Wassenaar Arrangement / COCOM [Sources 1, 5]

1. Export/ import controls

COCOM

COCOM (Coordinating Committee for Multilateral Export Controls) was an international organization for the mutual control of the export of strategic products and technical data from country members to proscribed destinations. It maintained, among others, the International Industrial List and the International Munitions List. In 1991, COCOM decided to allow export of mass-market cryptographic software (including public domain software). Most member countries of COCOM followed its regulations, but the United States maintained separate regulations.

Its 17 members were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxemburg, The Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom, and the United States. Cooperating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan.

The main goal of the COCOM regulations was to prevent cryptography from being exported to "dangerous" countries - usually, the countries thought to maintain friendly ties with terrorist organizations, such as Libya, Iraq, Iran, and North Korea. Exporting to other countries is usually allowed, although states often require a license to be granted.

COCOM was dissolved in March 1994. Pending the signing of a new treaty, most members of COCOM agreed in principle to maintain the status quo, and cryptography remained on export control lists.

Wassenaar Arrangement

The Wassenaar Arrangement controls the export of weapons and of dual-use goods, that is, goods that can be used both for a military and for a civil purpose; cryptography is such a dual-use good.

In 1995, 28 countries decided to establish a follow-up to COCOM, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The negotiations on the Arrangement were finished in July 1996, and the agreement was signed by 31 countries (Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States). Later, Bulgaria and Ukraine also became a participating state to the Arrangement.

The initial provisions were largely the same as old COCOM regulations. The General Software Note (applicable until the December 1998 revision) excepted mass-market and public-domain crypto software from the controls. Australia, France, New Zealand, Russia, and the US deviated from the GSN and controlled the export of mass-market and public-domain crypto software. Export via the Internet did not seem to be covered by the regulations.

There is a personal-use exemption, allowing export of products "accompanying their user for the user's personal use" (e.g., on a laptop).
In September 1998, Wassenaar negotiations in Vienna did not lead to changes in the crypto controls, although it was apparently considered to restrict the GSN (see an article in German) and possibly also to ease controls for key-recovery crypto. (Compare an article in Swedish of March 1998.)

The Wassenaar Arrangement was revised in December 1998. Negotiations were held on 2 and 3 December 1998 in Vienna, which resulted in restrictions on the General Software Note and in some relaxations:

- free for export are: all symmetric crypto products of up to 56 bits, all asymmetric crypto products of up to 512 bits, and all subgroup-based crypto products (including elliptic curve) of up to 112 bits;
- mass-market symmetric crypto software and hardware of up to 64 bits are free for export (the 64-bit limit was deleted on 1 December 2000, see below);
- the export of products that use encryption to protect intellectual property (such as DVDs) is relaxed;
- export of all other crypto still requires a license.

There was no change in the provisions on public-domain crypto, so that all public-domain crypto software is still free for export. Nothing was said about electronic exports (e.g., via the Internet), which consequently remain unclear.

In its meeting of 30 November-1 December 2000, the Wassenaar states lifted the 64-bit limit for export controls on mass-market crypto software and hardware (in the Cryptography Note, clause d. (the 64-bit limit) was deleted in its reference to category 5A2, as well as the related Validity Note, see the summary). The public statement of the meeting mentioned that "Participating States recognised that it is important to continue deepening Wassenaar Arrangement understanding of how and how much to control" intangible transfers.

The Wassenaar provisions are not directly applicable: each member state has to implement them in national legislation for them to have effect. (In the entries below, I have included mention of the pre-December 1998 regulations, which will stay into effect until the government enacts new legislation to implement the Wassenaar changes.)

See the Wassenaar List (crypto is in category 5 part 2). See further the Wassenaar Arrangement page (includes contact information for various national export control authorities), a Wassenaar FAQ (by US BIS), Greg Broiles' page on the Wassenaar Arrangement, which includes links to John Young's pages on the Wassenaar Arrangement and comments on the December 1998 changes, and the GILC Wassenaar page. See also Chapter 3 of Simo-Pekka Parviainen's thesis on Cryptographic Software Export Controls in the EU. Cf. an April 1996 article on the Wassenaar Arrangement.

Back to the Table of Contents

Council of Europe [Source 5]

2. Domestic laws and regulations

On 23 November 2001, the Council of Europe adopted the Convention on Cybercrime [search for convention 185] (see the text and Explanatory Report). The Convention deals with substantive and procedural criminal law. Article 18 contains a production order: "Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a). a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system of a computer-data storage medium". Para. 176 of the Explanatory Memorandum adds that "Parties could establish obligations that the specified computer data (...) must be produced in the manner specified in the order. This could include reference (...) to form, such as that the data or information be provided in 'plain text' (...)." Hence, the convention allows, but does not oblige, party states to create a decryption order.

Section 62 of the Explanatory Memorandum specifies the clause "without right" that is used in describing several offences the treaty penalises. It explicitly states that encryption "should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right". So, encryption can not be outlawed by party states, although the phrase "in principle" allows for a certain margin of appreciation.

The Convention was signed on 23 November 2001 by 26 of the 43 CoE Member States, as well as by Canada,
Japan, South Africa and the United States (who participated in the drafting process). Later, several states followed. As soon as 5 countries have ratified the convention, it will enter into force. (As of 8 January 2004, four countries had ratified.) The convention will not be directly applicable, but will have to be implemented by party states in their national laws. See the list of signatures and ratifications for the current status of the convention.

History of the Convention
A Committee of Experts on Crime in Cyber-Space (PC-CY) was established in January 1997, and published a first draft text for discussion on 27 April 2000 (version 19). The Assembly of the CoE approved a further draft on 24 April 2001, and a new version (no. 27) was published on 25 May 2001 (CDPC (2001) 2 rev).

The production order was earlier included in article 14 of the draft (version 19). Article 14, section 5 read: "Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order for the purposes of criminal investigations and proceedings any person who has knowledge about the functioning of the computer system or measures applied to secure the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking of the measures referred to in paragraphs 1 [search] and 4 [seizure]."

The "measures applied to secure the computer data" included cryptography. It was not quite clear whether the provision included a decryption order. Given the purpose of the seizure power of article 14, section 4 ("to seize or similarly secure computer data accessed (...) in view of their possible use in criminal investigations and proceedings"), one might infer that section 5 should be read as requiring persons to provide decryption information that enable the use of seized encrypted data in criminal proceedings. Admittedly, the text was a bit muddy here.

The text refers only to criminal investigation, not to national security purposes. Since section 7 refers to the "conditions and safeguards under national law", states must respect the privilege against self-incrimination, which is incorporated in article 6 of the European Convention on Human Rights and hence should be respected in national laws. Consequently, states should not require suspects to decrypt.

Earlier on, key escrow may have been considered in the draft convention. According to the 25 November 1998 minutes of the EU's Legal Advisory Board, it was unclear "whether the convention will contain any provisions on escrow of encryption algorithms". The current text does not contain anything to suggest key escrow.

3. Developments to restrict cryptography
The Council of Europe (a 46-member intergovernmental organisation, whose treaties are not directly applicable in national law), in its Recommendation R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology of 11 September 1995, stated that "measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary." The recommendation itself does not state which measures should be taken or how the "balance must be found" in the "conflict of interests between the needs of the users and law enforcement".

Back to the Table of Contents

European Union [Sources 5, 7, 8]

1. Export/ import controls

- Export to other EU countries is entirely liberalised, with the exception of some highly specialised products, such as cryptanalysis items. For these items, member states can issue General Intra-Community Licenses valid for export to one or more determined EU countries, provided basic requirements are met, such as a statement of the end use of exported items. For re-exports after intra-EU export, an information-exchange mechanism is established.
- For export to Australia, Canada, Japan, New Zealand, Norway, Switzerland and the US, a Community
General Export Authorisation (CGEA) can be applied for, which is valid for export from all EU countries.

- For export to other countries, a General National License can be applied for (except for cryptanalysis items), which are valid for export to one particular country. Otherwise, exporters have to apply for an individual license. For mass-market crypto software and hardware

**Former regulation**


In general, a license was needed for the export of crypto hardware and software outside of the EU, with the exception of mass-market and public-domain software. For a transitional period, the Regulation also required a licence procedure for intra-Community trade of encryption products. Export to seven "friendly" countries (Australia, Canada, Japan, New Zealand, Norway, Switzerland, USA) seemed to be less restricted.

The October 1997 Communication of the European Commission *Towards A European Framework for Digital Signatures And Encryption* (see below) noticed that the Dual-Use Regulation left room for national implementation and that, consequently, "a large variety of domestic licensing schemes and practices exist. These divergences can lead to distortion of competition." The Commission was of the opinion that the Dual-Use Regulation should be adapted in view of the requirements of the cryptography market. It advised to:

- progressively dismantle intra-Community controls on commercial encryption products (i.e. not necessarily for very advanced encryption);
- launch a discussion on the scope and interpretation of certain provisions, such as the General Software Note (stipulating that public-domain software is not subject to controls);
- deal with problems like intangible means of transmission (such as fax or email).

The EU discussed the December 1998 changes in the Wassenaar Arrangement in order to implement them. (Denmark might not approve of the new Wassenaar regulations.) By Council Decision 1999/193/GASP (Pub. EG Nr. L73) of 9 March 1999, in force since 18 April 1999, the export list of goods was amended. Then, mass-market crypto could be exported within the EU on a general license, without restrictions on key length.

The dual-use regulation was to be replaced by a new regulation by 1 January 1999, according to the *Proposal for a Council Regulation (EC) setting up a Community regime for the control of exports of dual-use goods and technology, COM(1998)257final* (Official Journal 21 December 1998, 98/C 399/01). According to the proposal, the present regime had not sufficiently stimulated a convergence of national policies and practices; it was complex and "too cumbersome to be useful in practice". The main change for cryptography would be that for exporting crypto products within the EU, export licenses would be replaced by a simple notification. Also, the controls would now also include export through intangible means. Eventually, the new regulation was not decided upon until 22 June 2000.

See for an overview of EU export controls Simo-Pekka Parviainen's thesis on Cryptographic Software Export Controls in the EU, and the documents page at UK's DTI.

**2. Domestic laws and regulations**

The European Council Resolution of 17 January 1995 on the lawful interception of telecommunications (96/C329/01) contains a requirement for network operators and service providers, if they use encryption, to provide intercepted communications to law-enforcement agencies "en clair" (which I interpret as meaning to provide the signal as they received it, since they cannot undo encryption by users).

**3. Developments to restrict cryptography**

The draft *Green Book on the Security of Information Systems* (Draft 4.0, 18 October 1993), which has not been officially adopted by the European Council, poses a case for the provision of "Public Confidentiality Services" (which would offer some sort of Government Access to Keys).

In 1996 and 1997, the European Commission was working on a draft proposal on the establishment of a Europe-wide network of Trusted Third Party Services (ETS). The network would be established for providing certification services by private TTP's. Although primarily meant for establishing an infrastructure for the use of public key encryption, the proposal might also try to address the legal access problem, e.g., through key recovery. The studies conducted did not address key recovery in-depth, but concentrated on issues related to establishing a public-key infrastructure for digital signatures. The Report on the results of 1995 TTP projects said that key recovery systems "can potentially provide at least part of the answer to the problems raised by confidentiality functions." These "should be investigated as a matter of priority, in order to complete the picture of TTP functionality." See the Infosec homepage and European Trusted Services preparatory studies. See also the KRISIS pilot project.
The 6-8 July 1997 Global Information Networks Conference Bonn Ministerial Declaration of European Ministers (from the European Union, EFTA, Central and Eastern Europe, and Cyprus) echoes the OECD guidelines. It recognizes the importance of strong cryptography, and declares that crypto products should be available internationally and users should have free choice, subject to applicable law. Measures to safeguard lawful access should be proportionate and effective. Like the OECD guidelines, this leaves ample room for interpretation (pro or con key recovery).

With the release in October 1997 of the Communication from the Commission Towards A European Framework for Digital Signatures And Encryption, COM (97) 503, the European Commission has chosen a direction away from key recovery. Building on its April 1997 Communication on Electronic Commerce, this communication aims at creating a reliable European framework for digital signatures. It also addresses confidentiality crypto policy. It stresses the economic and societal importance of cryptography: "the public needs to have access to technical tools allowing effective protection of the confidentiality of data and communication against arbitrary intrusions. Encryption of data is very often the only effective and cost-efficient way of meeting these requirements." The Commission is concerned that restrictions on encryption affect the right to privacy, its effective exercise and the harmonisation of data protection laws in the Internal Market. Also, "divergence between regulatory schemes might result in obstacles to the functioning of the Internal Market."

The Commission is wary of key recovery issues. "Key escrow or key recovery raise a number of practical and complex questions that policy makers would need to solve, in particular issues of privacy, vulnerability, effectiveness and costs. If at all required, regulation should be limited to what is absolutely necessary. Regulation would also need to distinguish between a multitude of possible key types (storage keys, session keys, authentication keys, etc.)." The Commission will examine whether national restrictions are totally or partially justified, notably whether they are proportionate, taking into account the provisions on the free circulation of goods in the Internal Market, and the requirements of the Data Protection Directive. Also, regulations should distinguish authentication services from confidentiality services. The Commission invites the Council of the European Union to initiate a debate on encryption issues. (In its Ninth Report, the Select Committee on European Legislation considered that this Communication does "not raise questions of legal or political importance").

At the RSA Data Security Conference, January 1998, Detlef Eckhert of the European Commission (DGXIII) said that no regulation is planned for the EU.

EU ministers of Justice and Home Affairs were reported to have agreed that law enforcement agencies must have access to keys or plaintext, at a conference in Birmingham, January 1998. The UK prepared a policy paper for the EU in February 1998, stating that it may be necessary for law enforcement to have lawful access in certain circumstances, which may be either overt (i.e., demanding decryption) or covert (probably through key recovery). The Council of Ministers, on 28 May 1998, decided to monitor closely the use of cryptography by serious criminals and terrorists; it recognised the promotion of key escrow as a possible approach to meet law-enforcement needs. Also, law-enforcement agencies may require access to decryption keys necessary to decrypt seized material. The Council agreed to prepare a Resolution on Encryption and Law Enforcement [source: Swedish government communication 1998/99:116].

ETSI (European Telecommunications Standardisation Institute) worked on a standard for Trusted Third Parties. Part of the standard would relate to lawful access to encrypted data. Great Britain was reported to have pushed here for its Royal Holloway scheme (for key escrow) to be used as a basis, but in early 1998, an interim draft to this purpose was rejected by ETSI.

See also Cryptography in Europe.

4. Developments favoring cryptography

The European Union has adopted a Green Paper on Legal Protection for Encrypted Services in the Single Market, a discussion proposal on protecting services which are encrypted to ensure payment of a fee (such as pay television and video-on-demand). The Green Paper considers proposing a harmonization of national laws to prohibit the manufacture, sale, importation, possession, and promotion of illicit decoders, as well as unauthorized decoding. On 9 July 1997, the European Commission proposed legislation (directive COM (97) 356 (in pdf)) to this purpose, which would also include online services with conditional access. Some cryptographers have voiced concern that the proposal might curb cryptanalytic research. See also Markus Kuhn's critical page on the subject.

