive, open market for encryption products: the European Union (EU) and the Organization for Economic Cooperation and Development (OECD).

### ***2.1.4 International Regulation of Decryption Products***

When an individual wants to protect his private information, he may choose to do so in a number of ways. In the home, digital protection mechanisms may be found in the form of a Pay TV decoder or in the form of a password upon entering a virtual shopping site or server. Each of these systems requires decryption in order to access and use the information.

International law regarding decryption has been enacted in three main areas: protection by means of legal frameworks that complement intellectual property rights (copyright), legislation related to conditional access to encrypted services, and legislation dealing with databases.

Copyright, in essence, provides its owner or holder with the right to control certain specified uses of his work. In recent years, various devices have been developed to offer technological protection of an individual's work. The law has chosen to recognize the right of the copyright holder to

---

<sup>12</sup> Cryptography & Liberty 1999/2000, E-commerce: A Guide to the Law of Electronic Business 63 (Daniel Tunkel & Stephen York eds., 2nd ed., 2000), available at <http://www.gilc.org/crypto/crypto-survey-99.html> and <http://www2.epic.org/reports/crypto2000/> (12.12.01).

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

use such devices in order to protect himself and his work in situations where others would like to circumvent those devices. The main legal arrangements that provide preferential status for technological means used in protecting copyright are the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).<sup>14</sup> These treaties are the work of the World Intellectual Property Organization, and underlying the organization's treaties are the Paris and Berne Conventions. They are aimed at updating the international protection given to copyright and related rights in the Internet age, taking into account developments in digital technology.

In accordance with the WCT, the creator-author of a work is entitled to legal protection regarding the distribution, commercial hiring, and public broadcast of his work over a network. Specific protection is given to systems for identifying and managing the author's work. Section 11 of the treaty provides protection against the circumvention of the technological measures that protect the author's rights.

## **2.2 The United States**

### ***2.2.1 Protection of the Right to Privacy***

The right to privacy is protected in the US by the Fourth Amendment to the Constitution:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.<sup>15</sup>

The Fourth Amendment restricts the American government's power to invade the privacy of the country's citizens and obliges the government not to infringe upon these rights without legal cause. It also sets a standard of "probable cause"<sup>16</sup> needed when the government wishes to intercept communications or obtain a search warrant, as carrying out actions of this kind may infringe upon the right to privacy of the person under surveillance.

---

<sup>14</sup> See: <http://www.wipo.int/treaties/>

<sup>15</sup> U.S. Const. Amend. IV.

<sup>16</sup> See *United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987).

This protection is supported by a system of checks and balances established in the various laws and case law.

In October 2001, the US Patriot Act was promulgated. This Act reinforced and extended the surveillance powers of US domestic law enforcement authorities and international intelligence agencies. It is argued by some that this Act violates the system of checks and balances that was shaped in the 1970s, following the uncontrolled use of surveillance powers by various agencies (when over 10,000 citizens were placed under permanent surveillance, including Martin Luther King).

Under the new law, the court can oblige a service provider to deliver mail logs and addresses of a specific person if the government is able to present facts to show that the records are relevant to an investigation in progress. The question is whether this standard corresponds to the “probable cause” condition in the Fourth Amendment. There are those who argue that a distinction must be made between the collection of “content data” concerning a specific person and the collection of “numerical information” (e.g., numbers that the individual dialed or e-mail addresses with which he corresponded), for which the collection standard can be lower.

The new Act introduced modifications in some fifteen laws. Many of these amendments infringed upon the right to privacy in the electronic communications between citizens. The government may now be entitled to monitor innocent surfers if they keyed in a concept that “arouses suspicion” in an Internet search engine. All that the government has to do is to swear before a court that the act might lead to information relevant to an investigation in progress. The person whose computer is monitored does not necessarily have to be the subject of an investigation or the suspect in any crime.

*Legal control of invasion of privacy by the enforcement agencies.* American law recognizes four surveillance means: (1) interception of broadcasts, including wiretapping (interception orders); (2) search and seizure orders of actual objects (search warrants); (3) orders for locating to whom or from where a call was made (pen/trap orders); and (4) subpoena and court orders (for obtaining of information). The various warrants and orders require different levels of certainty and legal intervention in direct relation to the expected invasion of rights (such as privacy and freedom of speech).

*Secret monitoring and interception.* Intelligence agencies are not restricted in the employment of surveillance means outside the US. There is no legislation on the matter, apart from a directive of President Reagan,



which is valid to this day.<sup>17</sup> The directive established that if a “United States person” is the subject of secret monitoring, then authorization must be received from the Attorney General, who has the power to decide whether there is probable cause that the target is a foreign agent.<sup>18</sup>

Two laws regulate surveillance within the US. One is the Federal Wiretap Act (1968),<sup>19</sup> which allows operation of surveillance and secret monitoring means through a court order after it has been demonstrated that there is probable cause that a crime has been committed, is being committed, or will be committed. The law contained a closed list of crimes for which a wiretap order can be given.<sup>20</sup> In the new law,<sup>21</sup> terror acts and offenses in line with the Computer Fraud and Abuse Act were added to the list.<sup>22</sup>

The Foreign Intelligence Surveillance Act of 1978 (FISA)<sup>23</sup> allowed the issuing of wiretapping orders by a special court for agents of a foreign power.<sup>24</sup> Here too, probable cause must be shown. However, in order to issue an order for someone who is a US person, it must be shown that the

---

<sup>17</sup> Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. § 401 note.

<sup>18</sup> “United States person” means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in § 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of whose members are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States. The definition does not include a corporation that is associated with a foreign power, as defined in 50 U.S.C. § 1801(a)(1), (2), or (3). See 50 U.S.C. § 1801(i).

<sup>19</sup> The Omnibus Crime Control and Safe Streets Act of 1968, commonly known as the “wiretap law.”

<sup>20</sup> 18 U.S.C. § 2516(1).

<sup>21</sup> US Patriot Act §§ 201–202.

<sup>22</sup> Computer Fraud and Abuse Act (CFAA), 18 USC § 1030.

<sup>23</sup> Pub. L. No. 95–511, 92 Stat. 1783, codified as 50 U.S.C. § 1801.

<sup>24</sup> See: United States Signals Intelligence Directive, July 27, 1993. The term ‘agent of a foreign power’ is defined as follows:

a. Any person, other than a U.S. person, who:

- (1) Acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation thereof;
- (2) Acts for, or on behalf of, a foreign power that engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

b. Any person, including a US person, who:

information is essential for national security, whereas for an individual who is not a US person, it must be shown that the information is related to national security. The definitions of an agent of a foreign power should be noted. According to this definition, the membership of a US citizen in a terror organization does not correspond to the definition of an “agent of a foreign power.” To be classified as such an agent, the citizen must work to advance the terrorist objectives. The distinction lies in the protection that the First Amendment gives to American citizens, wherein membership and activity in a terror organization may be for the advancement of a specific idea, and the citizen cannot be systematically prevented from expressing his opinion. In emergencies (to protect life and limb), it is possible to implement surveillance means in pursuance of both laws, even without a court order.

*Pen/Trap Orders.*<sup>25</sup> The purpose of these orders is to find the location of outgoing or incoming calls. The courts approve the orders as long as they can provide relevant information for a criminal offense, and their discretion is mainly technical regarding the manner of filing the application. Section 216 of the new Act extended the authorization for tracing calls from line communications to electronic communications.<sup>26</sup> Section 214 of the new Act also extended the possibility of issuing a warrant within the counterintelligence framework (FISA) in cases of terror, but forbade opening an investigation of a citizen due to First Amendment considerations.<sup>27</sup>

The FBI’s Carnivore system carries out similar activity on the Internet. The system is located at large data nodes and traces the source and the target of the messages transmitted over the Internet. The problem created is

- 
- (1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; or
  - (2) Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; or
  - (3) Knowingly engages in sabotage or international terrorism, or activities that are in preparation, for, or on behalf of, a foreign power; or
  - (4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in such activities.

<sup>25</sup> “Pen registers” are devices used to record telephone numbers that are dialed from a telephone; “trace devices” are used to determine where a telephone call originated.

<sup>26</sup> US Patriot Act §§ 216–202.

<sup>27</sup> *Id.* § 214.

that the system actually scans a very large quantity of data in order to find a specific piece of information for which the trace has been authorized. Another problem is that it is impossible to separate between the content and the data concerning the target, because they are transmitted together. Since the FBI does not specify the method of operation of the existing system, it is feared that such a system could collect not only information about the sender and receiver, but also information on the contents of the communication.

*Search and seizure orders.* Search warrants are issued by a judge when there is probable cause that a crime has been committed. At the time of or after execution of the search, the owner of the premises must be notified that a search was carried out. However, the new Act extends the power to secret searches in which the owner of the premises does not know that a search was carried out on his property/belongings. Search warrants also apply to seizing data that was received and stored by electronic means, including e-mail that has not yet been read.<sup>28</sup> The new Act allows interception, by search warrant, of line communication stored data, including voice mailboxes.<sup>29</sup> Under FISA, it is possible to carry out searches, without judicial control, with the authorization of the Attorney General.<sup>30</sup> Within the framework of this law, an investigation and search against a US citizen will not be carried out because of the freedom of speech protected by the First Amendment.