The Communication Towards A European Framework for Digital Signatures And Encryption stresses the economic and societal importance of encryption. It mentions that the institutions of the European Union will use digital signatures and encryption.

More recently, several other EU documents call for wider use of encryption as a tool to protect European citizens. The Draft report of the Temporary Committee on the Echelon Interception System of 18 May 2001 recommends "appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software" and "The European institutions and the public administrations of the Member States are called upon systematically to encrypt e-mails, so that ultimately encryption becomes the norm."

The Commission Communication on Improving the Security of Information Infrastructures and Combating Computer-related Crime of 26 January 2001, COM(2000) 890 final, affirms that the Commission will promote "the availability of products and services with an appropriate level of security and encouragement of a more liberalised use of strong encryption through a dialogue amongst all interested parties." The draft Proposal for a Recommendation on security of infrastructures and combating computer-related crime of 18 June 2001 calls for promoting "European research in encryption software to improve the possibility of self-defence by consumers".

Back to the Table of Contents

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
OECD (Organisation for Economic Co-operation and Development)

3. Developments to restrict cryptography/ 4. Developments favoring cryptography

The OECD released its Recommendation of the Council concerning Guidelines for Cryptography Policy on 27 March 1997. The guidelines are non-binding recommendations to Member governments, meaning that they will not be part of international law. The Guidelines provide principles which states should take into account and balance in developing a national crypto policy. The principles are:

1. Trust in cryptographic methods
2. Choice of cryptographic methods
3. Market driven development of cryptographic methods
4. Standards for cryptographic methods
5. Protection of privacy and personal data
6. Lawful access
7. Liability
8. International co-operation

The principles should be seen as "interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest."

Some have welcomed the OECD principles as a victory for privacy over US-pushed key recovery, while others object to certain points as being too inflexible or too vague. Although the guidelines do not endorse key recovery, they do not prohibit it either. In fact, the guidelines are vague enough to allow a broad range of interpretation, and states will be able to choose a privacy-oriented or a law-enforcement-driven policy line as they see fit. While the guidelines recommend states to cooperate to coordinate their crypto policies, one may be skeptical about the chances of governments coming to an agreement; after all, within the OECD, states have not been able to agree, and they have left the task of finding a balance between, roughly speaking, information security/ privacy and law-enforcement/ national security to individual states.

Cf. Stewart Baker's analysis of and comments on the OECD guidelines.

The process of discussing and drafting policy guidelines started with an Ad-hoc Meeting of Experts on Cryptography Policy on 18-19 December 1995, organized by the OECD Committee for Information, Computer and Communications Policy (ICCP). They proposed to make a study upon current Member Countries encryption policies, market for encryption, key escrow encryption, and to develop a cryptography policy guideline based on the following principles, among others: provides security with confidence, voluntary use, international perspective, recognise national responsibilities, legally effective. The Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure held subsequent meetings on 7-8 February 1996 in Canberra, on 8 May 1996 in Washington, DC, on 26-28 June in Paris, and on 26-27 September 1996, again in Paris. At the June 1996 meeting, according to one report, no agreement was established; the OECD was said to be split into two parties, one with countries favouring mandatory key escrow (notably the US, UK, and France), and one with countries opposing this approach (mainly Japan and the Scandinavian countries). See a 1 October 1996 press release.

One can compare the final version to an earlier draft of the Guidelines that was discussed at the December 1996 meeting (with rather optimistic personal comments by Robin Whittle). (Text between [square brackets] remained to be decided upon.) In January 1997, the OECD Group of Experts on Security, Privacy, and Intellectual Property Protection in the GII concluded the guidelines. The Guidelines were finally turned into a Council of the OECD resolution in March 1997.

Back to the Table of Contents

Business Government Forum

1. Export/ import controls / 3. Developments to restrict cryptography

On 19-20 December 1995, a meeting was held at the International Chamber of Commerce in Paris, with governments, businesses and computer experts attending. According to an ICC press release, the "meeting ended
in agreement that [encryption] controls should be kept to a minimum, consistent with the requirements of law enforcement and national security". Businesses agreed that independent trusted third parties could hold deposited keys, to which governments are allowed access under proper judicial warrant, provided sufficient safeguards are in place. Some governments appeared willing to relax export controls on strong cryptography as long as these safeguards applied. A second Business Government Forum on Global Cryptography Policy was held on 7 May 1996 in Washington, DC.

Antigua and Barbuda [Source 5]

2. Domestic laws and regulations
Art. 21(5)(c) of Computer Misuse Bill, 2006 contains a power to order people to provide decryption information. The power can be executed by police officers who execute a warrant, in case of offences defined in the Act or other offences disclosed while executing powers based on the Act. The police officer also has the power to access decryption information himself (art. 21(5)(a)(iii)). Obstructing the police or failing to comply with the decryption order is punishable with a fine of 15,000 dollars and/or two years' imprisonment (art. 21(6)). The Bill does not yet seem to have been enacted as of January 2007, according to the overview of laws.

Argentina [Source 5]

1. Export/ import controls
There are no import controls.

Argentina has signed the Wassenaar Arrangement, so export controls should be regulated according to the pre-December 1998 Arrangement, including the General Software Note.

2. Domestic laws and regulations
There are no controls on crypto use.

Australia [Sources 1, 3, 5, 8]

1. Export/ import controls
Export is regulated through the Defence and Strategic Goods List, last changed in June 1999 according to the December 1998 Wassenaar Arrangement. This includes the General Technology Note, exempting public-domain software from controls. Mass-market software is regulated according to the Wassenaar limits. There is a personal-use exemption (export is allowed for lawful permanent residents, provided they keep control of the crypto and make sure it is not transferred anywhere; a record must be kept for 3 years).

Before the 1999 implementation of Wassenaar, export regulations of December 1996 (see Cat 5.doc) were in accordance with the pre-December 1998 Wassenaar Arrangement, with the exception of the General Software Note. Written permission was needed for exporting cryptographic equipment designed to ensure the secrecy of communications or stored information. Public-domain or generally available crypto-software were included in the export controls (only public-domain "technology" (i.e. specific information necessary for the use of goods) was excluded).

Approval is also required for software that does not itself contain cryptography, but which has an interface specially designed for plugging in cryptography.
Crypto software transmitted electronically (e.g., over the Internet) was apparently not controlled. In mid-1998, the Defence Department became concerned that electronic exports were not covered by the controls, and to counter this, they have apparently threatened to use the Weapons of Mass Destruction Act. This in turn triggered a campaign by Electronic Frontiers Australia. After six months, the Defence Signals Directorate determined that no license was required for an online mirror of PGPi, provided that a warning is contained in the download page that the downoader may infringe Australian export rules if he does not have export approval; apparently, the burden of seeking a license is thus shifted to the downloader rather than the person who makes software available electronically.

Compare Nick Ellsmore's Cryptology for background on the Australian situation.

2. Domestic laws and regulations
On 27 September 2001, the Cybercrime Act, No. 161, 2001, was passed. Item 12 of the law inserts a section 3LA in the Crimes Act 1914, that requires release of encryption keys or decryption of encrypted data, upon a magistrate's order. The order may be granted if there are reasonable grounds for suspecting evidential material is held in or accessible from a computer, and the specified person is a suspect or (an employee of) the owner or lessee of the computer, who has relevant knowledge of the encryption. Failure to comply with the order is punishable with up to six months' imprisonment. The same power is granted in section 201A of the Customs Act 1901. The text of the Act is available at Scaleplus (search for "cybercrime act").
The Act is based on the Council of Europe's (then draft) Convention on Cybercrime. See EFA's comments on the Act.

3. Developments to restrict cryptography
    Earlier developments
There has been an apparently unfounded rumour in the mid-1990s that Australia was planning to restrict banks to Government Access to Keys.

At the OECD meeting of December 1995, Australia expressed little interest in the use of Trusted Third Parties for judicial access to keys. Instead, the paper of the delegation suggested to require suspects to decrypt in case of a warrant; this would require the rules against self-incrimination to be adapted.

A 1996 report by Gerard Walsh, Review of policy relating to encryption technologies, was barred from public release in February 1997 by the Attorney-General's Department. After a freedom of information request by Electronic Frontiers Australia (EFA), it was released, and it is now available online at EFA. The main finding of the Review was that major legislative action was not advised at the time to safeguard national security and law-enforcement interests, although a range of minor legislative and other actions were indicated (such as the creation of an aggregate statute on intrusive investigative powers). The review did not recommend specific options for encryption legislation at the time. One action indicated was to consider establishing a further and more serious category of offence where encryption is used to obstruct government investigation into a criminal offence, and to consider creating a power to require production of crypto keys (or other recovery information). The review did not support mandatory key recovery at that stage.

Compare Nick Ellsmore's Cryptology for background on the Australian situation.

4. Developments favoring cryptography
Transmission of confidential government information (classified "confidential" or above) must be encrypted by an encryption system supplied by the Defence Signals Directorate available only to government agencies.

On 6 May 1998, the Minister for Finance and Administration officially launched the Gatekeeper project, a strategy for the use of public-key technology within the Government.

Back to the Table of Contents

Austria [Sources 1, 5]

1. Export/ import controls

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM

2. Domestic laws and regulations
The Betriebsfunkverordnung forbade encryption in internal company and organisation radio transmissions, but the current version (in German) no longer seems to contain such a prohibition.

3. Developments to restrict cryptography
no

4. Developments favoring cryptography
no

Bahrain [Source 5]

2. Domestic laws and regulations
Cryptography is not allowed in telecommunications networks using the radio frequency spectrum. Section 50 of the 2002 Telecommunications Law (see unofficial translation) stipulates that frequency license holders may not use secret signs or codes in messages or conversations over their telecommunications network in contravention of the regulations.

Bangladesh [Source 5]

2. Domestic laws and regulations
There seems to be no law restricting cryptography.

Belarus [Source 5, 7]

1. Export/ import controls
Import and export of cryptography (coding equipment) is restricted through Resolution of the Council of Ministers of the Republic of Belarus No. 218 of 18 March 1997. One must obtain a license from the Ministry of Foreign Affairs or the State Center for Information Security of the Security Council.

2. Domestic laws and regulations
According to the 21 August 1995 decree N. 456, for application of cryptography means, a license is required by the State Center for Information Security of the Security Council. For design, production, sale, repair, and operation of cryptography, a license by the Committee for State Security is needed. Cryptography use by business people is restricted.

Belgium [Sources 1, 3, 5]

1. Export/ import controls
Belgium requires a license for exporting cryptography outside of the Benelux. Belgium has signed the Wassenaar
Arrangement, including the (pre-December 1998) General Software Note.

2. Domestic laws and regulations

Decryption order

The Law on information-science crime (Wet van 28 november 2000 inzake informaticacriminaliteit / Loi du 28 Novembre relative à la criminalité informatique), Belgisch Staatsblad / Moniteur Belge 2001 - 298, of 28 November 2000 contains a decryption order (see the documents of the Second Chamber, in Dutch and French). Article 9 creates a new provision in the Code of Criminal Procedure, Art. 88quater. Para. 1 of art. 88quater allows an investigation judge (or others on his order) to order someone whom he reasonably suspects to have special knowledge of encryption services to give information on the working or the accessing of the services or on how to decrypt (literally: how to get the data at stake in intelligible form). This order to give decryption information can be given to suspects and people with a right to non-disclosure. (This follows from the fact that para. 2 has a privilege-against-self-incrimination exception, whereas para. 1 does not.)

Para. 2 of art. 88quater allows the investigation judge to order any suitable person to decrypt herself, within her possibility (lit.: to make accessible the data in the form ordered by the judge). This order to decrypt oneself cannot be given to suspects or persons with a right to non-disclosure (para 2, section 2). A refusal of either order is punishable with 6 to 12 months' imprisonment and/or a fine of BEF26 to BEF20k. There is a secrecy duty for professionally involved people. If the ordered persons unintentionally cause damage to the system or data, the State is civilly liable for this.

Article 12 of the same law has a more or less similar provision for intercepted encrypted telecommunications, to be inserted as section 4 of art. 90quater of the Belgian CCP. However, here there is no exception for suspects or persons with a right to non-disclosure, nor is there a civil-liability clause for the State.

Compare an earlier draft of the Law on information-science crime (Wetsontwerp inzake informaticacriminaliteit / Projet de loi relatif à la criminalité informatique), Nrs. 213/1 and 214/1, of 28 October 1999; see articles 4 and 7.

Program Act

The Program Act (Programmawet / Loi-programme) of 30 December 2001, Belgisch Staatsblad / Moniteur Belge 2001 of 31 December 2001, inserts a provision, art. 109terE, para. 6, in the Law on the reform of certain economic state companies (Wet betreffende de hervorming van sommige economische overheidsbedrijven) of 21 March 1991, which may become a prohibition to use cryptography in telecommunications. The provision reads: 'The king determines (...) the technical and administrative measures applicable to (...) telecommunication-service subscribers and users, (...) in order to prohibit the provision of telecommunications services that prevent or hamper the measures of the [wiretap] Act of 10 June 1998 (...)." The provision will enter into force when the applicable Royal Decree appears.

Compare also art. 111 of the Act: "No-one is allowed to establish or try to establish communications via the telecommunications infrastructure in the Kingdom that harm the respect for the laws, the state security, the public order or the good morals or that constitute an insult to a foreign State." Violation of this article is punishable with imprisonment of one to four years (art. 114 para. 8 Reform Law).

However, the potential prohibition of article 109terE, para. 6, has to be read in conjunction with another article in the same Law, art. 109terF. This was inserted on 19 December 1997 (see the Belgisch Staatsblad/ Moniteur Belge of 30 December 1997) to clear the confusion that an earlier law had caused (see below) . This article states explicitly that the use of encryption is free. The provision of indicated encryption services to the public is subject to prior notification (four weeks in advance) to the Belgian Institute of Post and Telecommunications. The explanatory note states that the explicit mention that crypto use is free was needed to indicate the difference with the former law which wanted to subject encryption to procedures relating to key deposits. In the 1997 law, the government kept open the possibility of future action to gain access to coded messages; "this problem will be reviewed later, having regard to the development of the technology or of potential abuse of encryption by mafia organizations or terrorists".

History

In January 1996, Belgium found itself having a law which might prohibit the use of unescrowed encryption. The law was passed in December 1994 as part of a larger law and went unnoticed at the time. The law adds a condition under which telecoms equipment may be seized, namely in case of end equipment which renders tapping ineffective.