*Receipt of information collected by access providers.* Law enforcement agencies may request and receive information for purposes of carrying out investigations. Requesting the information is not subject to legal control. The new Act empowered law enforcement agencies to order and receive more extensive information from communications providers than in the past, including the time and duration of the telephone calls and Internet surfing, IP addresses, method of payment, and details of the person making the payment.<sup>31</sup> The authorities can order commercial records, such as data on transactions carried out by e-commerce and any non-content information related to subscribers.<sup>32</sup>

Section 217 of the new law allows for the study of information seized in computer trespasser communications.<sup>33</sup> The rationale for giving such

---

<sup>28</sup> 18 USC § 2703 (a) and (b).

<sup>29</sup> US Patriot Act, § 209.

<sup>30</sup> 50 USC § 1822.

<sup>31</sup> US Patriot Act, §§ 210, 211.

<sup>32</sup> 18 USC § 2703 (c).

<sup>33</sup> US Patriot Act § 217.

permission is that anyone hacking into a computer cannot expect privacy of his data. The new act allows the ISP to provide non-content data, without a warrant, voluntarily, to protect life and limb.<sup>34</sup>

The Communications Assistance for Law Enforcement Act (CALEA)<sup>35</sup> demands that communications companies adapt their systems to fulfill the control requirements of law enforcement agencies.

### ***2.2.2 Protection of the Freedom of Speech***

Issues about the preservation of freedom of speech have arisen in two contexts in the United States, with specific reference to encryption and decryption software. American law has viewed this issue from the perspective of the doctrine of “symbolic behavior” – a doctrine that was developed before the advent of digital technology. Case examples include public burning of the country’s flag or draft cards in order to protest a government policy. The O’Brien case that came before the United States Supreme Court in the 1960s illustrates this point.<sup>36</sup> Paul David O’Brien and others publicly burned their draft cards, claiming that they did so in protest against the Vietnam War. O’Brien was arrested and placed on trial on the charge of burning his draft card in contravention of a 1965 law. The Supreme Court rejected the argument that all behavior or actions can be considered “speech” when carried out to express an idea or position. Moreover, the Court analyzed the situation in which action (behavior) and “speech” (in its First Amendment sense) were intertwined, and came to the conclusion “that when ‘speech’ and ‘non-speech’ elements are combined in the same course of conduct, a sufficient government interest in regulating the non-speech element can justify limitations on First Amendment freedoms.” Thus in this type of case, an absolute standard of protection for freedom of speech need not be applied. Rather, a somewhat lower standard, known as “intermediate scrutiny,” may be applied.<sup>37</sup> Chief

---

<sup>34</sup> *Id.* § 212.

<sup>35</sup> 18 U.S.C. § 2522.

<sup>36</sup> *United States v. O’Brien*, 391 U.S. 367 (1968).

<sup>37</sup> American legal decisions accept three standards for evaluating the extent of protection for freedom of speech. The highest standard, “strict scrutiny,” is applied when the State prevents certain speech or the State discriminates between different types of speech based on their content. A lower standard, “intermediate scrutiny,” is used by the courts when the limitation on speech is not based on its content; according to this standard, the court weighs the free speech rights of the speaker against the national interest in limiting that speech, with the weightier

Justice Warren established a number of conditions for public regulation, which, when present, justify the limitation of First Amendment rights:

1. The regulation is within the constitutional power of the government;
2. The regulation furthers some important governmental interest;
3. The regulation is not designed to restrict freedom of speech;
4. The incidental limitation on freedom of speech is not greater than necessary to promote the governmental interest.

In the O'Brien case, it was ruled that the law under discussion was not aimed at restricting freedom of speech, but rather at ensuring the effectiveness of the draft procedure (the governmental interest). Thus, O'Brien was not placed on trial for his opinions, but because of his behavior, which damaged the national interest.

The question arises as to whether it is possible to adopt the O'Brien ruling in the context of encryption software. American courts have not been consistent on this issue.

The first instance is known as the Karn case. Philip Karn, a programmer working on cellular technology, requested a permit to export source code for encryption algorithms on diskette. The same algorithms had already been published in book form prior to Karn's request to export them digitally.<sup>38</sup> Although the book had been declared by the Department of State and the Department of Commerce to be a freely exportable commodity, these same bodies ruled that the export of the code in digital form was prohibited under the regulations controlling the export of encryption software. Karn appealed the Administration's decision to the District Court in the District of Columbia.<sup>39</sup> His argument was that the diskette constituted "speech," particularly since the program code included programmer comments, which were not aimed at the computer running the program, but at a human reader looking at the source code and trying to understand it. As the issue was one of expression, the diskette should be protected by the freedom of speech protections under the First Amendment. On this basis, Karn argued that the prohibition against exporting the diskette was unconstitutional and thus null and void.

The court rejected his case. Although the court agreed that the protections offered by the First Amendment also apply to program code, it

---

interest winning. The third, and lowest, standard is called "rational basis;" here the speaker has to show that state regulation does not have any logical basis.

<sup>38</sup> See Bruce Schneier, *APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE* in C 151–54 (2nd ed., New York, Wiley, 1996).

<sup>39</sup> Karn, Jr. v. U.S. Department of State, et al., 925 F.Supp. 1 (D.D.C. 1996).

ruled that when the restriction on speech is not content-based, but rather content-neutral, this implies that it is designed to restrict some other function that the speech serves, and is thus justified if it meets the conditions established in the O'Brien case.<sup>40</sup> In this case, the court ruled that the O'Brien test was met. The regulation of software exports is within the government's powers. Such regulation is not aimed at restricting freedom of speech, but at promoting an important governmental interest (here, to make it difficult for hostile states to interfere with the access of the United States government to information essential for national security); and the incidental limitation on freedom of speech is in appropriate measure.<sup>41</sup> It is important to note that Karn attempted to argue that the O'Brien test applied only to *behavior* that included in it speech. However, the court rejected that argument and ruled that the test applied to any form of expression.<sup>42</sup>

The Bernstein case led to a contrary decision in which freedom of speech had the upper hand. Daniel Bernstein, who was a mathematician researching cryptography at the University of Illinois in Chicago and the University of Berkeley in California, developed a novel encryption algorithm as part of his academic work. Bernstein wanted to distribute and export the program, which he called "Snuffle," accompanied by an article in which he analyzed and explained the program code. He also wished to share his findings at academic conferences, including some outside the United States. His intention was to disseminate his ideas within the scientific community throughout the world as part of the normal academic exchange of ideas and information. The Export Regulations prevented Bernstein from publishing or discussing his work – a move which, in his opinion, harmed his career and reputation. In 1996, Bernstein appealed to the United States District Court in California, claiming that his freedom of speech rights had been violated. Judge Marilyn Hall Patel ruled that the encryption program was a form of speech that was entitled to First Amendment Protection, because anything written in any language is, by

---

<sup>40</sup> *Id.* at 10.

<sup>41</sup> *Id.* at 11.

<sup>42</sup> The court rejected Karn's appeal for another, additional, reason – that the Arms Export Control Act established that decisions made by those authorized under that law were not subject to judicial review. Karn appealed the judgment, but the appeals court returned the case to the court of first instance (107 F.3d 923). The case was transferred because prior to consideration of the appeal, authority for issuing regulations restricting the export of encryption software was transferred from the Department of State to the Department of Commerce, and the latter was due to issue new regulations regarding that subject.

definition, a form of expression entitled to constitutional protection.<sup>43</sup> Further, Judge Patel ruled that the procedures for licensing encryption software constituted prior restraint on freedom of speech.<sup>44</sup> Finally, on this basis Judge Patel ruled that the Export Regulations were unconstitutional.<sup>45</sup>

The United States Court of Appeals for the Ninth Circuit, in a three-judge panel, upheld the ruling issued by Judge Patel,<sup>46</sup> but in a slightly more restrictive manner. The Export Administration Regulations were found to be unconstitutional, but not in an all-encompassing sense. An unconstitutional restriction can occur when the Administration imposes a restriction that prevents the flow of scientific ideas (whether by means of source code or some other means) without distinguishing between those and encryption products as commodities. In essence, the court ruled that not every program can be considered expressive speech. Only when “[c]ryptographers use source code to express their scientific ideas in [. . .] the same way that mathematicians use equations or economists use graphs” does the Constitution provide protection under the First Amendment.<sup>47</sup> Although the specific expression under discussion also includes a “non-speech element,” the court noted that the O’Brien ruling does not have to be applied in all cases. In light of the prior restraint of freedom of speech, the court applied the highest standard in examining the extent of First Amendment protection.

In response to this decision, the United States Justice Department petitioned the court for a rehearing in the Bernstein case by an expanded panel. The court accepted the petition and withdrew the ruling by the three-judge panel.<sup>48</sup> However, changes in encryption export policy made the appeal hearing unnecessary and the case was returned to the District Court.

The third case dealing with the issue of encryption software and freedom of speech is the Junger case. Professor Peter Junger was a lecturer at Case Western Reserve University in Cleveland who was teaching a course in “Computing and the Law.” Junger wrote a number of very basic encryption programs and wanted to place them on the course’s Internet site in

---

<sup>43</sup> *Bernstein v. United States Department of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996).

<sup>44</sup> *Bernstein*, 945 F. Supp. at 1279.

<sup>45</sup> *Bernstein*, 974 F. Supp. 1288 (N.D. Cal. 1997).

<sup>46</sup> *Bernstein v. United States Department of Justice*, 176 F.3d 1132 (9th Cir. 1999).