According to this law, crypto systems had to be agreed by the Belgian Institute for Posts and Telecommunications (BIPT), which some
interpreted as an obligation to deposit keys there. However, a BIPT spokesman said that "government does not know the consequences of the law". The law was not enforced, but Belinfosec (Belgium Information & Security) had apparently prepared a report proposing further specifications and enacting clauses. The regulation had to be further implemented by Royal Decrees. The Ministry of Justice stated they did not intend to prohibit encryption as a rule. The law was interpreted by some as allowing a phone to be disconnected when it uses (hardware) cryptography end equipment.

Two legislation proposals, by Hatry (in French or Dutch) and Bribosia/Maximus (in French or Dutch) were submitted to drop the debated provisions of the 1994 law. The proposed law of Mmes. Bribosia and Maximus additionally tried to solve the law enforcement problem by requiring everyone who would be able to help in decrypting to do this, provided the help is necessary for the investigation.

3. Developments to regulate cryptography
None.

Brazil [Sources 3, 5]

1. Export/ import controls
There are no export or import controls, but the government is working on a regulation.

2. Domestic laws and regulations
There are no controls on crypto use.

3. Developments to restrict cryptography
The government is working on a crypto law, but does not intend to restrict cryptography use.

Bulgaria [Sources 5]

1. Export/ import controls
Bulgaria has signed the Wassenaar Arrangement.

Burma (Myanmar) [Sources 5]

1. Export/ import controls
Export and import of cryptography may be restricted on the basis of the Computer Science Development Law (SLORC Law No. 10/96) of 20 September 1996, as amended by Law No. 3/98 of 23 February 1998. This law allows the Myanmar Computer Science Development Council to prescribe types of computer software and information that are not permitted to be imported or exported; violation of this prohibition carries a sentence of 5 to 10 years' imprisonment. According to an article by James Finch and Gladstone on the law (CTRL 2000: 67-70), as of March 2000, the Council had not promulgated any such permission or prohibition, implying that crypto import and export may be unrestricted.

2. Domestic laws and regulations
Cryptography is said to be restricted through a licensing regime.

Cambodia [Sources 5]
1. Export/ import controls
There are no import or export controls for cryptography. However, it is general practice to require licenses from
the Ministry of Posts and Telecommunications of Cambodia for exporting crypto hardware, and permission may
also be required to import crypto hardware. (See here for more details.)

2. Domestic laws and regulations
There is no regulation restricting use of cryptography. (See here for more details.)

Canada [Sources 1, 3, 4, 5, 8]

1. Export/ import controls
Canada follows (pre-December 1998) Wassenaar regulations. The export of items from Canada may be subject to
restriction if they are included on the Export Control List. In December 1996, Canada granted export of 56-bit
cryptography to most countries for a twelve-month trial period; this has been extended until 30 June 1998. Mass-
marker and public-domain software is excluded from the controls.

All types of cryptography can be transported between Canada and the United States, but cryptography imported
from the US which is not otherwise included in the Export Control List remains under US export rules and
cannot be exported from Canada if the US does not allow export. Public domain and mass-market software can
be freely exported, but if it contains US-origin goods, paperwork must be filled out.

A discussion paper by the Task Force on Electronic Commerce, from February 1998, A Cryptography Policy
Framework for Electronic Commerce, invited discussion over a review of Canada's crypto policy, including
export controls. It presented three policy options:

- relax controls either by matching the most liberal export policies of other countries, or through recognition
  of the availability of similar-strength crypto products in foreign markets;
- maintain the existing policy;
- extend the export controls by adding mass-market and public-domain software, possibly with a relaxation
  for key recovery products.

An analysis of the 189 responses to the discussion paper was published on 28 September 1998. Most respondents
favored relaxing controls on the export of cryptography.

Immediately following this publication, the government announced a new cryptography policy on 1 October
1998 (available at Industry Canada). Industry Minister John Manley affirmed the government's commitment to
the Wassenaar Arrangement. However, the export controls would take into account the practices of other
countries, so that they are not more restrictive than those of, in particular, the US, which had relaxed exports for
certain sectors in September 1998. Furthermore, the export-permit process would be streamlined. For many
products, users, or destinations, after a one-time review, general or multi-destination, multi-user permits would
be issued.

See the relevant sections of the Export Control List and a summary of Canada's export controls on cryptographic
software. Cf. also Baker and Hintze's comparison of US and Canada export controls.

2. Domestic laws and regulations
There are no domestic regulations on cryptography.

3. Developments to restrict cryptography
A discussion paper by the Task Force on Electronic Commerce, from February 1998, A Cryptography Policy
Framework for Electronic Commerce, invited discussion over a review of Canada's crypto policy. It presented
options for reviewing the domestic policy on encryption of stored data and on encryption of real-time
communications.
For domestic encryption of *stored data*, the paper suggested the following options:

- a laissez-faire model: continue with current policies and leave everything to the market;
- a minimum standards approach: encourage crypto users to store back-up crypto keys or to provide business data recovery; this would be done by stimulating industry self-regulation, and possibly through using the government's PKI (see below) to only cross-certify private crypto service providers that comply with the minimum standards;
- mandatory access legislation through prohibiting non-key recovery cryptography.

For domestic encryption of *real-time communications*, the paper suggested the following options:

- maintain the status quo, that is, telecom carriers are required to decrypt to the extent they are able to, and the only telecom carriers required for law enforcement and national security reasons to undo encryption they themselves employ are the new wireless providers of personal communications services and local multipoint communications services (the other carriers are currently not required to keep back-up copies of session keys);
- obligations on all carriers: require that all federally regulated telecommunications carriers providing encryption services retain the ability to decrypt for law enforcement and national securities agencies on receipt of a court order; this would be extended to provincially regulated service providers, but would not affect Internet service providers;
- mandatory controls: in addition to the second option, crypto service providers would be obliged to provide mandatory assistance for decryption, and users would be prohibited from using non-key recovery crypto.

An analysis of the 189 responses to the discussion paper was published on 28 September 1998. Most respondents favored relaxing controls on the use of cryptography.

Immediately following this publication, the government announced a new cryptography policy on 1 October 1998 (available at Industry Canada). Industry Minister John Manley affirmed the freedom to develop and use cryptography products. The government will not implement mandatory key recovery or a mandatory licensing regime for TTPs. The government does, however, encourage industry to use key-recovery techniques for stored data, and it will use government procurement to encourage commercial key escrow by acting "as a model user of cryptography". Finally, the government proposes to make it an offense to "wrongfully disclose private encryption key information and to use cryptography to commit or hide evidence of a crime." Moreover, "warrants and assistance orders also apply to situations where encryption is encountered - to obtain the decrypted material or decryption keys."

See the summary of Canada's crypto policy.

### 4. Developments favoring cryptography

The Federal Government is establishing a Public Key Infrastructure throughout its network of federal departments and agencies, enabling secure transactions between citizens and the state. The PKI will be fully implemented in late 1998. See the government's PKI information page, and the February 1998 discussion paper A Cryptography Policy Framework for Electronic Commerce.

---

**Chile [Sources 5]**

1. **Export/ import controls**
   There are no import controls.

2. **Domestic laws and regulations**
   There is no law regulating encryption use.
People's Republic of China [Sources 3, 5]

See also Hong Kong Special Administrative Region.

1. Export/ import controls
By State Council Order No. 273, "Commercial Use Password Management Regulations", published on 15 October 1999 and in effect since 7 October 1999, import and export of encryption products requires a license by the State Encryption Management Commission. According to a "clarification letter" sent to US businesses in China in early March 2000, this involves only hardware and software for which encryption and decoding operations are core functions. As a result, products in which cryptography is only built-in (such as mobile phones and browser software) are exempted. Moreover, the letter clarified that the regulations do not entail key escrow. However, the clarification letter only seems to apply to pre-2000 products. All products since 2000 seem to require a license.

2. Domestic laws and regulations
By State Council Order No. 273, "Commercial Use Password Management Regulations", published on 15 October 1999 and in effect since 7 October 1999, domestic crypto manufacture and use is severely restricted. Officially designated manufacturers must obtain approval from the State Encryption Management Commission for the type and model (including key length) of their crypto products. Organisations and individuals may not distribute encryption products produced abroad. People may only use encryption products approved by the Commission, and they may not use commercial encryption products developed by themselves or produced abroad. For this use, they must have approval by the Commission. Only foreign diplomatic missions and consulates are exempted from this approval. The deadline for registration of crypto users was 31 January 2000.

According to a "clarification letter" sent to US businesses in China in early March 2000, this involves, however, only specialized hardware and software for which encryption and decoding operations are core functions. As a result, products in which cryptography is only built-in are exempted. Moreover, the letter clarified that the regulations do not entail key escrow. However, the clarification letter only seems to apply to pre-2000 products. All products since 2000 seem to require a license.

For wireless crypto products, China seems to require use of a Chinese proprietary algorithm, and AES and WEP must be disabled.

Colombia [Source 5]

1. Export/ import controls
There are no import restrictions.

2. Domestic laws and regulations
Use of encryption is not restricted.

Costa Rica [Source 5]

2. Domestic laws and regulations
Use of encryption is apparently not regulated.
**Czech republic [Sources 5]**

1. Export/ import controls
Import is allowed "if it is declared by the importer not to be used for production, development, collection or use of nuclear, chemical or biological weapons."

Export is regulated according to the (pre-December 1998) Wassenaar Arrangement, implemented in the Law on the control of export and import of goods and technologies subject to international controls and further regulations on licensing export and import (regulations 43/1997 and 44/1997). However, the controls do not seem to be enforced, and the official government document Information Policy of the Czech Republic - Strategy Basics states: "The state shall not restrict import or export of cryptographic technologies."

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
No crypto regulation is expected.

**Denmark [Sources 1, 4, 5, 9]**

1. Export/ import controls
There are export controls according to the (pre-December 1998) Wassenaar Arrangement, including the General Software Note. The Danish representative agreed to the December 1998 Wassenaar changes, but this has met with serious resistance in the Danish parliament and the government's IT Security Council (see an article in Danish).

The Danish Encryption Policy (click on Emneord, Kryptering), published by the four responsible ministers on 7 April 2000, is based on the principle that "Efforts should be made to ensure the greatest possible liberalization of export control for dual-use goods and technologies, within the EU and Wassenaar, but with due consideration for the need to remain in control of the spreading of very sensitive products to sensitive end-users."

Import is not controlled, and this policy will be maintained, as confirmed the first principle of the Danish Encryption Policy.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
The Danish Technology Council, in an October 1995 report, discussed several options for cryptography policy, varying from doing nothing to prohibiting cryptography, without really taking a stand itself. According to the report, the issue is a Gordian knot, which should be cut soon by the Danish government.

The Danish IT Security Council adopted a policy on encryption in June 1996. The Council recommended that no limitations on encryption use should be introduced. Only in the case of telecommunications companies providing encryption as an integral part of their services, the companies should be able to decrypt a communication through a court order. The Council was of the opinion that secure and inviolable communication should be promoted and that any encryption prohibition at present is an illusion in reality, given the spread of efficient cryptography through the Internet.

The Committee, under pressure of time, restricted its study to a regulation of the *sale* of cryptography (not its manufacture, use or import). The Committee recommended that no regulation of cryptography should be introduced presently. It further recommended that the Expert Committee should continue to follow international developments, and carry out an analysis to assess the possibilities and consequences of introducing incentive schemes to induce people to use key-recovery crypto.

The Expert Committee was allowed to continue its work, and in May 1998, it presented its final conclusions (press release in Danish) in a "Report on incentive solutions" (updated version available in Danish and partly in English). The report recommended that no restrictions should be established on citizens' and companies' encryption capabilities. No initiative should be made to incite people to use key-recovery cryptography. Still, the Danish government should not reject the possibility of a future crypto regulation. The international development should be monitored, and the crypto question should be answered anew if an international direction of crypto policies should emerge.

The government was to take a final position on the crypto question in 1998, but it was only on 7 April 2000 that four ministers published a letter to the IT-security Council with the Danish Encryption Policy (click on Emneord, Kryptering). The four principles stress that the current policy of free use of encryption will be maintained. Moreover, the Danish government will actively promote the dissemination and use of strong encryption in Denmark. Denmark will not implement key recovery regulations, but the government should "also be mindful of the continued need of the police, in accordance with the legal protection guarantees afforded by the Administration of Justice Act, to make use of existing means of investigation to prevent and clear up crime."

### 4. Developments favoring cryptography

The Danish Teletrust Group has set up an Encryption Group to work on the technical and legal concept of public-key certifying authorities. A Centre Certifying Authority (CCA) would coordinate control and certification of key centres to provide secure keys within telecommunications. It would be necessary for such a CCA to have a legal basis. The Danish government has not (yet) implemented the initiative into law.

The Post Security Services (formerly Nordic), involving Denmark, Finland, Norway, Sweden, and Ireland, provides a 1024-RSA-based secure e-mail system, with the Post Office as Key Authority. Other countries have shown interest in being cross-certified.

---

**Egypt [Source 5]**

### 1. Export/ import controls

The import of tangible cryptography should take place through an importer who is registered on the Importers Register prepared by the Ministry of Economy and International Trade.

### 2. Domestic laws and regulations

According to the 2005 HRW report False Freedom, communications service operators and providers require permission for using encryption. Permission has to be given by the state communications agencies, national-security services and armed forces. Permission is granted only for 'satisfactory' reasons, which in practice has happened 'on numerous occasions'.

### 3. Developments to restrict cryptography

According to a 2002 document by the ITU on the legal framework for e-commerce in Africa, an 'encryption office shall be established for depositing the encryption keys, safeguarding the encrypted data, which cannot be decoded unless according to a court decision', suggesting an intention to mandate key escrow.
Estonia [Source 5]

1. Export/ import controls
There are no import controls, but export is controlled along the Wassenaar model. Licenses for export can be obtained from the Ministry of Foreign Affairs.

Back to the Table of Contents

Finland [Sources 4, 5, 8]

1. Export/ import controls
Import of cryptography is not regulated.

For export, a license is required through the Export Control of Dual-Use Goods Act (562/96), which implements the EU recommendation on export of dual-use goods and the Wassenaar Arrangement. A license is not needed if the crypto product is sold freely in retail and does not require extensive vendor support. The Ministry of Trade and Industry announced (in Finnish) on 4 December 2000 that as of Spring 2001, mass-market cryptographic software of unlimited key length can be freely exported to all countries, in line with the Wassenaar Arrangement decision of 1 December 2000.

The government agreed upon a crypto policy on 7 October 1998. The National Cryptography Policy guidelines of 12 October 1998 (copy available in Finnish) affirm the commitment to the Wassenaar Arrangement and EU recommendation. However, Finland aims to influence the reform of the international export regulations so that control lists correspond to technical development, and to ensure that the necessary restrictions will not unreasonably impede normal foreign trade.

See also section 5.1 of Simo-Pekka Parviainen's thesis.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
At the OECD meeting of December 1995, Finland did not approve key escrow proposals. The chairman of the Finnish public administration's group for data security affirmed that Finland will not require key escrow.