<sup>47</sup> *Id.* at 1141, 1145; Judge Nelson, in a minority ruling, held that computer software cannot be considered speech.

<sup>48</sup> *Bernstein v. United States Department of Justice*, 192 F.3d 1308 (9th Cir. 1999).

order to show his students “how a computer works.” However, he was required to obtain an export license from the Department of Commerce because under the International Traffic in Arms Regulations (ITAR), cryptographic computer software is considered a “munition.”<sup>49</sup> His application for the license was refused. Junger appealed to the Federal District Court in Ohio, claiming that his First Amendment rights had been violated.<sup>50</sup> The court accepted the position of the government and ruled that the export of cryptographic software is not protected by the First Amendment, even if encryption software occasionally includes a “speech” component. The explanation was that software primarily provides functionality and that expression is only a secondary aspect. Junger appealed to the Court of Appeals for the Sixth Circuit,<sup>51</sup> which rejected the decision of the lower court. In the appeal, the court ruled that the functional characteristics of source code do not overshadow its expressive nature and that the O’Brien ruling should be applied in such cases.

In two other cases, known as the DVD judgments, the courts in New York and California ruled on the constitutionality of restrictions on the publication and dissemination of software to break digital protection mechanisms. Here, too, the courts were not of one mind in their judgments.

The factual background of the two cases is almost identical. The American film industry attempted to protect its investment in films in digital format on DVD by means of a technology called Contents Scramble System (CSS), which is designed to prevent unlicensed viewing of the film or of a copy. A Norwegian teenager wrote a program – DeCSS – that broke this protection technology (according to the writer, with the aim of allowing the viewing of DVD films on computers operating under Linux). The code for the decryption program was disseminated to universities through the Internet, and the plaintiffs, who were interested in finding the most effective way of cutting off its distribution, decided to sue the operators of the websites that distributed the code.

In the first case, which was heard in New York, the main defendant was a well-known hacker named Eric Corley, who placed a copy of the decryption program on his website. The film companies sued him on the basis of the explicit provisions of the Digital Millennium Copyright Act (DMCA), which prohibits the publication or distribution of software that

---

<sup>49</sup> 15 C.F.R. § 734.2(b)(9).

<sup>50</sup> *Junger v. Daley*, United States Secretary of Commerce, 8 F.Supp.2d 708 (N.D. Ohio 1998).

<sup>51</sup> *Junger v. Daley*, United States Secretary of Commerce, 209 F.3d 481 (6th Cir. 2000).



can break digital protection mechanisms.<sup>52</sup> Judge Lewis A. Kaplan, sitting on the District Court,<sup>53</sup> ruled in favor of the film companies. Corley appealed, but the appeal was rejected.<sup>54</sup> One of Corley's main arguments was that applying the DMCA to the distribution of the decryption program violated his constitutional rights to freedom of speech, because it had already been ruled that computer code is a form of protected speech under the First Amendment. Both courts agreed that computer code does constitute protected speech.<sup>55</sup>

Judge Jon O. Newman, sitting on the Court of Appeals, agreed with the designation of computer code as protected speech and provided an interesting analogy. Just as musical notes, which constitute protected speech, are only comprehensible to musicians, so is decryption code comprehensible only to programmers.<sup>56</sup> The extent of the protection of speech is influenced by the nature of the program as a combination of a speech element and a functional, non-speech element.<sup>57</sup> Thus, the appropriate standard to be applied when determining the level of protection is that of "intermediate scrutiny," rather than the absolute standard. In other words, the appropriate test to apply in this instance is the O'Brien test.<sup>58</sup> Furthermore, the court ruled that the DMCA was not aimed at inhibiting freedom of speech, but at serving another important, constitutional interest, namely protecting copyright works and preventing "piracy." Therefore, the limitation on freedom of speech imposed by the law was proportionate and the DMCA prohibition on the distribution of DeCSS was constitutionally valid.<sup>59</sup>

Similar proceedings took place on the West Coast of the United States in a suit submitted by the DVD Copy Control Association (DVD CCA). DVD CCA is the holder of the rights to the DeCSS system and licenses the installation of the system to producers of DVD players. The suit named Andrew Bunner, who published the DeCSS program on his website, as the defendant. However, the decision of the California court was fundamentally different from that of the courts in New York. This time, freedom of speech won out. Under the Uniform Trade Secret Act, the lower

---

<sup>52</sup> 17 U.S.C. § 1201(a)(2), (b)(1).

<sup>53</sup> *Universal City Studios, Inc. v. Reimerdes*, 111 F.Supp.2d 294 (S.D.N.Y. 2000).

<sup>54</sup> *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2nd Cir. 2001) (*Universal I*).

<sup>55</sup> *Universal City*, 111 F.Supp.2d, at 327.

<sup>56</sup> *Universal II*, 273 F.3d, at 445.

<sup>57</sup> *Universal City*, 111 F.Supp.2d, at 328–29.

<sup>58</sup> *Universal City*, 111 F.Supp.2d, at 329–30; *Universal II*, 273 F.3d, at 450.

<sup>59</sup> *Universal City*, 111 F.Supp.2d, at 330–33.

court issued an injunction against Bunner and others, ordering them not to publish or distribute DeCSS on the grounds that the decryption program contained CSS trade secrets. Bunner appealed to California's Appellate Court, which overturned the original ruling. Again, the court held that computer code constitutes protected speech under the First Amendment, but in this instance, the court did not adopt the O'Brien test and permitted publication of the code. The reasoning was as follows: In determining the balance between freedom of speech and trade secrets protection, which is not a constitutional protection, the court applies the highest standard, rather than the "intermediate scrutiny" standard, which corresponds to the O'Brien test.<sup>60</sup> It may be that the plaintiff's strategy undermined the claim, as the plaintiff only made a trade secrets argument against the alleged freedom of speech violation and did not present arguments based on copyright and DMCA infringement issues.<sup>61</sup>

### ***2.2.3 American Regulation of Encryption Products***

In recent years, the legal policy applying to encryption in the United States has undergone a fundamental change, with a move toward reducing restrictions and governmental control. Until 1996, the export of the means of encryption with a key length (strength) above 40 bits<sup>62</sup> was considered an export of munitions, and the control of trade in encryption means was carried out through the ITAR – International Traffic in Arms Regulations. Due to these severe restrictions and in order to respond to the needs of the software market, in 1993 the Administration proposed the idea of the Clipper Chip as a means of encryption. With control over licensing, the Administration would also retain the ability to decipher the Clipper Chip and to access any content encrypted therein. The idea was not successful. Opposition came from software companies, which were restricted in terms of software exports and competitively disadvantaged in world markets, as well as from human rights organizations and privacy advocates.

In November 1996, the Administration changed its position. The previous policy of a sweeping prohibition with limited exceptions was replaced

---

<sup>60</sup> DVD Copy Control Association v. Bunner, 113 Cal. Rptr. 2d 338, 350–51.

<sup>61</sup> Haim Ravia, "Pitzuah Ha-DVD [Cracking the DVD]." <http://www.law.co.il/hebarticles/bunner.htm>.

<sup>62</sup> For a technical explanation, see Chapter 4.

by a regime of export restrictions with exemptions.<sup>63</sup> Encryption means were now only considered as munitions if they were for military purposes. The Administration's goal was to support electronic commerce, protect global information infrastructures, protect privacy and intellectual property rights, and allow American companies to compete equally with their overseas counterparts. Authority for the control of encryption was transferred to the Bureau of Export Control (BXA), which is subject to the Department of Commerce. Encryption items were reclassified and transferred from the Munitions Control list to the Commerce Control list. The new regulations created a process by which the owner of means of encryption with a key length of up to 40 bits could have the product removed from the Commerce Control list after a single examination by the Bureau of Export Administration (BXA) and would then be exempt, in practice, from any export restrictions.<sup>64</sup> Similarly, it was possible to obtain an export license, but not removal from control, for encryption items that operated with 56-bit keys using DES technology<sup>65</sup> (or equivalent), subject to two conditions: first, a one-time examination of the product prior to export, and second, the existence of Key Escrow or Key Recovery technology to circumvent the encryption.<sup>66</sup>

The Administration is entitled to establish restrictions on export without the need for separate legislation, by virtue of emergency legislation.<sup>67</sup> A trend toward liberalization in the area of encryption exports from the United States, first evidenced by a series of permits issued in 1998 and 2000, which are described in detail below, continues today. However, closer examination of the regulations shows that political, economic and security considerations influence the possibilities of export to various countries.

As of this writing, there is no restriction on production or commerce of the means of encryption of any strength within the United States. Outside the United States, regulation is conducted by means of export regulations implemented by the BXA which is responsible for the administration

---

<sup>63</sup> Executive Order 13026 (November 15, 1996).

<sup>64</sup> 61 FR 68572 (1996), [http://w3.access.gpo.gov/bxa/fedreg/ear\\_fedreg96.html#encryption1](http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg96.html#encryption1)

<sup>65</sup> For a technical explanation of DES, see Chapter 4.

<sup>66</sup> These terms mean that a third party, who is not the owner of the encrypted information, will have the possibility of deciphering the information. The regulations define who can be the third party and the manner in which that party can be contacted in order to decipher the information.

<sup>67</sup> International Emergency Economic Power Act (IEEPA), codified as 50 U.S.C. § 1701; National Emergencies Act, codified as 50 U.S.C. § 1601; The Export Administration Act, codified as 50 U.S.C. § 2401.

of the export of encryption items.<sup>68</sup> The only blanket prohibition that remains in force is the export of means of encryption to states that support terrorism or their citizens.<sup>69</sup>

The first set of permits in the area of encryption exports from the United States was issued in 1998.<sup>70</sup> The most significant step in that year was the Administration's waiver of the blanket requirement for the means to decipher encrypted messages (back door). A further step was the strengthening of the technological defenses of financial institutions. Following are some of the changes implemented in that year:

- It is permitted to export, subject to license and after examination, technologies integrating means of encryption, to banks and financial institutions (including insurance companies), in 45 countries,<sup>71</sup> without the means of decipherment,<sup>72</sup> and without restriction on the strength of encryption. This permit is designed not for mass-marketing products, but for a limited market and for the purpose of carrying out secure transactions between financial institutions and their clients.
- An export permit is allowed for all encryption up to 56-bit strength after technical examination.
- It is permitted to export encryption to American subsidiaries or branches of American companies outside the United States.
- It is permitted to export encryption technologies for electronic commerce, under license, to 45 countries, on condition that the transactions are secured and that direct customer-to-customer communications are not carried out.
- A permit may be issued to export encryption commodities or software for health and medical uses to 45 countries without limitation on the strength of encryption, provided these are designated for end-users only.

---

<sup>68</sup> See Export Administration Regulations 740.13, 740.17, 742.15. <http://www.bxa.doc.gov/Encryption/Default.htm>.

<sup>69</sup> The states supporting terror, according to the American Government, are Syria, Iran, Iraq, Libya, Sudan, North Korea, and Cuba. Additional information relating to the policy of defining states as terror-supporting can be found in a document by the Congressional Research Service from March 2001, which deals with Terrorism and United States Foreign Policy: <http://www.fas.org/irp/crs/IB95112.pdf>. An additional explanation can be found at the State Department website: <http://www.state.gov/www/global/terrorism/1999report/sponsor.html>.

<sup>70</sup> See 63 FR 50516 (09.22.98), 63 FR 72156 (31.12.98), available at: <http://www.bxa.doc.gov>.

<sup>71</sup> See: Supplement No. 3 to (EAR), 15 C.F.R. Sections part 740. Today this Section no longer appears, since the restrictions are no longer unique to these countries.

<sup>72</sup> Key escrow or key recovery.

- Anyone who received an exemption from export restrictions for 40-bit encryption may upgrade the product to 56 bits.

Changes in 2000<sup>73</sup> led to a much more liberal situation regarding the export of encryption items, in particular to the countries of the European Union. After 2000, it became possible to export products and software that included encryption of any strength to companies, individuals, and non-governmental organizations without license and after a technical examination only. The mechanism of examination at an early stage and post-export reporting requirements provide the Administration with information regarding the strength and final destination of the encryption technology. These regulations facilitate business for communications companies and Internet service providers by allowing them broader use of encryption. Producers of short-wave radio technologies also benefit. Following are some of the key changes resulting from the legislation passed in 2000:

- After examination by the Administration, commodities or software with encryption of any strength may be exported to individuals, companies, and other non-governmental end-users. Similarly, it was now permissible to distribute encryption to all destinations, because uploading of an encryption item to the Internet no longer constituted “knowledge” of transfer of encryption to a terror-supporting state. The amendments allowed the exporter to simply notify the Administration that encryption means had been exported.<sup>74</sup>
- The regulations simplified export to countries of the European Union and additional countries in Europe, as well as Japan, Australia, and New Zealand.
- The regulations simplified the export of encryption items designed for short-wave radio technologies.
- It was now permissible to export encryption items to American companies outside the United States without prior technical examination. Encryption companies operating in the United States that employ foreign nationals no longer required an export license.

---

<sup>73</sup> See 65 FR 62600 (19.10.00), 65 FR 2492 (14.1.00), <http://www.bxa.doc.gov/encryption/default.htm>. See also the statement by the White House regarding the change in policy relating to the export of encryption: <http://www.cdt.org/crypto/CESA/whousepress091699.shtml>.

<sup>74</sup> In 2002, The Bureau of Export Administration (BXA) fined a software company, NeoPoint, for knowingly exporting 128-bit encryption software to South Korea without a license.

- It was now permissible to export Open Source Code subject to license, but the Administration had to be notified regarding the location of the code.<sup>75</sup>
- The regulations permitted communications companies and Internet service providers to integrate encryption in the services they provided.
- In most cases, there was an obligation to allow the BXA a one-time examination of the product.

These changes reduced the criticism of human rights and privacy organizations. The Center for Democracy and Technology<sup>76</sup> published two criteria by which the policy should be measured. The first is the extent to which the export regulations limit people around the world from using encryption technology in order to protect their privacy. The second is the freedom given to individuals to participate in the information economy without contravening US law. Based on these criteria, the Center raised certain criticisms of the new regulations, specifically in four areas:<sup>77</sup>

- The export permit was only granted for products that were “sold” (for payment), which means that there was no express permit for the free distribution of products containing encryption items, including products that were distributed online at no charge, such as secure Internet browsers.
- The broad definition of “government,” which includes any state-owned or related organization or corporation, placed too high a demand on small businesses and individuals who would like to export strong encryption products to those bodies that are, unjustifiably, defined as governmental.
- The reporting and screening obligations that prevented strong encryption technologies from reaching terrorism-sponsoring states handicapped small and medium sized organizations and individuals from distributing these technologies. The reporting obligations regarding the destination of these technologies should take into account the fundamentally anonymous distribution of technologies through the Internet.

---

<sup>75</sup> Open Source Code is code in machine-readable language (See Computers Law, 5745–1995, Section 1, Definitions), which may be modified or from which encryption algorithms can be extracted. The term “open” means that the code is accessible to the public.

<sup>76</sup> <http://www.cdt.org>.

<sup>77</sup> See details of the Center’s position in the letter to the BXA: <http://www.cdt.org/crypto/admin/991206comments.shtml>

- The restrictions on the export of encryption-related source code<sup>78</sup> affected the distribution of non-commercial source code designed for use and development by large numbers of users. Companies and organizations might be able to cope with the restrictions. However, the distribution of source code that was “not subject to any proprietary commercial agreement or restriction” created problems of enforcement, and the imposition of restrictions on everyone involved in developing the code was not practical.

### ***2.2.4 American Regulation of Decryption Products***

*American regulation of copyright.* The Digital Millennium Copyright Act (DMCA)<sup>79</sup> was passed by the United States Congress in 1998 as part of bringing American law into line with the 1996 WIPO Copyright Treaty.<sup>80</sup> This law is designed to prevent the circumvention of the technological measures that protect copyright works. The heart of the prohibition is in § 1201, which prohibits the circumvention of technological access measures.<sup>81</sup>

No person shall circumvent a technological measure that effectively controls access to a work protected under this title.

In addition, the law prohibits the production, sale, provision, or distribution of any measure that, wholly or in part, is designed to circumvent technological measures that protect copyrighted materials:<sup>82</sup>

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

Several questions may be asked about the extent of the prohibition: Does the law apply to the decryption of technological protections in general or only to those technological measures that protect works that are

---

<sup>78</sup> This refers mainly to encryption algorithms found in machine-readable source code.

<sup>79</sup> Pub. L. No. 105–304, 112 stat. 2860 (Oct. 28, 1998). <http://www4.law.cornell.edu/uscode/17/1201.html>.

<sup>80</sup> WIPO Copyright Treaty <http://www.gseis.ucla.edu/iclp/wipo1.htm> (1996).

<sup>81</sup> 17 U.S.C. § 1201(a)(1)(A).

<sup>82</sup> *Id.* § 1201(b)(1).

themselves protected by copyright law? The prohibition against deciphering technological protections is not limited to local (American) technologies, and therefore the deciphering of a protective technology that originates outside the United States is also an infringement of the law. The law establishes a civil offense, but when the infringement has been carried out for commercial advantage or private financial gain, then the infringement is also a criminal offense.<sup>83</sup>

The law establishes a number of general protections, including the protection given to acts for research, examination, and evaluation of protection mechanisms:

- The law does not override the authority of the Administration, intelligence services, or law enforcement agencies to carry out activities for the purpose of investigation, protection, data protection, and intelligence gathering.<sup>84</sup>
- There is an exception that permits the circumvention of technological access protections for the purposes of research aimed at finding flaws and vulnerabilities in encryption technologies.<sup>85</sup> This exemption was inserted because of the concern of lawmakers that the prohibition of decryption would hamper the development of research into the flaws in existing technologies.<sup>86</sup>
- The “fair use” defense does not justify decryption in contravention of the provisions of this section.<sup>87</sup>

The first criminal prosecution under this law was against a Russian citizen, Dmitri Sklyarov,<sup>88</sup> who developed a program that bypassed the technological defenses of eBook, a technology that belongs to Adobe. The program was developed for a Russian company called ElcomSoft,<sup>89</sup> which was also named as a defendant. In December 2001, a plea bargain agreement was signed, and the prosecution agreed in effect to waive

---

<sup>83</sup> *Id.* § 1204(a).

<sup>84</sup> *Id.* § 1201(e).

<sup>85</sup> *Id.* § 1201(g).