The government crypto policy guidelines (in Finnish) of 12 October 1998 affirm the support of free trade and use of cryptography. The provision of crypto services will be subject to a licensing and other authorization systems, based on voluntary action. Key escrow will not be mandatory. In criminal investigation, suspects do not have to assist in decryption of encrypted stored or transported data, but the authorities "may demand the provider of certification services or the maintainer of the encryption system to hand over a secret key in their possession or to otherwise contribute to the investigation of individual encrypted data". By 31 December 1998, the Ministries of Justice and the Interior will clarify the need to reform the Coercive Criminal Investigation Means Act.

4. Developments favoring cryptography
The Post Security Services (formerly Nordic), involving Denmark, Finland, Norway, Sweden, and Ireland, provides a 1024-RSA-based secure e-mail system, with the Post Office as Key Authority. Other countries have shown interest in being cross-certified.

The Privacy and Data Security in Telecommunications Act of June 1999 (no. 565-1999) allow telecoms users and subscribers "right to code their telecommunications message in the way they wish utilising the technical possibilities available thereto". Telecom operators have to inform users about the possibilities to protect communications. See sections 5 and 6 of the Act (also available in Finnish).

Back to the Table of Contents
France [Sources 1, 3, 4, 5, 6, 7]

1. Export/ import controls
France has signed the Wassenaar Arrangement for export controls, with the exception of the (pre-December 1998) General Software Note. See the government's SSI site for a list of applicable laws and decrees.

The import from countries outside the EU and the EEA (European Economic Area) and export of cryptography is regulated by the Law No. 2004-575 of 21 June 2004 for the trust in the digital economy (Loi pour la confiance dans l'économie numérique) and Decree No. 2007-663 of 2 May 2007 (... relatifs aux moyens et aux prestations de cryptologie). Articles 29, 30, 31, 34, 35, 36 and 40 of the Law, and further specified by the Decree, restrict import and export of cryptography products and services. Cryptography that can only be used for authentication is free of restrictions (art. 30(II)); the same holds for various specific types of cryptography mentioned in Annex 1 of Decree 2007-663. The procedure and forms for declaration and authorisation are specified in an Order of 25 May 2007 (définissant la forme et le contenu des dossiers de déclaration et de demande d'autorisation d'opérations relatives aux moyens et aux prestations de cryptologie).

Import from within the EU/EEA is free; import from other countries is subject to declaration, except for categories designated by decree (art. 30(III)). Export is subject to authorisation, except for categories designated by decree (art. 30(IV)). Authorisations and declarations executed prior to this law remain valid until their expiry date (art. 40). Failure to comply with these requirements is punishable with up to one (declaration) or two (authorisation) years' imprisonment and a fine of maximum 15,000 or 30,000 euro, respectively (art. 35).

History
Formerly, the regulation was the law of 26 July 1996 (see article 28 (in French)) and the decrees implementing it of 24 February 1998, no. 98-101 (in French), as changed by decree 2002-688 (in French), and of 17 March 1999. Decree 99-200 of 17 March 1999 (text in French, and again) specified categories of cryptography which do not require any prior formality. Decree 99-199 of 17 March 1999 (text in French and again) specified categories of cryptography for which prior declaration is required (and no longer prior authorization). These decrees replaced the decrees 98-206 and 98-207 of 23 March 1998 (text in French).

In accordance with Jospin's January 1999 speech (text in French), a law was proposed for full liberalization of crypto import. A Bill on the Information Society (No. 3143, text in French) was approved by the Council of Ministers on 13 June 2001, but stranded in parliament. Chapter II of the Bill contained an extensive revision of the crypto regulations. The import and export rules were proposed as follows.

- authentication-only crypto is entirely free (art. 37-II);
- transfer from an EU member and import of crypto that can be used for confidentiality must be declared (decrees may specify crypto exempt from this requirement) (art. 37-III);
- transfer to an EU member and export of crypto that can be used for confidentiality requires authorization (decrees may specify crypto exempt from this requirement) (art. 37-IV);
- failure to declare is punishable with up to one year imprisonment, failure to comply with authorization with up to two years' (art. 43);
- declarations and authorizations executed prior to this law remain valid until their expiry date (art. 49).

Similar provisions have now been enacted through the law on trust in the digital economy (see above).

2. Domestic laws and regulations
France used to restrict the domestic use and supply of cryptography for a long time (see below under History). This restrictive legislation (authorization and declaration were required for almost all cryptography) was slightly liberalized in 1996, when a law was passed mandating key deposits with Trusted Third Parties (TTPs). However, the domestic use of cryptography was liberalized in January 1999. Subsequently, other kinds of regulation (decryption order, raising punishment) have followed.

Current state of the law
The use of cryptography is free, according to article 30(I) of the law No. 2004-575 of 21 June 2004 for the trust in the digital economy (Loi pour la confiance dans l'économie numérique). The provision of crypto services is subject to regulation: service provision must be declared, except for services designated by decree that do not harm security or defense interests. Service providers are subject to professional secrecy (art. 31 of the digital-economy act). Failure to declare is punishable with up to two years' imprisonment...
and a fine of up to 30,000 euro (art. 35(III)). The law also creates liability for service providers that store private keys (art. 32). Moreover, the Prime Minister can prohibit circulation of cryptography if its supplier does not comply with the regulations, even of the supply is free of charge (art. 34, sanctioned with up to two years' imprisonment (art. 35(II)).

A decryption order has been enacted by the Law 2001-1062 of 15 November 2001 on daily security (JO 16 November 2001, p. 18215). Article 30 inserts a Title IV in the Code of Criminal Procedure that entails a power to require all qualified persons to decrypt or to hand over decryption keys if encrypted data are encountered during an investigation (art. 230-1 para. 1 FCCP). If it is necessary for the investigation of a crime with a maximum penalty of at least two years' imprisonment, the police can ask the national-security services to crack encrypted data (art. 230-1 para. 2 through 230-5 FCCP). To this end, a Technical Assistance Center (Centre technique d'assistance) was created within the Ministry of the Interior by Decree 2002-1073 of 7 August 2002 (JO 10 August 2002, p. 13713), the activities of which are secret. Article 31(II) inserts a penalization in the Criminal Code: someone who fails to comply with a decryption order is punishable with a maximum of three years' imprisonment and 45,000 euro, or with five years' and 75,000 euro if decryption could have prevented or mitigated the effects of a crime (art. 434-15-2 FCC). According to article 31(I), TTPs offering confidentiality services are required to hand over the decryption keys of their customers or to decrypt themselves, under threat of two years’ imprisonment and a fine of 45,000 euro (art. 11-1 of the Law of 10 July 1991 on the secrecy of correspondence by telecommunications).

Maximum penalties for crimes are raised if cryptography was used to prepare or commit a crime or to facilitate the preparation or commission of a crime, according to article 37 of the law No. 2004-575 of 21 June 2004 for the trust in the digital economy (Loi pour la confiance dans l'économie numérique). The maximum punishments of crimes punishable with up to three years' imprisonment are doubled, and higher maximum punishments are raised one category (with categories of 5, 7, 10, 15, 20, 30 years and life imprisonment). The punishment rise is not applicable, however, if the perpetrator, upon request, submits the plaintext and private key of encrypted messages.

Investigation powers are attributed to competent officials to investigate crimes related to the crypto regulations, including search and seizure of cryptography. Failure to comply with a request for information or documents or blocking the investigation is punishable with up to six months’ imprisonment and a fine of 7,500 euro (art. 36).

History of French domestic crypto laws

Before 1996, delivery, importation, exportation, and use of cryptography were subjected to: a) prior declaration if the cryptography can have no other object than authenticating communications or assuring the integrity of transmitted messages; b) prior authorisation by the Prime Minister in all other cases.

Simplified procedures existed for certain cryptography products or services or certain user categories. For authorisation, a dossier containing technical details and administrative data had to be submitted. Authorisation could be subjected to certain conditions in order to reserve the use of certain types of cryptography to defined user or application categories.

A press release of 16 October 1995 specified that use of cryptography for protecting passwords, access codes, subscriber numbers or bank card numbers for authentication purposes only necessitated a declaration by the provider when installing the service.

On 18 June 1996, France passed a law adapting its restrictions on cryptography (text in English or French). The law was published in the Journal Officiel on 27 July 1996 and is referred to as the 26th July law. Decrees on the application of the law (which have to be promulgated before the law is applicable) were published on 25 February 1998 (see the Journal Officiel of that date) (decree 98-101 of 24 February 1998 on the conditions of declarations and authorizations, and decree 98-102 of 24 February 1998 on the conditions for key escrow agencies), and several more decrees were published on 13 and 23 March 1998.

Cryptography that does not provide confidentiality could be used without restriction (so the prior requirement of declaration is cancelled); supply of authentication-only cryptography still had to be declared. Use and supply of confidentiality cryptography required authorization. Decree 98-206 of 23 March 1998 (text in French) specified categories of cryptography which did not require declaration or authorization (such as video-scramblers and ATMs). A supplier was exempted from the formalities for use exclusively for developing, validating, or demonstrating cryptography, if he informed SCSSI at least two weeks in advance. No authorization was given for cryptography for use by radio amateurs. A supply authorization for collective use exempted users from acquiring a use authorization. The use of cryptography with key lengths limited to 40 bits was exempted from declaration or authorization if ciphertexts can be cracked in maximum of 2⁴⁰ trials, according to decree 98-207 of 23 March 1998 (text in French) (this requirement was interpreted by Yves le Roux as a requirement to incorporate in every ciphertext a known plaintext (that is given to the authorities) to enable a known-plaintext attack); the supply of such cryptography was subject to declaration.
The law furthermore introduced Trusted Third Parties (TTPs), or rather, Key Escrow Agencies (KEA). If a KEA and its key-escrow scheme had been approved, users who escrowed their keys with the KEA would be able to freely use the cryptography scheme with these keys. The KEAs would be required to hand over keys to law enforcement under certain conditions. The only authorized Key Escrow Agency was SCSSI, according to a decree of 13 March 1998.

Decree 98-102 (text in French) specified the conditions for KEAs. It addressed, among others, the duration of a license to operate, the information the KEA had to provide to SCSSI, the information to register, user contract terms, a register of key requests by law enforcement and a separate (classified) one for key requests by security agencies, security measures, and how to handle when ceasing the activity. KEA employees were required to have a French security clearance.

In a 16 January 1998 press release, State Secretary of Industry Pierret welcomed the statement by Jospin that 56-bit cryptography should be liberalized as soon as possible to a simple regime of authorization.

The action plan on "Electronic Commerce" (see part III, "Creating Confidence", in particular part III.3), published 7 January 1998 by a task force led by Francis Lorentz, stated that the government was "resolutely oriented towards a liberal reading of the law". It urged a rapid implementation of the new law. It proposed further:

- a strong communication policy to promote the decrees;
- to promote with its (especially European) partners the principles underlying the policy;
- to bring about an agreement with France's most important trading partners on the principles and establishment of TTPs/ key deposits;
- to regularly review the regulatory framework (in particular, the 40-bit limit should be reviewed rapidly), conducting a broad consultation on this before the end of 1998;
- a government TTP/deposit service to be established as a role model, while stressing the importance of developing private operators for this function as well;
- that the decrees should not impose technical architectures for TTPs, but should limit themselves to functional demands.

It was unclear to what extent the restrictive regulation was enforced in practice; it was rumoured to be widely ignored. It seemed impossible for individuals or enterprises to obtain authorisation for "strong" cryptography. Even for state-owned industry, cryptography that does not serve military or high-grade security purposes had to be breakable. SCSSI, the office dealing with authorisation, rendered decisions without motivation.

For the state of the law before 1999 (NOTE: this is outdated now), see also the summary of the French encryption regulation (in pdf) by Yves le Roux, including a list of the then applicable laws and decrees. The French pre-1999 regulation (now outdated) could be summed up in the following table (reprinted with the kind permission of Yves le Roux):

<table>
<thead>
<tr>
<th>functionality</th>
<th>supply</th>
<th>import from outside EU/EEA</th>
<th>use</th>
<th>export</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication-only</td>
<td>declaration</td>
<td>declaration</td>
<td>free</td>
<td>declaration</td>
</tr>
<tr>
<td>confidentiality with key length under 40 bits</td>
<td>authorization or declaration (*)</td>
<td>authorization or free (*)</td>
<td>authorization or free (*)</td>
<td>authorization</td>
</tr>
<tr>
<td>confidentiality using Key Escrow Agency</td>
<td>authorization</td>
<td>authorization</td>
<td>free</td>
<td>authorization</td>
</tr>
<tr>
<td>other confidentiality</td>
<td>authorization</td>
<td>authorization</td>
<td>authorization</td>
<td>authorization</td>
</tr>
</tbody>
</table>

(*) The dispensation was given for crypto which is sure to be cracked in maximum $2^{40}$ rounds.

At a press conference (text in French) on 19 January 1999, Prime Minister Jospin announced the liberalization of the domestic crypto legislation. Use of cryptography of up to 128 bits is allowed as per direct (this was raised from 40 bits), while a law is being prepared for the complete liberalization of crypto use (see below). The mandatory nature of key deposits with TTPs is abolished. These changes were implemented in decrees 99-200 of 17 March 1999 (text in French) and decree 99-199 of 17 March 1999 (text in French), pending the law which is to offer full liberalization of crypto use. See the summary table above (under 1) for a specification of cryptography of which the use is free.

Subsequently, a law was proposed to relax the previous restrictive crypto regulations. As outlined in the October 1999 Policy paper on the adaptation of the legal framework to the information society, the Bill on the Information Society (No. 3143, text in French) was approved by the Council of Ministers on 13 June 2001 (see general information in French on this bill). The bill stranded in parliament, however. Chapter II of the Bill contained an extensive revision of the crypto regulations. Some of these amendments (below indicated with (#)) were enacted in the November 2001 Law on daily security, others (indicated with &) in the June 2004 Law on trust in the digital economy (see above). The proposed domestic rules were as follows.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM
use and provision
- use of crypto is entirely free (art. 37-I); (&)
- authentication-only crypto is entirely free (art. 37-II); (&)
- provision of cryptography that can be used for confidentiality must be declared (decrees may specify crypto exempt from this requirement) (art. 37-III); failure to declare is punishable with up to one year imprisonment (art. 43); declarations executed prior to this law remain valid until their expiry date (art. 49); (&)

TTP services
- provision of crypto services must be declared (sanctioned with up to two years' imprisonment (art. 43-III)); such TTPs can subject themselves to voluntary accreditation (art. 38);
- TTPs are held liable under certain conditions, both for confidentiality (art. 39) (&) and authentication (art. 40) services;
- the Prime Minister can prohibit circulation of cryptography if its supplier does not comply with the regulations (art. 41, sanctioned with up to two years' imprisonment (art. 43-II)); (&)
- Key Escrow Agencies have to decrypt or give decryption keys upon order, sanctioned with up to two year's imprisonment (art. 42); (#)

criminal procedure and decryption order
- competent officials are attributed several powers to investigate crimes related to the crypto regulations; failure to comply with a request for information or documents or blocking the investigation is punishable with up to six months' imprisonment (art. 44); (&)
- if cryptography was used to facilitate the preparation or commission of a crime, the maximum punishment can be raised by a certain amount (but not if the offender handed over plaintext or decryption keys) (art. 45); (&)
- failure to comply with a decryption order (see below) is punishable with maximum three years' imprisonment, or with five years' if decryption could have prevented or mitigated the effects of a crime (art. 46); (#)
- a power is introduced to require all qualified persons to decrypt or to hand over decryption keys if encrypted data are encountered during an investigation (proposed art. 230-1 para. 1 FCCP); (#)
- if it is necessary for the investigation of a crime with a maximum penalty of at least two years' imprisonment, the police can ask the national-security services to crack encrypted data (proposed art. 230-1 para. 2 - 230-5 FCCP). (#)

See the government SSI site on the applicable laws and decrees. For former regulations, see the (now outdated) summary of the pre-1999 French encryption regulation (in pdf) by Yves le Roux.