<sup>86</sup> See the reports of the various Congressional committees: H.R. Rep. No. 105–551, pt. 2, at 27 (1998); S. Rep. No. 105–190, at 15 (1998). One year after the law took effect, the legislature demanded a report on whether the law actually had a negative effect on encryption research. According to the report, it is still too early to draw conclusions. See: [http://www.loc.gov/copyright/reports/studies/dmca\\_report.html](http://www.loc.gov/copyright/reports/studies/dmca_report.html).

<sup>87</sup> 17 U.S.C. § 1201(c).

<sup>88</sup> For details of this case, see: [http://www.eff.org/IP/DMCA/US\\_v\\_Elcomsoft/](http://www.eff.org/IP/DMCA/US_v_Elcomsoft/).

<sup>89</sup> See the company’s website: [www.elcomsoft.com](http://www.elcomsoft.com).



Sklyarov's prosecution without a conviction being recorded.<sup>90</sup> The law has been interpreted in the context of a number of civil cases:

- Film companies sued to prevent websites from distributing the code that breaks the technological protections of DVD movies. Arguments regarding fair use and the unconstitutionality of the DMCA – in that it is restrictive of freedom of speech – were rejected by the initial court and the court of appeals.<sup>91</sup>
- In another case, also related to the question of DVD encryption, the California state courts dealt with the question of decryption in light of laws protecting trade secrets.<sup>92</sup> An interim decision removed the restraining order that prohibited distribution of the decryption code through websites. In this case, the court stated:

DVDCCA's [The Plaintiff] statutory right to protect its economically valuable trade secret is not an interest that is 'more fundamental' than the First Amendment right to freedom of speech or even on equal footing with the national security interests and other vital governmental interests that have previously been found insufficient to justify a prior restraint.<sup>93</sup>

- Another case related to a researcher who wanted to publish his research and was threatened with action under the DMCA. Professor Edward Felten cracked the protection technology of digital watermarks within the framework of a public competition sponsored by the developers of the protection scheme. Felten waived the prize with the intent of publishing the results of his research. However, he claimed, the music industry (the RIAA) threatened to sue him under the DMCA. Felten applied to the courts for a declarative judgment that would recognize his right to publish his research as a part of his right to freedom of speech. Although the District Court of New Jersey rejected his claim,<sup>94</sup> the music industry declared that it did not object to the publication.<sup>95</sup>

---

<sup>90</sup> Sklyarov testified against ElcomSoft. The court papers related to the plea bargain can be found on the Justice Department's website: [http://www.usdoj.gov/usao/can/press/assets/applets/2001\\_12\\_13\\_sklyarov.pdf](http://www.usdoj.gov/usao/can/press/assets/applets/2001_12_13_sklyarov.pdf)

<sup>91</sup> See: Universal, *supra* note 53, at 346, *aff'd* Universal City Studios, Inc. v. Corley 2001 WL 1505495 (2nd Cir. 2001).

<sup>92</sup> Trade Secret Act, Cal. Civ. Code, § 3426.1 et. seq.

<sup>93</sup> DVD CCA v. Bunner 93 Cal. App. 4th 648 (2001).

<sup>94</sup> Felten v. RIAA (D.N.J.)

<sup>95</sup> <http://www.wired.com/news/politics/0,1283,48726,00.html>.

The trend that appears to be developing in American law is to prohibit the decryption of codes that protect works subject to copyright protection. It is not yet possible to draw any conclusions regarding the prohibition of decryption within the framework of trade secret protection.

## 2.3 The European Union

The European Union exists by virtue of the treaties that created it (Treaty of Rome, the Single European Act, and the Treaty of Maastricht). In creating these treaties, certain areas were placed from the start in the Union's sole jurisdiction, while a few areas were made subordinate to a kind of "parallel authority" and others were left to the exclusive authority of the individual countries.<sup>96</sup> Due to this division of powers, numerous qualifications appear in the different legislative items of the European Union concerning areas that were left outside the Union's jurisdiction, including: (1) issues of security and general state interests (excluding economic interests) and (2) the possibility of creating local legislation that will allow exceptions to the provisions in these cases.<sup>97</sup> Another aspect of the division of powers cited above can be found in the issue of enforcing legislation in the private sector in various countries. An example of this occurs in the context of imposing obligations on a private entity (such as service providers) to act in accordance with the demands of the enforcement authorities.

---

<sup>96</sup> Eran Lev, *Mishpat Hakehiliya He-Eropait* THE EUROPEAN COMMUNITY LAW 32–4 (Bursi, 1994).

<sup>97</sup> The European Union's legislation is made up of four types of legislation: The treaty (convention) is the supreme legislative item and can be compared to a law in a federal state, but it does not have direct application within the countries; regulations, which are considered the legislative item closest to normative legislation in a sovereign state and which constitute the only legislative item in the Union that is directly applicable; directives are an "original" creation in that they constitute the legislation that determines binding objectives, but leave the member countries to determine how to implement the objectives; and decisions, which are at the lowest level on the normative scale and resemble an individual order. The use of regulations is more accepted in those fields where the EU has clear jurisdiction and as a tool for bringing the domestic law of the member countries into line. See Lev, *supra* note 97, at 43–45.

### ***2.3.1 Protection of the Right to Privacy***

The EU Directive on Data Protection of 1995<sup>98</sup> required member countries to create laws for the private sector regarding the right to privacy in the areas of the collection, processing, storage, and transmission of personal data. In fact, the Directive allows for the free movement of electronic data between countries of the EU, while guaranteeing that individuals will be protected against possible abuses of the data.<sup>99</sup> The main points of the EU Directive on Data Protection are provided below. Personal data is defined in the Directive as any information relating to an identified person or a person who can be identified, either directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.

The Directive defines several exceptions to the application of the regulation. Article 3(2) stipulates situations in which application to the entire data processing activity is qualified:

- In the course of an activity that falls outside the scope of EU law (in pursuance of the founding Treaty) and in any case of data processing operations concerning public security, defense, state security (including the economic well-being of the State), and the activities of the State in areas of criminal law. Within the framework of the treaties establishing the European Union, it was agreed that these laws would remain in the jurisdiction of the member countries; hence the reason for the exception.
- Processing of data by an individual in the course of a purely personal or household activity.

Domestic legislation in each country must be in line with the spirit of the Directive. However, Article 5 of the Directive expressly states that the countries may determine the precise conditions under which the processing of personal data is lawful.

---

<sup>98</sup> Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. For the wording of the Directive, see: [www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html](http://www.cdt.org/privacy/eudirective/EU_Directive_.html) (last visit: 24.12.01).

<sup>99</sup> Bar-Sadeh, *supra* note 7, at 187.

In respecting the Directive, every business must meet several conditions. First, the company must guarantee that personal data collected from customers will be used in a legitimate and fair way for specific, explicit, and legal purposes and that the data will be kept updated and properly stored. Additionally, the business must notify the customers of the person responsible for the data and offer the customer the right to access and correct the data if necessary. The Directive emphasizes that once collected, the data will be used only with the customer's clear consent. Violation of these obligations entitles the customer to compensation. The penalties assigned to the business will be in accordance with the laws of the member state. Each country in the EU was also required to establish an independent supervisory body with a variety of powers, including investigation, monitoring, and blocking of businesses that collect personal data on their customers.

Regarding countries outside the EU, a prohibition exists on the transfer of personal data to countries not complying with the European data protection standard. The US and the European Union reached an agreement called the "Safe Harbor Framework," whereby American companies would be considered as meeting the standard. However, American companies are still subject to independent, non-governmental regulation, according to these seven basic principles: notice, choice, limitation of onward transfer, security, data integrity, access, and enforcement.<sup>100</sup>

Regarding countries other than the US, on December 4, 2001 the committee of member states approved a proposal for standard contractual articles to be adopted by data-processing organizations in countries outside the EU. This proposal was designed to prevent the refusal of onward data transfer due to non-compliance with the treaty requirements.<sup>101</sup>

Although the Directive dates from 1995, the relevant legislation in many countries came into force only in early 2000. Furthermore, legal proceedings were carried out in the European court against five countries because of their delay in adopting appropriate legislation in accordance with the schedule determined in the Directive (Luxembourg, Denmark, Ireland, Germany, and France). Of these countries, only the first three have since issued the required law, which came into force in July 2000. All of Germany's provinces except Sachsen and Bremen have passed the

---

<sup>100</sup> For a report on the implementation of the agreement with countries outside the EU, see [http://ec.europa.eu/justice\\_home/fsj/privacy/thridcountries/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm) (The incorrect spelling of /thridcountries/in the link is correct)

<sup>101</sup> Ibid.

required legislation, and France has modified its existing laws, but has not yet entered them into effect.<sup>102</sup>

The European Union's 1995 Directive for Protection of Personal Data created a comprehensive working framework in which other directives and decisions were adopted to expand the scope of application of the principles. Additional provisions were subsequently added in relation to the telecommunications market, dealing mainly with various obligations imposed on ISPs. These additional provisions will be discussed separately in the section on data collection by commercial organizations below.

After September 11, another convention was signed that affected law enforcement agencies and their relations with service providers: the International Convention on Cyber-crime. This convention originated with the European Union<sup>103</sup> and was opened for the signature of the European countries and other countries that participated in its formulation (Israel was not one of them). As of May 2006, 38 countries have signed the convention, including the US, Canada, South Africa, Montenegro, and Japan.<sup>104</sup>

The explanatory notes clarify that the aim of the convention is to realize three main objectives: (a) the harmonization of national criminal law to incorporate the field of cyber crime; (b) the creation of national procedural powers needed for the investigation and prosecution of cyber-crime and other offenses committed using computer systems; and (c) the establishment of an efficient framework for international cooperation.<sup>105</sup> In pursuit of these objectives, the covenant is made up of four chapters: (1) terms; (2) measures to be taken at the national level regarding substantive law and procedural law; (3) international cooperation; and (4) articles of reservations and their application. The convention defines eight offenses as substantive law including illegal access, illegal interception, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and offenses related to infringements of copyright and related rights. Areas covered by procedural law apply to the basic offenses indicated above as well as to any offenses carried out by

---

<sup>102</sup> See: "Status of Implementation of Directive 95/46/ EC" [http://ec.europa.eu/justice\\_home/fsj/privacy/law/implementation\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm)

<sup>103</sup> The text of the convention can be found at: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. The Council of Europe is an international organization that was founded in 1949. Today it has 45 member states, including countries of Eastern Europe.

<sup>104</sup> For monitoring of the countries signing the convention and their status, see: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=10/5/2006&CL=ENG>

<sup>105</sup> <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>

using computer systems or by electronic means. The convention permits law enforcement authorities to search and seize computer data, collect traffic data in real time, and intercept content data.

The third chapter of the covenant defines provisions regarding traditional computer crimes and provisions for international cooperation, such as principles of extradition. The provisions deal with international assistance in two types of cases: (1) if there is a legal basis in the form of treaties or reciprocal legislation, then the existing agreement will be expanded to situations cited in the covenant; and (2) if there is no prior legal basis, then the provisions stipulated in the third chapter will apply. The chapter also contains a special provision on transborder access to stored computer data that does not require mutual assistance (with consent or where publicly available). A different special provision allows for the creation of a network designed to guarantee rapid assistance between signatory countries of the covenant.

Article 22 of the covenant deals with jurisdiction and provides criteria for determining jurisdiction over the criminal offenses stipulated in the covenant. The Article also allows the creation of additional jurisdictional bases within the framework of national law. In cases where a jurisdiction is established for more than one country, for instance in trans-border virus attacks on the Internet, the relevant countries shall consult with each other in order to determine in which country the trial will be held. Article 42 is another important article in the covenant, dealing with reservations and allowing several reservations (this is a closed list) in light of the nature and character of the covenant.

The field of telecommunications has been the subject of extensive legislation in the European Union as part of the effort toward free competition in this market. Within the scope of this legislation, the field of privacy was addressed in the EU Directive on Personal Data and Privacy in the Telecommunication Sector.<sup>106</sup> The directive imposed a broad range of obligations on service providers in order to guarantee the privacy of the users of communication means, including activities related to the Internet. The rules relate to fields, which, prior to these directives, fell between the cracks in the existing data protection laws. The rules of the directive apply to the processing of personal data in the telecommunications

---

<sup>106</sup> European Parliament and Council Directive 97/66/EC of December 15, 1997 concerning the processing of Personal Data and the Protection of Privacy in the Telecommunication Sector, OJL 24 (30.01.1998).

services available to the public in the EU, such as digital services (Integrated Services Digital Network – ISDN) and mobile telephones.

The Directive imposed restrictions on access to the information. For example, Caller ID technology must incorporate the possibility of blocking the transmitted number. Information collected during the course of a communication must be “cleansed” upon conclusion of the call. Subscribers are entitled to receive non-itemized bills. The provider must allow the subscriber to block automated calls coming from third parties. Subscriber directories must be limited to essential details only. Use of recorded advertising messages and faxes must be limited to subscribers who have given their consent.

As an extension of this directive, in July 2000 the Commission proposed a directive on data processing and protection of privacy in the electronic communications sector.<sup>107</sup> The proposal was submitted as part of an overall package, with the aim of encouraging electronic communications competition in the European market. The proposal suggested that a new directive replace the existing one of 1997 by extending the protection for communications of the individual to a broader technological and legal category of “electronic communications.” The proposal replaced existing definitions of “telecommunication services and networks” with a new definition of “electronic communication services and networks.” The proposal also added new definitions and protections for calls, connections, traffic data, and location data, the aim of which was to reinforce the consumer’s right to privacy and provide the possibility of control in processing the various types of data.

These provisions would guarantee the protection of all the data related to Internet transmissions, ban unsolicited marketing by e-mail (spam) without prior consent by the “opt-in” method, and give mobile telephone users protection from wiretapping and immediate place location. The proposed directive also gives subscribers the opportunity to choose whether they wish to be entered in public directories. However, this proposed directive also gives the countries the possibility of limiting the provisions with security and enforcement need restrictions.<sup>108</sup>

This proposal was discussed in the European parliament, which has already submitted amendments to allow spam and to restrict the saving of service providers’ information for law enforcement purposes. In pursuit of

---

<sup>107</sup> A Proposal for a Directive of the European Parliament and of the Council concerning the processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector (2000) 385, OJC 365 (19.12.00).

<sup>108</sup> <http://www.privacyinternational.org/survey/phr2000/overview.html#Heading12> (24.12.01)

the amendment, any surveillance and monitoring must be essential, appropriate, proportional, and time-limited. The means must be anchored in jurisprudence and approved on an individual basis by a relevant authority. This authority must be committed to the European Human Rights Convention and the ruling of the Human Rights Court. All these measures are in place to ensure that extensive or general electronic surveillance is not possible.<sup>109</sup>

EU Directive 1999/93/EC on Electronic Signatures<sup>110</sup> extended the provisions of the directive on personal data and imposed a supervisory and data storage obligation on certification service providers. These entities may collect personal data only directly from the data subject or after receipt of his explicit consent, and only in relation to what is required and obligatory for purposes of issuing the certification. The data must not be collected for other purposes (Article 8).

*Liability of service providers.* The Convention on Cyber-crime discussed above deals extensively with imposing obligations on service providers within the framework of procedural steps and powers granted to the enforcement authorities. This covenant gives a very broad definition to the term “service provider.” The term is designed to include a wide category of individuals serving in a specific role in communications or in the processing of data in computer systems. According to this definition, both public and private entities that provide users with the ability to communicate with others are included.

Therefore, the question of whether the users create a closed group or whether the service is offered to the public, or whether the service is free of charge or provided for a fee, is irrelevant. A closed group can consist of employees in a private company who have access to the service by way of the company server. The definition also includes entities that store or process information in another way for the entities cited above or for the users. For instance, the definition includes “hosting” and “caching” services as well as Internet connection services. On the other hand, the definition of “service provider” does not include a content provider that does not also offer connection or data processing services.<sup>111</sup>

---

<sup>109</sup> For amendment of the directive in the framework of the European Parliament committees, see: [\(24.12.01\)](http://www.privacyinternational.org/issues/cyber-crime/index.html#coe).

<sup>110</sup> Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJL 013 (19.01.00) pp. 0012–0020 [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0093&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=31999L0093&model=guichett).

<sup>111</sup> See the Covenant Explanatory Report: <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>



Within the framework of the procedural powers established by the Convention, obligations are imposed on the service providers. Section 18 of the Convention calls for legislation that requires the service providers to transmit customer information about the type of communication, as well as the subscriber's identity and geographic location. According to §§ 20–21, the service providers will also be obligated to provide information on content and communications in real time about the messages on their servers. Yet, the Convention makes it possible to demand that the service providers maintain the confidentiality of their consumers. One may wonder what effect this obligation of confidentiality, on the one hand, and the obligation to provide information, on the other, will have on the commercial (and legal) relations between the service providers and their consumers.

### ***2.3.2 EU Regulation of Encryption***

In 1992, the European Union Commission established a committee to study the issue of information security and encryption. This initiative was part of a program that included a strategic working framework for information security; analysis of data protection needs; provision of solutions for those needs; specification, standardization, and verification of information security; integration of technological developments in the area of data protection; and integration of security functions in information systems.<sup>112</sup> The Commission published a number of reports and position papers,<sup>113</sup> which indicated an intention to develop a strategy to protect the internal market for encryption products and associated services. These position papers were translated into a number of directives, some of which are reviewed below.

One expression of the trend toward a free market for encryption products and encryption services can be found in the Directive on Electronic Signatures (Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999 on a Community framework for electronic signatures).<sup>114</sup> The issue of electronic signatures is closely connected with the area of encryption, because all certification processes are based on encryption keys. The definitions section of the Directive gives explicit and formal expression to concepts related to the encryption pro-

---

<sup>112</sup> Council Decision 92/242/EEC of March 31, 1992 in the field of information security.

<sup>113</sup> <http://europa.eu.int/scadplus/leg/en/lvb/l24121.htm>

<sup>114</sup> OJL 013 (19.01.2000) pp. 0012–0020

cess used in verifying electronic signatures. Examples of such techniques are signature-verification data (including codes or public encryption keys used to verify an electronic signature); signature-verification devices (configured software or hardware used to implement signature-verification data); and digital certificates, which are electronic attestations that link signature-verification data to a person and confirm that person's identity.

Sections 3–4 prescribe that the member states may not introduce restrictions on certification providers who wish to enter the market, nor can they establish any requirement for prior authorization as a prerequisite for receiving the necessary governmental permits. At the same time, voluntary programs may be introduced to enhance levels of certification service. All conditions related to such programs must be objective, transparent, proportionate, and non-discriminatory. Similarly, a supervisory system for service providers needs to be set up. Among other things, the Commission requires member states to report to the Commission on any national proposal to impose rules or restrictions on encryption products.