Germany [Sources 1, 3, 4, 5, 7]

1. Export/ import controls
Export is regulated according to the EU regulation and the Wassenaar Arrangement, in the regulations as amended according to the General License Nr. 16 (pdf text in German, published in the Bundesanzeiger of 31 August 1999, in force since 1 September 1999 (earlier version in Bundesanzeiger 32a of 15 February 1997)).

A press release of 27 August 1999 of the Ministry of Economic Affairs specified the new export controls, which stated that export controls for mass-market cryptography are limited to the absolute necessary. Mass-market crypto export within the EU has already been liberalized by the EU. Except for export to a few countries or for sensitive (military) applications, companies can now decide themselves whether a product falls within the category of mass-market crypto for which a general license suffices. There is no general requirement to declare, but exporters must be able, when requested, to hand over the specifics of exports. When in doubt, the Federal Export Agency (BAFA) will help (see address list).

See also section 5.3 of Simo-Pekka Parviainen's thesis.
A good article by Stefan Schuppert on Germany's export regulations (in German) appeared in Computer und Recht 2001/7, p. 429-434.

2. Domestic laws and regulations
The Amateur Radio Ordinance (Verordnung zum Gesetz ueber den Amateurfunk) of 15 February 2005, BGBI. 2005, 242, prohibits encryption of amateur radio traffic 'to mystify its contents' (zur Verschleierung des Inhalts) (art. 16(8)). Formerly, the Ordinance required amateur communications to be in 'plain language', initially for international communications (in the 1982 Order for the Radio Service Implementing the International Telecommunications Treaty) and since 1998 also for domestic communications.
3. Developments to restrict cryptography
On 2 June 1999, the German government announced its "Corner points of the German crypto policy" ([Eckpunkte der deutschen Kryptopolitik](http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM)). There are five cornerstones.

1. The government does not intend to restrict the free availability of cryptography. It will actively support the spread of secure encryption in Germany.
2. The government will take measures to establish a framework of trust for secure encryption.
3. The government considers indispensable the ability of crypto manufacturers to develop secure and powerful crypto products.
4. The spread of strong cryptography should not erode the government's interception powers. Developments will therefore be closely monitored, and a report will be issued after two years. Besides, the government will make an effort to enhance the technical competence of law-enforcement and security agencies.
5. The government greatly values the international cooperation in crypto policy. It will advocate market-driven, open standards and interoperable systems.

History of the discussions about crypto regulation
Several politicians have expressed a desire to regulate cryptography. There have been many conflicting rumours on the likelihood of a crypto regulation. Interior Minister Kanther stated on 22 July 1997 that presently, there will be no crypto law; first, one should investigate what is technically feasible and useful. Overall, the government seemed to lean toward an intention not to regulate cryptography.

Allegedly, the government has been considering three variants of a crypto regulation:

1. crypto service providers would have to store escrowed keys and if necessary hand these over to law-enforcement
2. 1 + marketing of encryption products would require a license
3. 1 + 2 + prohibition of non-licensed (escrowed) encryption

Federal Interior Minister Kanther stated, in a speech on 28 April 1997, he wants to control encryption, by allowing only technologies whose manufacturers agree to provide keys to law enforcement (this seems option 2 in the above). In June 1997, however, the Interior Ministry seemed to favor a two-year voluntary key-escrow approach, in which the government would certify cryptography products which incorporate key-escrow (which seems option 1 in the above). Use of certified products would be voluntary. In October 1997, parliamentarian Tauss revealed that Kanther favours a crypto chip, comparable to the US Clipper chip, for use by the government, in order to create market pressure to push others to use the same technology. There is little support from industry for such an approach. The discussion over this "Pluto chip" was downplayed in early 1998, when producer Siemens and commissioner BSI (government agency for IT security) stated that the chip did not contain a backdoor.

The German federal government was, however, itself divided over the issue. Contrary to Kanther, the Minister of Economic Affairs Rexrodt opposed any restriction on crypto use. Likewise, the state Ministers of Economic Affairs in a March 1997 conference in Eltville spoke out against a ban on cryptography. Justice Minister Schmidt-Jortzig also opposed a restrictive crypto regulation. The initiative on Electronic Commerce ("Elektronischer Geschäftsverkehr"), dated 29 October 1997, declares: "The federal government does currently not intend to legally regulate the marketing or use of crypto products. In Germany, therefore, crypto systems can be freely chosen and used." Ulrich Sandl, from the Ministry of Foreign Affairs, said at the RSA Data Security Conference, 13 January 1998, that GAK systems were ruled out until at least the end of the year; moreover, he implied that use of US key recovery products may not be in accordance with German privacy law.

In December 1996, a meeting behind closed door was apparently held by federal and state Secretaries of State, discussing crypto regulation. The outcome of the meeting seemed to be some proposal to regulate cryptography: only licensed crypto could be used, and crypto manufacturers and distributors would be required, in order to have their products licensed, to ensure deposit of private crypto keys for law-enforcement and national security access, as well as to deposit the crypto source code. Distribution and use of non-licensed crypto would be banned. However, rumours over the status of such a proposal widely differed: some claimed that the proposal was merely a shot in the blue to trigger reactions, others claimed it was a (preliminary) draft of a impending regulation.

The Bavarian Secretary of Internal Affairs demanded a federal law against conspiratorial encryption technologies in telecommunications.
In the April 1997 parliamentary debate on the Information and Communication Services Law, the FDP explicitly spoke out against a crypto regulation. CDU/CSU-MP Marschewski stated that encryption should forthwith be put under a Europe-wide licensing regime. The political party Bündnis/ Die Grünen opposes a cryptography prohibition or a restrictive (e.g., key-escrow) regulation. The German Federal Parliament, in a 20 June 1996 resolution, found that effective encryption procedures may be freely chosen by participants within the scope of the constitutional right to confidential communication (which may be breached for internal or external security reasons).

An interministerial Task Force on Crypto Politics was set up in October 1996 to develop concrete suggestions for an overall political strategy on IT security until the end of 1996. The federal Minister of Economic Affairs, in announcing the Task Force on 7 October 1996, stated that a trade-off should be found between the equally important principles of freely choosing cryptography and preventing criminal crypto abuse.

The German Council for Research, Technology and Innovation, in a December 1995 report on the Information Society, recommends that legal preconditions have to be made for the decryption of documents by state authorities, that specify the criteria for decryption competence and unequivocally regulate the seizure of documents. The report states that in developing and implementing cryptography products it has to be realized that it must be possible to decrypt single documents in relation to the execution of criminal procedure law.

A conference of Justice Ministers in December 1995 expressed concern that law enforcement is not keeping pace with technological developments. Federal Minister of Justice Schmidt-Jortzig acknowledges the problem of law enforcement, but doubts that an encryption prohibition could be enforced. Moreover, a German regulation would be inadequate to deal with the global matter of cryptography. In March 1997, at a conference of his FDP party, he called demands to ban cryptography deeply illiberal.

In its policy document *Info 2000: Deutschlands Weg in die Informationsgesellschaft*, the German government supported the European Commission's ETS initiative. A focal point was promoting encryption to protect confidential information by network operators. "In this respect the legal preconditions for the decryption by state bodies are to be examined." As regards the fight against crime, "dangerous gaps" in law enforcement's ability through criminals' use of encryption should be stopped as soon as possible. "Where this should not be possible with the available methods, new forms also of technical information provision should be considered, to not let crime get a lead." The deployment of criminal law means should be considered only as an "ultima ratio".

The Enquiry Committee "Future of the media" of the German Parliament recommended in 1998 not to restrict cryptography. "The capabilities of users to protect themselves through cryptography should, given the current state of understanding, not be legally restricted. A restriction of the free use of such techniques can not, in this understanding, be justified in a cost-benefit analysis." (BT/DS 13/11002, recommendation 13)

Magazine "Der Spiegel" reported on 8 January 1996 that the German Ministry of the Interior is working on a draft law which would prohibit (unescrowed?) cryptography. It published another article in December 1996 on impending restrictive legislation (see above).

See Ulf Moeller's *Kryptographie: Rechtliche Situation* (in German), an action page by Nicolas Reichelt with many newspaper articles (in German), and more documents collected by Christopher Kuner (mostly in English), including a list of opinions of political parties (in English). There is also an extensive list of opinions and newspaper reports by Lutz Donnerhacke.

Back to the Table of Contents

### 4. Developments favoring cryptography


Back to the Table of Contents

Ghana [Sources 5]

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
1. Export/ import controls

There are no import or export controls. [Source: 2002 ITU document]

2. Domestic laws and regulations

None. [Source: 2002 ITU document]

Greece [Sources 5, 9]

1. Export/ import controls

Greece has signed the Wassenaar Arrangement, so export controls should be regulated according to the (pre-December 1998) regulations, including the General Software Note.

2. Domestic laws and regulations

None.

Hong Kong Special Administrative Region [Source 5]

1. Export/ import controls

Import, export, and transit of cryptography are regulated by the Import and Export (Strategic Commodities) Regulations, which closely follow the Wassenaar controls. Generally, a license is required from the Director-General of Trade and Industry for importing or exporting cryptography (symmetric over 56-bit key length), except for personal use or for generally available, unchangeable crypto. Contravening the licensing controls is punishable, on conviction on indictment, with an unlimited fine or seven years' imprisonment, and liable to administrative sanctions. For more information, see the Strategic Trade Controls Circular No. 12/04 on Import and Export of Encryption Products.

2. Domestic laws and regulations

There are no regulations on the use of encryption. Crypto products that are to be connected to the public telecoms network, however, must comply with the relevant Telecommunications Authority's network connection specifications.

3. Developments to restrict cryptography

The September 2000 Report of the Inter-departmental Working Group on Computer Related Crime investigated the problem of cryptography for law enforcement. Ch. 5 recommends legislation for some form of decryption order. The order should be modelled on current production orders of the Organized and Serious Crimes Ordinance. As safeguards, the report recommends judicial scrutiny, a requirement that the offence at issue has a maximum penalty of at least two years' imprisonment, and that there be legal protection of the confidentiality of the information thus obtained. To enforce the power, penalties "commensurate with those for the specific offence under investigation" are recommended (although the report does not suggest how the offence under investigation is to be determined if the encrypted material does not yield evidence). Complying should be possible by giving plain text or the necessary passwords, codes, software and hardware to enable decryption. Suspects would be required to comply, similar to suspects addressed with current production orders (which do not have a privilege against self-incrimination clause). See reactions to the report on FIPR's page.

Back to the Table of Contents
Hungary [Source 5]

1. Export/ import controls
Wassenaar and EU export controls are implemented through the Government Decree No. 50/2004 (III.23.) on Licensing foreign trade in dual-use goods and technologies. Export of mass-market encryption software is exempted.
Import of cryptography also falls under the Decree (see Part II): for import from outside of the EU to Hungary, an International Import Certificate is required (see artt. 14, 16ff).

2. Domestic laws and regulations
A provision in the Hungarian Digital Signature Act (text in Hungarian), which entered into force on 1 September 2001, holds that signature-creation data (such as a cryptographic key) shall not be used for other purposes than signing. The ministerial reasoning explains that the intention of this is to prohibit the use of private keys for cryptographic purposes, in the interest of national security. (Note that cryptographic keys not used for creating signatures can be used for encrypting.)

3. Developments to restrict cryptography
No.

4. Developments favoring cryptography
In February 2001, the Data Protection Commissioner issued a recommendation against regulating cryptography.

There is a law that provides an agency with the competence to assess cryptography; the agency can declare that it satisfies a minimum security level.

Iceland [Source 1]

2. Domestic laws and regulations
no

India [Sources 3, 5]

1. Export/ import controls
India requires an import license for encryptors. Import of crypto software is not restricted.

2. Domestic laws and regulations
The Information Technology Act 2000 (No. 21 of 2000) contains a decryption order. The Controller of Certifying Authorities may, according to art. 69 section 1, for national-security or crime-prevention reasons, direct any agency of the Government to intercept any information transmitted through any computer resource. Subsequently, according to art. 69 section 2, the "subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." Failure to comply can be punished with imprisonment of up to seven years, according to art. 69 section 3.

3. Developments to restrict cryptography
None.
Indonesia [Source 5]

1. Export/ import controls
There are no import restrictions for cryptographic products.

The export regulation is unclear. In any case, travellers with crypto software on a laptop do not require a license.

2. Domestic laws and regulations
I have had conflicting reports about crypto use: one source claims it is illegal, whereas another source says there are no use restrictions.

Iran [Source 5]

2. Domestic laws and regulations
According to the 2005 HRW report False Freedom, use of encryption for exchanging information requires a license. Users have to request permission by submitting crypto algorithm and keys and information about 'related parties' to the Supreme Council for Cultural Revolution, as regulated in art. 5.3.8 of the Rules and Regulations for Computer Information Providers.

Ireland [Sources 1, 9]

1. Export/ import controls
Import is not controlled.

Export is regulated according to the EU dual-goods regulation and the Wassenaar Arrangement, including the restriction of free export for mass-market software to 64-bit key lengths. The Framework for Ireland's Policy on Cryptography and Electronic Signatures of June 1998 and the Consultation Paper of August 1999 affirm the commitment to this legislation.

The responsible agency is The Licensing Unit of the Department of Enterprise, Trade and Employment (see address).

2. Domestic laws and regulations
The Electronic Commerce Act 2000 (nr. 27), which was enacted on 19 July 2000, contains a decryption order in article 27 (2) (c). A judge can issue a search warrant if there are reasonable grounds to suspect an offence under the Act has been committed. Such a warrant authorises investigation officers, among other things, "when the thing seized is or contains information or an electronic communication that cannot readily be accessed or put into intelligible form, to require the disclosure of the information or electronic communication in intelligible form". Persons or public bodies who fail or refuse to comply are guilty of a summary offence (art. 27 (4)). [What is the penalty for this?]

According to article 28, "Nothing in this Act shall be construed as requiring the disclosure or enabling the seizure of unique data, such as codes, passwords, algorithms, private cryptographic keys, or other data, that may be necessary to render information or an electronic communication intelligible." Hence, investigation officers can only require people to decrypt, not to hand over keys or passwords, and the power can only be used in relation to material seized during a search. The Act does not make an exception for suspects or mention the privilege against self-incrimination.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM
History
The Framework for Ireland's Policy on Cryptography and Electronic Signatures of June 1998 included the following basic principles: "The production, import and use of encryption shall not be subject to any regulatory controls 'other than obligations relating to lawful access'," and "Legislation will be enacted to oblige crypto users to release plaintext or crypto keys upon a lawful authorisation."

The Consultation Paper Outline of Legislative Proposals on electronic signatures, electronic contracts, certification service provision and related matters of August 1999 had a smaller set of basic principles, including "The production, import and use of cryptography will continue to be free from regulation." So, the lawful-access principle had been altered. The relevant section 20 of the Consultation Paper entailed a power to search and seize, but it did not contain a provision on requiring access to plaintext or crypto keys. According to the explanatory note, this provision provided lawful access to evidence, and it was not an enabler of mandatory key escrow or key recovery.

3. Developments to restrict cryptography
The Framework for Ireland's Policy on Cryptography and Electronic Signatures of June 1998 comprised the following basic principles:

- Users shall have the right to access strong and secure encryption and to choose any cryptographic method.
- The production, import and use of encryption shall not be subject to any regulatory controls "other than obligations relating to lawful access".
- Legislation will be enacted to oblige crypto users to release plaintext or crypto keys upon a lawful authorisation.

The Consultation Paper Outline of Legislative Proposals on electronic signatures, electronic contracts, certification service provision and related matters of August 1999 has a smaller set of basic principles:

- E-commerce users have the right to access strong and secure encryption, and users have the right to choose any cryptographic method. (Does this mean that non-e-commerce users of cryptography do not have the right to access strong crypto?)
- The production, import and use of cryptography will continue to be free from regulation.

On the history of the lawful-access principle, see above at 2.

Back to the Table of Contents

Israel [Sources 3, 5]

1. Export/ import controls
Import and export of cryptography require a license from the Director-General of the Ministry of Defence (who is aided in this by an advisory committee). The Director-General can grant a general license for certain crypto to make it freely exportable. There is no specific limit on key size. Licenses are granted on a case-by-case basis; according to the statistics (2002, Jan-Jun 2003) most requests are granted. See Encryption Controls in Israel for the applicable laws and the Ministry of Defence DDEC's policy of control and licensing, where forms are available for requesting a license.

See the address list for contact details.

2. Domestic laws and regulations
Engagement in means of cryptography (including use, manufacture, transport, and distribution) is regulated and requires a license from the Director-General of the Ministry of Defence (who is aided in this by an advisory committee). The Director-General can grant a general license for certain crypto that is subsequently free for use or distribution. Persons are exempted from applying for a license for engagement if they purchase from a license holder for sale and distribution, or if they download the crypto from the Internet for personal use.

According to an article (click on "The New Code Order") by Haim Ravia, the applicable laws are:

- Control of Commodities and Services (Weapons and Security Know-How) Declaration, 5747-1986
- Control of Exports (Weapons and Military Know-How) Order, 5737-1977
- Control of Commodities and Services Law, 5718-1957
- Control of Commodities and Services (Engagement in Means of Encryption) Order, 5734-1974

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
It appears that licenses are virtually always granted. No prosecutions for using unlicensed crypto are known, and strong encryption is widely used in Israel. See the Ministry of Defence DDEC's policy of control and licensing, where forms are available for requesting a license.

See the address list for contact details.
controls in October 1996 (allegedly under US pressure), establishing that businesses acquire approval for a cryptography export order larger than 50,000 yen. In July 2000, MITI announced its intention to mitigate the export controls for encryption software for Internet use.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
Japan sees encryption as an important tool for establishing information security in electronic commerce. Although initially it did not consider encryption a threat to law enforcement or national security, Japan's attitude seems to have shifted somewhat; the government has not (yet) decided which approach to choose. See Stewart A. Baker's article Japan Enters the Crypto Wars.

Japan's proposed wiretap law contains a reference to cryptography: if encryption renders partial eavesdropping or wiretapping difficult, law-enforcement is allowed to record all communications taking place.

4. Developments favoring cryptography
The Ministry of International Trade and Industry (MITI) (now called METI) published a draft policy paper "Towards the Age of the Digital Economy" in May 1997. For ensuring security, encryption and authentication technologies should be sophisticated through market competition. Development of cryptography and experiments of projects should be promoted, and network users should be provided with much more information about these, according to the draft.

Kazakhstan [Source 5]

1. Export/ import controls
The import and export is governed by Resolution No. 1037 Article 266 (30 June 1997) and Regulation No. 29. For importing or exporting cryptographic products, a license is required from the Licensing Commission of the Committee of National Security. The decisions of this Committee are subject to judicial review. The regulation is not enforced for travellers with crypto software on their laptops (a personal-use exemption).

2. Domestic laws and regulations
Cryptography is controlled by Resolution No. 967, Article 240 (13 June 1997) and Regulation No. 27. A license from the Committee of National Security is required for the development (including research), manufacture, repair (including technical support), and sale (including use and advertising) of cryptographic products.

Kenya [Source 5]

1. Export/ import controls
There are no import controls. [Source: 2002 ITU document]

2. Domestic laws and regulations
There is no requirement for key escrow, nor any restriction on key size. [Source: 2002 ITU document]

Kyrgyzstan [Source 5]

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM
1. Export/ import controls
There are no export controls.

Back to the Table of Contents

Latvia [Sources 4, 5]

1. Export/ import controls
Export controls in line with the EU dual-use regulation. Import controls mirror the export controls, i.e., an import license is required if export is controlled.

2. Domestic laws and regulations
There is no domestic restriction of cryptography.

3. Developments to restrict cryptography
None.

Back to the Table of Contents

Lithuania [Source 5]

1. Export/ import controls
Lithuania has signed the Wassenaar Arrangement, and export controls are regulated according to these regulations, by law of 25 June 1998 amending the Law Concerning Control of Import, Transit and Export of Strategic Goods and Technologies (see also the current version, in Lithuanian). Licenses for export can be obtained from the Ministry of Economy.

Import controls do not seem to be distinguished from export controls, and so, import licenses would be required for the listed crypto products.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
None.

Back to the Table of Contents

Luxembourg [Source 5]

1. Export/ import controls
Luxembourg has signed the Wassenaar Arrangement, so export controls should be regulated according to the (pre-December 1998) regulations, including the General Software Note.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
A draft Law on Electronic Commerce (text in French, Word; text in French, html) was proposed in mid-1999. It affirms in article 2 that the use of cryptography is free. Because cryptography is one of the major problems for law enforcement, the draft proposes a new article 66-1 in the Code of Criminal Procedure. The investigating judge (and only he) can command someone whom he considers to have a specific knowledge of the encryption, to give

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
him access to the "understanding of the seized protected or encrypted data" ("donne accès (...) à la compréhension de données saisies protégées ou cryptées"). The command can not be given to a suspect; the persons protected in articles 72, 73 and 76 of the CCP and persons who are obliged to keep secret information given them in the course of their professional activities, can excuse themselves. Otherwise, the person addressed is required to cooperate, under threat of a fine of LuxF 100,000 maximum.

Malaysia [Source 5]

1. Export/ import controls
There are no export or import restrictions.

2. Domestic laws and regulations
There is no regulation of crypto use.

Three Acts contain a power to require people to decrypt during a search; such a search is allowed when there is reasonable cause to believe that an offence under the Act at issue is being or has been committed. There is therefore no general power to order decryption.

- Art. 10 (1) (b) of the Computer Crimes Act 1997 requires (likely) users and people otherwise concerned with the operation of computers or material, during a search, to provide reasonable assistance for the purpose of accessing data or material that is reasonably suspected to be used in connection with an offence under the Act, as well as to produce any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible. Refusal to cooperate is punishable with at most 25k ringgit and/or three years' imprisonment (art. 11).
- Art. 79 of the Digital Signature Act 1997 requires people, during a search, to give access to computerised data whether stored in a computer or otherwise, which includes providing the necessary password, encryption code, decryption code, software or hardware required to enable comprehension of computerised data. Refusal to cooperate is punishable with at most 200k ringgit and/or four years' imprisonment (art. 83).
- Art. 249 of the Communications and Multimedia Act requires people, during a search, to give access to computerised data whether stored in a computer or otherwise, which includes providing the necessary password, encryption code, decryption code, software or hardware required to enable comprehension of computerised data. Refusal to cooperate is punishable with at most 100k ringgit and/or two years' imprisonment (art. 242). This Act contains a provision (art. 256(2)) allowing people to refuse answering questions if they thereby would incriminate themselves; by contrast, the privilege against self-incrimination can be deemed not to hold for complying with a decryption order.

Mauritius [Sources 5]

1. Export/ import controls
There are no export or import controls. [Source: 2002 ITU document]

2. Domestic laws and regulations
There are no domestic restrictions on cryptography for civilian use. [Source: 2002 ITU document]

Mexico [Sources 3, 5]
1. Export/ import controls
There are no export or import controls.

2. Domestic laws and regulations
There are no restrictions on crypto use.

Moldova [Source 5]

1. Export/ import controls
For import and export of cryptography, a license from the Ministry of National Security is required through Governmental Decision No. 859 of 13 August 1998.

2. Domestic laws and regulations
For use of cryptography, a license from the Ministry of National Security is required through Governmental Decision No. 859 of 13 August 1998.

Morocco [Source 5]

1. Export/ import controls
Import and export of cryptography requires a license from the government, according to Art. 13 of Law No. 53-05 (see under 2. Domestic laws). If the crypto only has the goal of ensuring authenticity or integrity, then prior declaration to the government suffices.

2. Domestic laws and regulations
Law No. 53-05 of 30 November 2007 on Electronic Data Exchange (Loi 53-05 relative à l'échange électronique de données juridiques) inter alia regulates cryptography services. Provision, utilisation (exploitation) and use of cryptography requires a license from the government (Art. 13). (If the crypto only has the goal of ensuring authenticity or integrity, then prior declaration to the government suffices.) The government can determine simplified regimes for certain types of crypto or for certain user categories.

The provisioning of cryptography means and services is exclusively reserved for electronic certification providers, and their personnel must be approved by the government (Art. 14).

The Netherlands [Sources 3, 4, 5, 7]

1. Export/ import controls
Wassenaar rules, including the (pre-December 1998) General Software Note. (The regulation was to be adapted according to the December 1998 Wassenaar changes before April 1999.) The applicable regulations are the 1962 Law on Import and Export (In- en uitvoerwet), the Decree on Export of Strategic Goods and its Annex (In- en uitvoerbesluit strategische goederen), and the 2006 Regulation on penalisation of unallowed transfer of software and technology of strategic goods by electronic media, faxes or telephone (Regeling houdende strafbaarstelling van ongeoorloofde overdracht van programmatuur etc.). All Dutch laws can be found at wetten.overheid.nl.

The licensing authority is the Afdeling Exportcontrole en Sanctiebeleid of the Ministry of Economic Affairs (see address). Technical details of license applications are reviewed by the Nationaal Bureau voor Verbindingsbeveiliging. For more information, see the Ministry's general export controls page.
2. Domestic laws and regulations

Decryption command (law enforcement)
If encrypted information is found in a computer during a house search, the police can order anyone who can reasonably be supposed to know the means of encryption to decrypt the information (article 125k section 2 Dutch Code of Criminal Procedure (DCCP)). The command cannot be given to a suspect, and persons with a right to non-disclosure can refrain from complying (article 125k para. 3 DCCP). (Through an oversight of the legislator, the former provision covering these privileges, art. 125m-old DCCP, was abolished on 1 January 2006 (in the Data Delivery Act, see below) without being replaced, temporarily - and unintentionally - abolishing the privilege against self-incrimination in case of decryption orders for 8 months, until it was repaired by the Computer Crime II Act (Staatsblad 2006, 300), in effect as of 1 September 2006, introducing art. 125k para. 3.)

If encrypted information is found in data delivered to the police on the basis of data-delivery orders (artt. 126nc-nf, 126uc-uf and 126zk-zn DCCP), the police can order anyone who can reasonably be supposed to know the means of encryption to decrypt the information; the command cannot be given to a suspect, and persons with a right to non-disclosure can refrain from complying (art. 126nh, 126uh and 126zp DCCP). These provisions were introduced together with the data-delivery powers in the Data Delivery Act (Wet bevoegdheden vorderen gegevens), Staatsblad 2005, 390, in force since 1 January 2006; art. 126zp was introduced by the Extension of Terrorism Investigation Act (Staatsblad 2006, 580) which allows terrorism investigations without probable cause. The Data Delivery Act was based on the Mevis Committee on Investigatory Data Gathering in the Information Society with its May 2001 report (in Dutch). According to the report, the proposed data-delivery orders would include an indication of the way in which the data are to be handed over, which implies that the data have to be produced in plaintext (see p. 82).

If encrypted communications were intercepted through wiretapping, the police can similarly order anyone who can reasonably be supposed to know the means of encryption to decrypt the communication (art. 126m para. 6, 126t para. 6 and 126zg para. 5 DCCP). The command cannot be given to a suspect, and persons with a right to non-disclosure can refrain from complying (paras. 7 and 8).

Failure to comply with any of these orders is punishable with up to three months' imprisonment (art. 184 Dutch Criminal Code).

Decryption command (telecom providers)
In case of a lawful wiretap, telecoms providers are required to undo encryption they themselves have applied, according to article 2 under e of the Wiretapping of Public Telecommunications Networks and Services Decree (Staatsblad 1998, 642, as adapted by the Decree of 5 June 2001, Staatsblad 2001, 262, available at www.overheid.nl/op/).

Decryption command and powers (security services)
The Intelligence and Security Services Act 2002 (Wet op de inlichtingen en veiligheidsdiensten 2002, Staatsblad 2002, 148, available in Dutch at www.overheid.nl/op/), grants a power to the national-security services to request decryption. Anyone who has knowledge of the decryption of encrypted data (encountered by security services when they hack computers (article 24, section 3) or intercept telecommunications (article 25, section 7)) is required to provide all necessary cooperation to decrypt upon written request by the head of the service. Failure to comply with the request is punishable with up to six months' imprisonment if it was not intentional, and with up to two years' imprisonment if the not-complying was intentional (art. 89).

The services also have the power to install technical provisions in order to disable encryption of the data stored or transmitted in the computers they hack (article 24, section 1 at b). Moreover, the intelligence and security service are granted the power to disable encryption of data, telecommunications, or data transfers (article 25, section 1, article 26, section 1, and article 27, section 1).