In 1997, the Organization for Economic Cooperation and Development (OECD)<sup>115</sup> published guidelines for encryption policy. These guidelines were directed mainly at governmental authorities, but were written with the expectation that they would stimulate interest from both the private and the public sector. Following are the principles listed in the document:

1. Encryption methods should be trustworthy in order to generate confidence in the use of communications systems.
2. Users should have the right to choose any encryption method, subject to applicable law.
3. Encryption methods should be developed in response to the needs and demands of the target audience.
4. Technical standards for encryption should be developed at the national and international level.
5. The fundamental right to privacy, including secrecy of communications and protection of personal information, should be respected in national encryption policies and in the implementation and use of the various methods.

---

<sup>115</sup> Organization for Economic Cooperation and Development. This is a forum established in 1961 and based in Paris. The organization includes the 29 developed nations (Israel is not a member). This international forum publishes guidelines on various topics related to economics and trade. These recommendations, although not officially binding, have a great deal of influence on the member states, as well as on states that are not members of this forum. See: <http://www.oecd.org>.

6. National encryption policy may permit legal access to the non-encrypted text (plaintext) and to encryption keys.
7. The responsibilities of bodies providing certification of encryption services or holding or accessing encryption keys need to be clearly stated.
8. Governments should cooperate to coordinate encryption policies. To this end, governments should remove, or avoid creating in the name of encryption policy, unjustifiable obstacles to trade.

The third principle is particularly noteworthy in that it stipulates the need for developing encryption methods based on the requirements of the free market. This principle states that research and development in encryption should be dictated by the needs, requirements, and responsibilities of individuals, businesses, and governments. As such, it ensures that developments keep pace with changing technologies, the demands of users, and market developments in general.

Along with the rejection of approaches based on local or national frameworks, most countries have rejected Key Escrow (Key Recovery) policies. These policies refer to the idea that users may use encryption in their systems, but a third – governmental – party would receive the keys to the code from encryption service providers. That government body would be responsible for providing the keys to the appropriate authorities when asked to do so.

This policy was adopted under French law in 1996, but the law was repealed in 1999. The British government also promoted this policy for a few years, and the United States tried to promote it, but was met with rejection on the part of the OECD. The United States also faced criticism from security experts who emphasized the problematic nature of a situation in which a central body holds the encryption key. The final rejection of this policy came in the Wassenaar agreements of December 1998 (see below). Today, only a few countries use this approach, and in the United States, the export restrictions that encouraged such an approach were repealed in January 2000.

As a result of the rejection of Key Escrow policies, a new approach was adopted by many countries: the demand for “lawful access” to encryption keys or message plaintext. Under this approach, individuals may be asked to reveal encryption keys to law enforcement authorities, and, if they refuse, they may be liable to criminal prosecution. Until the year 2000, only a few countries had enacted laws of this type. The OECD guidelines described above noted the principle of “access,” but did not necessarily support it. The guidelines noted that national policy may permit legal access to the plaintext or encryption keys, but that this policy must respect

the other principles in the organization's guidelines. This issue provoked sharp debate within the OECD until the organization finally decided not to support a global approach to "legal access."

In the context of the "lawful access" approach, consideration should be given to the right against self-incrimination, which is well founded and binding in many countries in the world. Underlying this right is the prohibition on governmental bodies to coerce an individual into giving testimony that may incriminate him. In this context, the argument exists that it is not possible to coerce individuals to reveal encryption keys or passwords that are not recorded elsewhere. In the United States, this argument has been raised in connection with the Fifth Amendment to the Constitution,<sup>116</sup> while in Europe the argument is based on the European Convention on Human Rights, which permits an individual to retain his right to remain silent.<sup>117</sup>

The EU has also made use of the Wassenaar Arrangement<sup>118</sup> in this context. The Arrangement refers to a series of agreements between 33 states to control the export of conventional arms and "dual use" (usable for both commercial and military purposes) goods and technologies. Under the heading of technologies, a number of encryption products that are considered "dual use" are included. The Wassenaar Arrangement is not a convention or type of legislation, but rather the exchange of opinions at the international level. Compliance of the participating states is a matter for each state's consideration and is carried out by means of legislation at the national level.

The main provisions of the Arrangement relate to the free export of encryption products based on key length, the easing of restrictions on the export of encrypted products in order to protect intellectual property rights, and licensing requirements for the export of encryption products not mentioned in the agreements. This is important in light of the fact that there is a significant loophole allowing for the free trade and distribution of non-tangible encryption assets by means of downloading from the Internet.<sup>119</sup>

---

<sup>116</sup> See, for example: *Doe v United States*, 487 US 201, 219 (1988) (Stevens J, dissenting) ("[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe – by word or deed").

<sup>117</sup> <http://www.fipr.org/ecom99/ecommand.html>

<sup>118</sup> <http://www.wassenaar.org>

<sup>119</sup> CRYPTOGRAPHY & LIBERTY 1999/2000, *supra* note 12

Within the framework of the international report mentioned above, countries are categorized according to the means of control applicable to trade in encryption products and services.<sup>120</sup> The report divides the countries that were investigated into three categories on the basis of how they control encryption. This categorization is designed to allow a world map of encryption policies to be drawn up for purposes of comparison. There are no accompanying sanctions to this categorization.

The “green” category includes countries that promote a policy permitting trade in encryption products without legal impediments, such as countries that have adopted the OECD guidelines. The “yellow” category applies to countries that have proposed state controls over encryption, including limitations on use or import, or those countries operating strictly within the provisions of the Wassenaar Arrangement. The last category – the one considered least desirable – is the “red” category, which includes countries that impose sweeping restrictions on encryption. Many countries do not fit exactly into one of these categories, in which case the report lists them as falling between the different categories.

### ***2.3.3 EU Regulation of Copyright***

On March 16, 2000, the EU ratified the two WIPO treaties (WCT and WPPT), noted above, which constituted the main legal arrangements providing preferential status for technological means used in protecting copyright. It also empowered the Commission to act on the issue of regulating copyright at various levels as a representative of the European Union. In line with this decision, the European Union could now become a party to the WIPO treaties for the regulation of copyright and related rights.

The following year, the European Parliament passed Council Directive 2001/29/EC, which sought to harmonize certain aspects of copyright and related rights in the information society.<sup>121</sup> The aim of this directive was to adopt legislation regarding copyright and related rights in a manner that reflected technological developments in the Information Age. It also introduced the WIPO treaties into EU law. The Directive deals with three main areas: copyright, public broadcast and transmission rights, and distribution rights.

---

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

<sup>121</sup> OJL 167 (22.06.2001).

First, the member states are required to provide legal protection against the circumvention of effective technological means that protect copyrighted works. This legal protection relates to preparatory acts, such as the production, import, distribution, sale, or provision of services that circumvent technological protections. Another provision relates to rights-management information included in the copyrighted work, that is, information about the copyright owner or the terms and conditions for use of the work. The Directive also provides legal protection for the technological measures taken by copyright holders to prevent illegal modification or circumvention.<sup>122</sup>

A second means of protecting copyrighted material and encryption methods, as well as restricting decryption, is the legal protection given to technological services that operate by restricting access to content. A 1998 European Directive established a uniform legal framework for proceeding against devices or services that provide unlicensed access to copyright-protected services, such as television, radio, cable transmissions, satellite transmissions, and electronic publications. The framework applies when such services are provided to the public through subscriptions or payment for viewing.<sup>123</sup>

In this context, an “illicit device” is defined as any equipment or software designed to give access to a protected service (Article 2(e)) in an intelligible form without the authorization of the service provider. “Infringing activities” include the manufacture, import, distribution, sale, rental, or possession for commercial purposes of illicit devices. The installation, maintenance, or replacement for commercial purposes of illicit devices is also prohibited. Furthermore, the member countries of the European Union are prohibited from restricting the protections afforded to protected services that originate in another member country and from restricting the free movement of conditional access devices, except those defined as illicit. The member countries were required to enact internal legislation in line with the provisions of the Directive by June 28, 2000.<sup>124</sup>

---

<sup>122</sup> <http://europa.eu.int/scadplus/leg/en/lvb/l26053.htm>.

<sup>123</sup> See: Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, OJL 320, 28/11/1998 P. 0054–0057. [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnum\\_doc&lg=EN&numdoc=31998L0084&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnum_doc&lg=EN&numdoc=31998L0084&model=guichett)

<sup>124</sup> <http://europa.eu.int/scadplus/leg/en/lvb/l26050.htm>

England, for example, has implemented the Directive within the framework of its Copyright, Designs and Patents Act 1988 (CDPA).<sup>125</sup>

Note that, in spite of the broad definitions found in the Directive, it is not clear whether passwords obtained illicitly fall into the category of “illicit devices,” because a password is not necessarily a device nor, is it software designed to provide access to the protected service.<sup>126</sup>

A third means by which encryption is protected – in that there exists a legal restraint on decryption – is by means of the protection given to databases. The European Union’s directive on the legal protection of databases is Directive 96/9/EC of the European Parliament and of the Council of March 11, 1996.<sup>127</sup> The Directive created, within a framework separate from traditional copyright laws, a new intellectual property right regarding databases. This new right is based on the substantial investment (measured either qualitatively or quantitatively) in obtaining or verifying the material in the databases, as opposed to the criteria of creativity and originality required for protection under copyright law.