3. Developments to restrict cryptography

1994 pre-draft law
In March 1994, a Dutch predraft law on cryptography leaked out, the drift of which was a prohibition of having, using, or trading strong cryptography. Those with a "legitimate concern" could apply for a user license or a trade authorization. One condition for granting a license was giving information to an administration agency; the text did not state whether this information concerned only the algorithm or also all the keys used.

See the text of the Voorontwerp and Memorie van Toelichting (in Dutch).
After many protests from those who would be affected by the proposed regulation, it was withdrawn. The Dutch authorities are currently studying on alternatives to handle the issue. Although the draft regulation will not be continued in its present scope, it shows how much the national-security and judicial authorities fear wide dissemination of strong cryptography.

At a December 1996 public debate on cryptography, representatives from the Ministries of Economic Affairs, Transport (responsible for telecommunications) and the Interior clearly were in favour of the use of a key-escrow scheme, in line with (their interpretation of) the OECD discussions. Such a scheme would initially be voluntary and left to market self-regulation. However, the Ministry of the Interior (responsible for national security) stated that, although he did not think primarily of legislation, in the long run, use of non-escrowed encryption could give rise to (criminal) suspicion by law-enforcement, thus effectively mandating escrowed encryption.

Extension of decryption command (law enforcement)
Initially, the draft Computer Crime Act II (version of January 1998) also proposed to extend the power of the police to demand decryption to be given to suspects, in case of grave evidence against the suspect and if this is urgently necessary for finding the truth. After protests from the legal community against this infringement of the privilege against self-incrimination, this provision was deleted from the draft.

Trusted Third Parties policy
A document on TTPs, Nationaal TTP-project, was submitted to parliament on 3 June 1999 (TK 26 581) (text in Dutch). This sets a framework for TTPs, proposing a number of preconditions for TTPs who want to be part of a national TTP Chamber. For TTPs offering confidentiality services, there is a precondition of "lawgal access", but the document is not particularly clear on what this entails. There is not a particular requirement for confidentiality TTPs to store or recover private user keys.

For legal access, a "partnership approach" of government and industry should develop a "set of instruments acceptable to all parties" that ensures government access to encrypted data. This has been attempted in a project "Legal Access" (Rechmatige toegang), in which several large companies, ministries and security services participated. The project initially suggested that TTPs offering confidentiality services would be required to operate in such a way that they could provide access to their subscribers' keys or plaintext (see the coordination group's March 2001 minutes in Dutch, basing themselves on the technical report (in Dutch)). However, given the economic consequences, it was found to be unfeasible to establish a self-regulatory mechanism or to require confidentiality TTPs to store keys. The government therefore decided to refrain from measures for the time being, in the memorandum Lawful access: options deciphered of 9 December 2002 (TK 26581, nr. 2, available at www.overheid.nl/op/).

Given this outcome, the earlier government threat of legislation (according to the 1998 TTP document, "If industry does not participate sufficiently actively in developing said set of instruments, the government will emphatically consider to fulfil the need for legal access with further legislation") will probably not be acted upon in the near future.

The Mevis Committee report (see above) recommends that TTPs be required primarily to decrypt themselves, not to hand over decryption keys (p. 83).

The overall TTP policy is being implemented in a project called TTP.NL, with representatives of government and industry, which performs several pilot projects. See for information in Dutch ECP.NL.

Back to the Table of Contents

4. Developments favoring cryptography
The government's policy document "Legislation for the electronic highway", of 12 February 1998 (TK 25 880), affirms that one of the premises to be balanced in establishing law enforcement powers is that the use of cryptography will remain free.

The draft Computer Crime Act II (submitted to parliament in July 1999 (TK 26 671)) contains a provision which would enable the police to "seize" data by making them inaccessible; one means of doing so would be for the police to encrypt the data on the computer of the holder.

The government Memorandum Vulnerability on the Internet (Nota KWINT, TK 26643, nr. 30) of July 2001 states that the government could stimulate the use of cryptography by serving as a role model and use cryptographic solutions in its own e-government security policy (p. 27).
New Zealand [Sources 1, 5]

1. Export/ import controls
New Zealand has signed the Wassenaar Arrangement, which it implemented verbatim in 1999. The current law includes the General Technology Note of Wassenaar, which exempts public-domain software from controls. For export of mass-market software, the Wassenaar restrictions hold. Export of cryptography was regulated through the Customs Act 1966 and the Export Prohibition Regulations of 1953, and since October 1996 by the Customs and Excise Act 1996. The responsible agency is the International Security and Arms Control Division (ISAC) of the Ministry of Foreign Affairs and Trade (MFAT).

Approval is also required for software that does not itself contain cryptography, but which has an interface specially designed for plugging in cryptography. Export of crypto software by electronic means does not fall under the export regulation.

Formerly, New Zealand did not implement the (pre-December 1998) General Software Note of Wassenaar. A license was required to export cryptography, including mass-market and public-domain software. What is more, MFAT seemed to interpret the regulations very strictly, even to the extent that publishing cryptography in books or academic journals required permission, according to an article by Peter Gutman. However, the export regulations did not seem to have been enforced.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
None.

North Korea [Source 5]

1. Export/ import controls
When requested to provide information about its encryption laws, the government of the Democratic People's Republic of Korea stated that they never release such information.

2. Domestic laws and regulations
When requested to provide information about its encryption laws, the government of the Democratic People's Republic of Korea stated that they never release such information.

Norway [Sources 1, 5, 6, 8]

1. Export/ import controls
Norway has signed the Wassenaar Arrangement, including the (pre-December 1998) General Software Note. Export is regulated by the Strategic Goods Export Control Act of 18 December 1987, nr. 93 (Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.) and the accompanying regulations of 10 January 1989, nr. 51 (Forskrift til gjennomføring av utførselsreguleringen for strategiske varer, tjenester og teknologi). For more information, see the Norwegian Department of Foreign Affairs' export control page (in English). A list of technologies is available in Norwegian.

There are no import controls. The 2001 policy document (see below, at 3) states that import of cryptography will remain free.
2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
In August 2001, the Norwegian government released their Norwegian Crypto Policy (Norsk kryptopolitikk, text in Norwegian). The policy in general takes a positive stance towards cryptography, arguing its value for securing data and for the economy. The policy declares itself against mandatory key-escrow, at least as far as individuals' use of cryptography for private purposes and authentication-only cryptography are concerned. Local mandatory key-escrow is, however, recommended for companies for internal use, because of the risk of data loss when a crypto key is lost. The policy also indicates that telecommunications service providers, including Internet access providers, can be required to provide plaintext to the government, if they are in possession of the plaintext or of the keys to produce the plaintext.
See also A basis for developing an integrated national crypto policy (text in Norwegian) by Lee Bygrave.

At the OECD meeting of December 1995, Norway called in question the use of Trusted Third Parties for judicial access to keys.

4. Developments favoring cryptography
A bill on central medical registries was proposed in 1994 that would use cryptographically pseudonymized entries.

The Post Security Services (formerly Nordic), involving Denmark, Finland, Norway, Sweden, and Ireland, provides a 1024-RSA-based secure e-mail system, with the Post Office as Key Authority. Other countries have shown interest in being cross-certified.

See also A basis for developing an integrated national crypto policy (text in Norwegian) by Lee Bygrave.

Pakistan [Source 5]

2. Domestic laws and regulations
The Pakistan Telecommunication (Reorganization) Act empowers the government to regulate cryptography. The sale and use of encryption hardware and software require approval by the PTA (Pakistan Telecommunications Authority?).

Peru [Source 5]

1. Export/ import controls
There are no import or export controls on cryptography software.

2. Domestic laws and regulations
There are no domestic laws regarding encryption.

Philippines [Source 5]

2. Domestic laws and regulations
E-mail encryption is not restricted.
Poland [Source 5]

1. Export/import controls
A license is required for exporting encryption software or hardware, in accordance with the EU dual-use goods regulation and the (pre-December 1998) Wassenaar Arrangement, including the General Software Note.

Import of cryptography is regulated as well, through a 1993 law; a general authorization or import certificate is required to buy encryption products abroad. The end-user must detail the kind of information to be encrypted and where the cryptography is to be installed. Legitimate businesses will be helped with their application. There is no need for declaration for crypto software exported from abroad under the Wassenaar General Software Note.

2. Domestic laws and regulations
None.

Portugal [Source 9]

1. Export/import controls
Portugal has signed the Wassenaar Arrangement, so export controls should be regulated according to the (pre-December 1998) regulations, including the General Software Note.

2. Domestic laws and regulations
None.

3. Developments to restrict cryptography
None.

Puerto Rico [Source 5]

1. Export/import controls
There are no import controls.

2. Domestic laws and regulations
There are no restrictions on crypto use.

Romania [Sources 5]

1. Export/import controls
There are no import controls.

Romania has signed the Wassenaar Arrangement, so export controls should be regulated according to the (pre-December 1998) regulations, including the General Software Note.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM
Russia [Sources 3, 5, 7]

1. Export/ import controls
A license is required for the importation of encryption facilities manufactured abroad. The export of cryptography is subjected to a tightened state control. Importers and exporters need licenses by the Ministry of Trade. Russia has signed the Wassenaar Arrangement, but does not implement the (pre-December 1998) General Software Note; its regulations are more stringent than the Wassenaar Arrangement.

2. Domestic laws and regulations
On 3 April 1995, president Yeltsin issued a decree prohibiting unauthorized encryption. State organizations and enterprises need a license to use encryption (for both authentication and secrecy, for storage as well as transmission). Other enterprises and organizations using uncertified cryptography do not receive state orders. The Central Bank shall take measures against commercial banks that do not use certified cryptography when communicating with divisions of the Central Bank.
The development, production, sale, implementation, or operation of cryptography without a license is prohibited. Apparently, a license is also required for all users for using cryptography.

Licenses are issued by the Federal Security Service, FSB, in which the former FAPSI (the Federal Bureau for Government Information, a former department of the KGB) was integrated in 2003. The license process is based on internal regulations.

The government intended to amend the domestic regulations on cryptography, it announced in a Duma hearing on 18 May 2000. [source: World Internet Law Report 2000/8, p. 29]

Back to the Table of Contents

Rwanda [Sources 5]

3. Developments to restrict cryptography
At a 1998 workshop on ICT Policy and Strategy in Rwanda, organised by the Rwanda government, ECA, UNESCO and USAIS in December 1998, the draft report stated: "Transparency as a rule in communication: encryption of information should be regulated." It is not known whether this has led to any concrete legislative proposals or legislation.

Back to the Table of Contents

Saudi Arabia [Sources 3, 5]

1. Export/ import controls
There are no import or export controls, according to source [3].

2. Domestic laws and regulations
It is reported that Saudi Arabia prohibits use of encryption, but that this is widely ignored.

Back to the Table of Contents

Singapore [Source 5, 10]

1. Export/ import controls
Export is covered by Wassenaar controls. See the Strategic Goods (Control) Act, in force since 1 January 2003, and the Strategic Goods (Control) Regulations, gazetted on 5 January 2004; the latter contains, among other things, provisions on electronic transmission of technology. See generally the Strategic Goods Control website.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
Formerly, there were import restrictions (requiring a license from the Trade Development Board), but these were abolished on 21 January 2000.

2. Domestic laws and regulations
There are no domestic controls on crypto use, but according to the Singapore Trade Development Board, "hardware equipment that will be connected directly to the telecommunications infrastructure will require approval from the Telecommunications Authority (TA) of Singapore. This is to ensure compliance and non-interference with telecommunications requirements." [source: EPIC survey 2000]

There is a decryption order for offences under the Computer Misuse Act, as amended in 1998 and in force since 27 February 1999. Art. 15 of this Act entitles the police (or other people authorised by the Commissioner of Police), with consent of the Public Prosecutor, at any time to have access to decryption information, code or technology for the purpose of investigation any offence under the Act (or any other offence disclosed by means of this power). Also, they are entitled to require users or people otherwise concerned with the operation of any computer that is likely related to an offence under the Act to provide reasonable technical or other assistance. Moreover, they are entitled to require any person in possession of decryption information to grant access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence. Obstructing the lawful exercise of these powers or failing to comply with an assistance or decryption request is punishable with at most S$10,000 or three years’ imprisonment.

3. Developments to restrict cryptography
The Infocomm Development Authority of Singapore press release of 19 January 2000 that announced the lifting of import controls, strongly encouraged companies to implement key recovery.

Slovakia [Source 5]

1. Export/ import controls
Slovakia has signed the Wassenaar Arrangement, so export controls should be regulated according to the (pre-December 1998) regulations, including the General Software Note.

Slovenia [Source 5]

2. Domestic laws and regulations
There are no restrictive domestic crypto laws or regulations.
For transfer of sensitive personal data (e.g., on race, sex, health) across telecommunications networks, the data must be protected by encryption methods, according to art. 14(2) of the Personal Data Protection Act (Zakon o varstvu osebnih podatkov). (See the article by Matej Kovacic about privacy in Slovenia.)

South Africa [Sources 1, 3, 5]

1. Export/ import controls
There are import and export controls for military cryptography, as regulated by the Defense Armaments Development and Protection Act 1968, No. R. 888, published May 13, 1994, and the General Armaments Control Schedule. Import of cryptography from military suppliers abroad and export of cryptography from military suppliers in South Africa are controlled (a military supplier being a company who has developed the technology specifically for sale to governments such as a government military contractor). Otherwise crypto import and export is free.
2. Domestic laws and regulations

Use of encryption is free for commercial or private organizations.

The provision of cryptography products or services, however, is strictly regulated through Chapter V of the **Electronic Communications and Transactions Act** of 31 July 2002, in force since 30 August 2002, and the implementing **Cryptography Regulations** of 10 March 2006 (Government Gazette No. 28594).

The Act has a broad scope: it includes the provision of cryptography within South Africa, but also the provision to someone who is in South Africa when he uses it, and to a person who uses it for the purpose of a business carried on in South Africa. Thus, it includes providing cryptography through the Internet to South Africans, providing crypto to foreign subsidiaries of SA companies, and providing crypto to persons who at one time or other will visit SA from abroad if they will use the crypto within the country. (For a further discussion of the scope, see the article Decoding the ECTA Cryptography Regulations by Louw & Augustine.)

Crypto providers can only operate after they have been registered, for which they have to provide the registration authority (the Director-General of the Department of Communications) with the information required (art. 29-30 Act + additional information listed in Art. 2 Regulations, including 'detailed profiles of trusted personnel' with 'supervisory or managerial responsibilities'), and pay an application and annual administration fee (art. 4 Regulations). The providers have to disclose information to relevant authorities investigating a crime, security agencies or cyber-inspectors (art. 31(2)). Violation of the law is punishable with up to two years' imprisonment (art. 32(2)).

A draft version of the Regulations, the 1 September 2004 Notice inviting Comment on Proposed Cryptography Regulations, also included as information to be provided contact details of all customers to whom a crypto product or service was provided in the preceding 6 months (art. 2(b)(vi), but this was struck in the final Regulations.