The Directive prohibits the extraction or other use of information in such amounts as would be deemed qualitatively or quantitatively significant (Article 7(1)). It also establishes a prohibition against extracting data from a database and reusing such data in any manner or in any forum. As such, it creates an effective prohibition against breaking the encryption of such material. The fair use protections in respect of this right have been narrowed. Permitted uses include the extraction for private use of data from a non-electronic database for purposes of teaching or scientific research and for purposes connected with public security and/or judicial procedure (Article 9). This last protection – a specific exception aimed at public security needs – permits the extraction of data from a database for security purposes. Such an act will not be deemed an infringement of the intellectual property rights that exist with respect to that database. These rights are in addition to the copyright protections applicable to the database as a result of originality of design or arrangement of the data.<sup>128</sup>

---

<sup>125</sup> See §§ 297A-298, and an explanation in: ALAI 2001 Congress Questionnaire, [http://www.law.columbia.edu/conferences/2001/Reports/uk\\_ic\\_en.doc](http://www.law.columbia.edu/conferences/2001/Reports/uk_ic_en.doc).

<sup>126</sup> CRYPTOGRAPHY & LIBERTY 1999/2000, *supra* note 12, at 71.

<sup>127</sup> See: OJL 77 (27.03.96).

<sup>128</sup> [http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb\\_docs=25&domain=Legislation&coll=&in\\_force=NO&an\\_doc=1996&nu\\_doc=9&type\\_doc=Directive](http://europa.eu.int/servlet/portail/RenderServlet?search=DocNumber&lg=en&nb_docs=25&domain=Legislation&coll=&in_force=NO&an_doc=1996&nu_doc=9&type_doc=Directive)

## 2.4 Other Countries

### 2.4.1 Britain

A comprehensive law called the Anti-terrorism, Crime and Security Act 2001 was promulgated by the British Parliament<sup>129</sup> in order to amend the anti-terrorism law passed in the year 2000 and to lay down additional provisions on terror and security. The law extended the prevention and enforcement powers of the government authorities, allowed storage of traffic data for a long period of time, and determined the provisions for disclosure of information to the authorities. The law also deals with a variety of areas, including immigration; xenophobic crimes; weapons of mass destruction, poisons, and the nuclear industry; security in the field of aviation; bribery and extortion; and the handling of property and funds of terrorist organizations.

*British regulation of encryption.* In May 2000, a law implementing the European Directive on Electronic Signatures (99/93/EC) came into effect. Under the Cryptography Service Provider and the Electronic Communication Act 2000, British law established the registration process for encryption service providers and establishes legal recognition of electronic signatures. In line with the provisions of the law, the Secretary of State is required to establish and operate a Register of Encryption Service Providers.<sup>130</sup> Companies that are entitled to registration are those that provide services such as public key verification for individuals, administration of encryption keys, timestamping services for electronic signatures, and storage of encryption keys. Although the law does not provide specific criteria for registration approval, it does list the necessary details to be submitted upon application, including the proposed technology, the identity of the applicant for registration, and the means by which the applicant will offer the technology to the public. This law explicitly rejects the Key Escrow approach – whereby a secret government body would collect the keys – in favor of keeping a register of service providers that is open to the public.

An important aspect of the law is the fact that the register is voluntary. As a result, any encryption service provider can trade in the open market

---

<sup>129</sup> <http://www.hmso.gov.uk/acts/acts2001/20010024.htm> (last visit: 23.12.01)

<sup>130</sup> Encryption service providers are defined in Section 6 of the law: “Any service which is provided to the senders or recipients of electronic communication, or to those storing electronic data, and is designed to facilitate the use of cryptographic techniques.”



without reference to his absence from the public register or concern for the fact that his application for registration was rejected. At the same time, it should be remembered that the significance of the register's being public is the fact that it is open to public scrutiny and examination, and thus serves as a tool to assist in selection and review in this area.<sup>131</sup>

*British regulation of copyright.* The British Copyright, Designs and Patents Act 1988 established, in §§ 296–297, a prohibition against the development, import, sale, rental, or advertisement of any device or measure aimed at circumventing the protection against copying a protected work. The broad terms of the prohibition include the publication of information that assists in carrying out acts designed to circumvent such protections. In addition, the law also prohibited unlicensed decryption.<sup>132</sup>

One of the tests of this law came in the case of *Mars UK v Teknowledge Ltd*<sup>133</sup>, which dealt with a claim for breach of confidentiality by means of reverse engineering of a device that held encrypted data. In line with the requirements developed in a previous judgment,<sup>134</sup> the court found that the encrypted information itself was not confidential, considering that the device (Cashflow) was available to the public, and that there were no special circumstances suggesting an obligation to maintain confidentiality on the part of the respondent. It is important to note that the judgment made clear that encryption itself does not make encrypted material confidential in the absence of any other relationship between the source and the decoder.<sup>135</sup>

*British regulation of decryption.* Another important item of British legislation is the Regulation of Investigatory Powers Act 2000. The legislation obliges service providers to disclose encryption keys or location of the keys. However, the object of the legislation is to guarantee a balance between the right of enforcement authorities to interfere in electronic transmissions and the protection of business interests and individual rights. The regulations deal with four different actions: (1) interception of transmissions; (2) close surveillance; (3) human data sources; and (4) disclosure of encrypted information. It is possible to carry out an action against an individual or an organization only upon receipt of a corresponding order, which must be based on proof that the action is for the sake

---

<sup>131</sup> See CRYPTOGRAPHY & LIBERTY 1999/2000, *supra* note 12, at 59.

<sup>132</sup> *Id.* at 70.

<sup>133</sup> *Mars UK v. Teknowledge Ltd* [2000] FSR 138.

<sup>134</sup> *Coco v. AN Clark* [1969] RPC 41.

<sup>135</sup> CRYPTOGRAPHY & LIBERTY 1999/2000, *supra* note 12, at 63–64.

of national security, to prevent a serious crime, or to guarantee British economic interests.

In such a case, the service provider would be required to grant access to transmissions and to disclose any protected information (namely, any encrypted information), both for transmissions still in progress and for information stored with the service provider. Some maintain that the legality of this law is doubtful in light of the European Human Rights Convention, which was assimilated into British law in the Human Rights Act 1998.<sup>136</sup>

### 2.4.2 *Canada*

In December 2001, most sections of the C-36 Anti-Terrorism Bill, influenced significantly by the events of September 11, were enacted into law.<sup>137</sup> This legislation introduced several new sections into the criminal code that were designed to fight terror. The new offenses extended the existing law to include a group of situations considered to be indicative of terrorist activity, such as offenses against international notables or UN personnel, offenses that involved the use of explosives or other lethal devices, and offenses relating to the funding of terror acts.<sup>138</sup>

The objectives of the Canadian law were to regulate personal, financial, and medical data privacy, and to create reliable and uniform regulation for e-commerce and electronic documents. The law was designed to give the individual personal data protection rights. It defines the methods by which organizations can collect and use personal data, and outlines the rights of the individual to access and modify the data. The law requires that businesses disclose the object of the data collection and receive consent before collecting the data. The law does not exempt non-Canadian companies from abiding by the law. This category includes entities that are not Canadian, but collect data in Canada or on Canadian citizens.

---

<sup>136</sup> *Id.* at 60.

<sup>137</sup> The Canadian parliament passed the legislation on November 28, 2001 and was submitted for approval by the Senate, after which the law returned to Parliament for implementation. [http://www.canadianliberty.bc.ca/.\(24.12.01\)](http://www.canadianliberty.bc.ca/.(24.12.01))

<sup>138</sup> [http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36\\_1/90168bE.html](http://www.parl.gc.ca/37/1/parlbus/chambus/house/bills/government/C-36/C-36_1/90168bE.html)

The law also indicated that its objective was to adapt the legal situation in Canada to meet European requirements. As of January 2003, all organizations have become subject to the laws' dictates.

### ***2.4.3 Australia***

In Australia, the Privacy Protection Law of 2000<sup>139</sup> relates to the management of company information systems and seeks to protect personal and sensitive electronic data. The law, which came into force in December 2000, sets two basic requirements:

1. Protection of personal data from misuse and unauthorized access, modification, or disclosure.
2. Destruction or permanent de-identification of unnecessary information.

According to the principle of NPP4, "reasonable steps" must be taken to safeguard the physical security of the data, the security of the computer systems and networks, and to establish secure communications. Appropriate training of the staff or workers is also required.

After the events of September 11, several cyber crime laws were legislated in Australia, including a 10-year prison sentence for cyber crimes. The laws dealt with "standard" computer offenses and offenses by means of computer, such as unauthorized use. The cyber crime laws also permitted investigations for "pure" criminal cases, such as murder and fraud. The laws included seven new "high-tech" offenses that covered hackers, prevention of service attacks, vandalism at sites, dissemination of viruses, and the use of computers in offenses such as harassment, fraud, and sabotage. Since 2000, the law has been periodically reviewed, but its substance has remained the same as when it was originally enacted.

---

<sup>139</sup> <http://www.efa.org.au/Issues/Privacy>.



<http://www.springer.com/978-0-387-73577-1>

Fighting Terror Online

The Convergence of Security, Technology, and the Law

Golumbic, M.C.

2008, XIV, 178 p., Hardcover

ISBN: 978-0-387-73577-1