Before the ECT Act, there were some specific regulations that may still apply. Use or supply of telecommunications facilities or equipment must first be approved by ICASA, the Independent Communications Authority of South Africa (formerly SATRA), except on explicit prescription by ICASA. This does not apply if the device is connected between a modem or router and the computer. It is unclear whether and to what extent "telecommunications facilities or equipment" covers cryptography.

Use or provision of cryptography by government bodies requires approval from the relevant agency; likewise, crypto systems approved for government use require approval from the relevant agency to be used by commercial or private organizations.

Apart from restricting crypto services, there is also a power for the police to demand decryption in case of encrypted telecommunications. The **Regulation of Interception of Communications and Provision of Communication-Related Information Act** (No. 70, 2002), published in the Government Gazette on 22 January 2003, gives the police the power to request a designated judge to give a decryption direction (art. 21). This is possible before or during interception of telecommunications according to the act. The addressee has to comply by giving the decryption key or by providing decryption assistance (art. 29). Costs for decryption can be compensated (art. 31). Failure to comply is punishable with a fine of up to 2 million Rand or imprisonment of maximum 10 years for natural persons and employees, or a fine of 5 million Rand for organisations (juristic persons) (art. 51(4)). Numerous detailed provisions and conditions apply, see articles 1, 21 and 29. (Cf. also Discussion Paper 99 by the South African Law Commission on Computer-related crime (also at 2600), which was to lead to a Computer Misuse Act, but which has in the meantime been addressed by the ECT Act and the RICPCRI Act. Section 4.5.3 under 4(b) of the report proposed search and seizure powers, including the requiring of any person concerned with a computer or computer data to provide "the reasonable assistance that may be required to facilitate the execution" of the search warrant.)

3. Developments to restrict cryptography

None.

Back to the Table of Contents

---

South Korea [Source 5]

1. Export/ import controls

Import of encryption devices is restricted in South Korea through a government policy, not by legislation; it requires approval from the Ministry of Trade, Industry, and Energy. The import of encryption devices is prohibited, even for banks. The government is considering a law to give this a legal basis. The import of encryption software is not controlled. However, one report claims that the import license system was abolished several years ago.
South Korea has signed the Wassenaar Arrangement, so export controls should be regulated according to the (pre-December 1998) regulations, including the General Software Note.

2. Domestic laws and regulations
It seems that encryption services provided within a public switch telephone network can be restricted on an ad-hoc basis. There is no regulation governing the use of encryption.

3. Developments to restrict cryptography
Encryption policy is not published, despite a 1994 indication by the Ministry of Information and Communication that a policy would be published defining acceptable public, private, government, and telephone uses of encryption services and approved algorithms. Enquiries with the Ministry indicate it does not have plans for specific legislation.

Draft bills on electronic signatures and electronic commerce, however, may affect crypto use. The Draft Electronic Commerce Basic Law seems to oblige people to provide the government with crypto keys.

Spain [Source 1]

1. Export/ import controls
Export of cryptography is controlled according to the (pre-December 1998) Wassenaar and EU regulations, including the General Software Note. The international regulations are implemented in the Reglamento del Comercio Exterior de Material de Defensa y de Doble Uso, in force since 9 May 1998. The regulation does not make distinctions based on key lengths.

2. Domestic laws and regulations
The General Telecommunications Law (text, now outdated, in Spanish) of 24 April 1998 provided in article 52 that all information transmitted across telecommunications networks could be encrypted. Conditions on the encryption procedures could be established in the decrees that implement this law. The second paragraph of article 52 established that, if encryption is used for confidentiality, an "obligation could be imposed to notify either a General Administration body, or a public organisation about the algorithm or whatever encryption procedure is used, with an effect to control it following prevailing normatives. This obligation will affect all the developers which incorporate cryptography in their equipments or devices, the operators that include it in their networks or in the services they offer, and, if applicable, to the users that employ it." (translation GILC). People have warned that this might lead to mandatory key escrow or key recovery, if users would be obliged to "notify" the government about the "key procedure". See an article of July 1998 of Fronteras Electrónicas in English.

The same article 52 of the General Telecommunications Law required telecoms network and service providers who use encryption to accommodate the General Administration Body with the decoding devices they employ.

The General Telecommunications Law was replaced by a new General Telecommunications Law, 32/2003 of 3 November 2003 (text in Spanish, see Title III, Chapter III). The crypto provision was transferred to article 36. Para. 1 maintains that telecommunications may be encrypted. Para. 2, however, was changed somewhat. It now reads: "Encryption is an instrument for information security. Among its conditions of use, when it is used to protect the confidentiality of information, the obligation may be imposed to notify a General Administration State authority or a public authority, the algorithms or any other crypto procedure used, as well as the obligation to facilitate without any cost the encryption devices, in order to control it according to the law in force." The impact of the change is unclear.

3. Developments to restrict cryptography
See under 2.

Back to the Table of Contents
1. Export/ import controls

The import of cryptography is not restricted, nor will it in the future, according to the government's May 1999 Government Communication 1998/99:116 On cryptography.

Since January 1995, Sweden restricts export of encryption according to the Wassenaar Arrangement, including the General Software Note. This regulation refers to the EU regulation (1334/2000) instead of maintaining a national list of controlled goods. The relevant regulations are the Law on control of dual-use goods and of technical assistance (SFS 2000:1064) of 30 November 2000, and the corresponding Decree (SFS 2000:1217) (that replaced SFS 1998:400).

The Inspection for Strategic Products keeps supervision and information regarding the export controls (SFS 1995:1680).

The Government Policy On cryptography affirms the need for export controls, but states that these should be gradually liberalised. It stipulates that the regulations should explicitly place physical export on an equal footing with electronic export (via computer networks), so that Internet exports will also fall under the export regulations.

A Foreign Affairs press release of 23 June 1999 announced that as of 1 August 1999, the Inspection for Strategic Products has the power to proclaim rules for general export licenses for crypto products. The general export license published (TFS 1999:40, 1 July 1999) allows crypto exports of up to 128-bit symmetric mass-market crypto to a list of about 60 approved countries (Argentina, Australia, Bahrain, Bangladesh, Brazil, Bolivia, Brunei, Bulgaria, Canada, Chechnya, Chile, China, Cyprus, Ecuador, Egypt, Estonia, Hong Kong SAR, Hungary, Iceland, India, Indonesia, Israel, Japan, Jordan, Kuwait, Latvia, Lebanon, Lithuania, Macao SAR, Macedonia, Malaysia, Mauritius, Mexico, Morocco, New Zealand, Norway, Oman, Pakistan, the Philippines, Poland, Qatar, Romania, Russia, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Sri Lanka, Switzerland, Taiwan, Thailand, Tunisia, Turkey, Ukraine, the United Arab Emirates, Venezuela, Vietnam). Transport within the European Union is not considered export, so any crypto transfer is allowed. For other countries and products, an individual license is required. (See a paper with information about the application process.)

A report from the Swedish Cabinet Office (Regeringskansliet), Cryptography Policy: Possible Courses of Action for Sweden (in pdf) (original Kryptopolitik - möjliga svenska handledningslinjer in Swedish), from October 1997, set out the basis for discussion on a national crypto policy. It took as starting points that import of cryptography would continue to be free, and that the export controls would remain.

In February 1998, a Swedish company, Idonex, published the government's ruling that they could not export 128-bit crypto via ftp; they were granted an export license for 40-bit. The decision leaves unclear whether electronic export (through ftp) is covered by the controls or not. See the English info page.

See also section 5.2 of Simo-Pekka Parviainen's thesis.

2. Domestic laws and regulations


For the rest, there are no laws regulating cryptography domestically.

3. Developments to restrict cryptography

Sweden outlined its crypto policy in the 6 May 1999 Government Communication 1998/99:116 On cryptography. This affirms that there is at present no reason to limit the use of cryptography in Sweden. All shall have the right to choose such technologies themselves. "If developments should warrant more stringent regulations, the government will consider appropriate measures for creating means of legal access to the plaintext of encrypted information for law enforcement and supervisory authorities."

Although the government does not encourage key recovery, the Communication says that government authorities themselves should use key management systems with built-in functions for key recovery. For this, internal key-management bodies probably must be set up. Such bodies should be regulated "in such a way that they can serve as a model for the private market too." Moreover, the government should investigate whether there are reasons for the State to involve itself in a voluntary authorisation procedure of special TTPs that provide confidentiality services.
Before deciding upon this policy, Sweden discussed crypto policy in view of the discussions within the EU and the OECD. The October 1997 report by the Cabinet Office (Regeringskansliet), Cryptography Policy: Possible Courses of Action for Sweden (in pdf) (original Kryptopolitik - möjliga svenska handlingslinjer in Swedish), set out the basis for this discussion. The three starting points of the report were:

- "everybody has the right to use cryptography in order to secure stored data and communication";
- "prerequisites for Swedish users' voluntary deposit of their keys in Sweden should be created in response to the requirements of key deposit";
- "in order to enable law enforcement agencies to fight terrorism and drug dealers, rules and regulations for lawful access to plaintext and keys must be installed".

The report considered as a possible solution for balancing law-enforcement and user needs the voluntary deposit of private crypto keys, with legal access. It assumed that "many countries" will impose mandatory key deposits, and in order to facilitate communication with those countries, possibilities should be created for law enforcement to cooperate, either through key deposits in both countries or through international agreements. For national traffic in Sweden, the report considered that the current policy of free crypto use will be continued, and monitored "from time to time, how the various interests are balanced".

4. Developments favoring cryptography

The Swedish IT commission, which advises the government on strategic questions in the information technology field, released a report (SOU 1997: 73) in May 1997, Inför en svensk policy för Säker Elektronisk Kommunikation (Towards a Swedish Policy for Secure Electronic Communications). It recommended that no restrictions on the use of cryptography should be introduced. The trust in ICT could be severely reduced, and the prerequisites for maintaining an effective key management system are lacking. The commission dismissed the various forms of key management systems for private keys, such as key deposits and key recovery. The fight against serious crime and terrorism should use other police and security measures. The Swedish government should quickly make up its mind, so that it can influence the international work in the field, according to the commission. See the statement by the IT commission Avseende användning av kryptering (in Swedish).

Computer Sweden magazine, in July 1997, could not find anyone (who knows anyone) willing to publicly favor mandatory key deposits.

The Post Security Services (formerly Nordic), involving Denmark, Finland, Norway, Sweden, and Ireland, provides a 1024-RSA-based secure e-mail system, with the Post Office as Key Authority. Other countries have shown interest in being cross-certified. A representative of the Swedish post said that the encryption key in the smart card would not be escrowed unless forced by law.

The October 1997 report by the Cabinet Office (see under 3) stated there are no plans to change the policy not to restrict the use of cryptography in Sweden. It also mentioned that part of the electronic communication by government bodies will require the use of digital signatures and encryption.

Switzerland [Sources 1, 3, 5, 9]

1. Export/ import controls

Crypto import is not controlled. Import certificates will be given if the country of origin requires this.

The export of cryptography is regulated by the Goods Control Decree of 25 June 1997 (Verordnung über die Aus-, Ein- und Durchfuhr zivil und militärisch verwendbarer Güter sowie besonderer militärischer Güter) (text in German or English), which is based on the Goods Control Law of 13 December 1996 (text in German or English), in force since 1 October 1997. The export controls mirror the (pre-December 1998) Wassenaar Arrangement, including the General Software Note which excludes mass-market and public-domain software from the controls. Export to the about 25 members of the four international export control regimes (Australia Group, Missile Technology Control Regime, Nuclear Suppliers Group, Wassenaar Arrangement) requires an ordinary general license issued within a few days; export to other countries requires an individual license, although for exports to bona fide companies in uncritical countries, an extraordinary general license may be given. Crypto export through intangible means is covered by these regulations.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM

2009-02-02
Re-export is not permitted if the country of origin does not allow the export to the destination country.

See the information page of the State Secretary of Economic Affairs (German).

2. Domestic laws and regulations

Study [1] did not find cryptography regulations, but its follow-up study [9] claims there was a restriction on the use of certain cryptography: radio communications must remain understandable, and if a person wants to encrypt messages for professional reasons, he must obtain specific permission. This is presumably the same law as the paper to the OECD December 1995 meeting refers to: article 14 of the Telecommunications Concession Regulation (VFKV) required a license for radio traffic encryption; the license was given if the concessionaire can prove he needs confidentiality of his messages. The VFKV regulation were replaced on 1 January 1998 by the Frequency Management and Radio License Decree (Verordnung ueber Frequenzmanagement und Funkkonzessionen, FKV, current version from 9 March 2007). There is no license requirement for radio encryption, but article 10 on identification of broadcasts provides that if the radio traffic is not conducted in plain speech, the License Board will establish how identification of the traffic is to take place (para. 2), and the Board can require to make available the contents of the radio traffic (para. 3).

Encryption products that can be connected to a public telecommunications network must follow certain basic technical requirements, posed by the Swiss Federal Council, to ensure overall compatibility. This can be done by a declaration of conformity issued by the manufacturer, or by a review by the Federal Office for Communications (OFCOM).

Apart from these two specific regulations, there are no domestic crypto regulations.

3. Developments to restrict cryptography

None.

Syria [Source 5]

2. Domestic laws and regulations

According to the 2005 HRW report False Freedom, there is no law regulating use of encryption in electronic communications.

Trinidad & Tobago [Source 5]

2. Domestic laws and regulations

The Computer Misuse Act, 2000, passed in October 2000, contains a decryption order. Clause 16 provides that a "police officer executing a warrant (...) is entitled (...) to (...) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted program or data held in or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section; (...) and entitled to require any person in possession of decryption information to grant him or the authorised person access to such decryption information necessary to decrypt data required for the purpose of investigating an offence." Failure to comply with a decryption order can be punished with a fine of fifteen thousand dollars and imprisonment for two years.

See a summary and some comments on the act at TTCS.

Back to the Table of Contents
Tunisia [Sources 5]

1. Export/ import controls
Import of cryptography is restricted. It seems a government agency (Centre d'Etudes et de Recherches des Télécoms, CERT) has to examine and approve the crypto product. [Note: this may have changed in light of the decrees mentioned below, but I have no specific recent information on the import controls.]
I have no information about export restrictions in Tunisia.

2. Domestic laws and regulations
Telecommunication service providers need authorisation if they want to use encryption, and they have to deposit keys with the government, according to Decree No. 1997-501 of 14 March 1997 (Official Journal of the Tunisian Republic, 25 September 1997). [Source: 2000 EPIC survey] A September 1997 Order on crypto use in value-added telecoms services requires users and service providers to apply for a license to use encryption, while providing decryption keys. [Source: 2005 HRW report False Freedom]

A later decree, No. 2001-2727 of 20 November 2001, regulates the "conditions and procedures for the use of encryption means or services through telecommunications networks, as well as the exercise of related activities" [Source: August 2002 Telecoms Market Access Study]. This decree builds on the September 1997 Order, stipulating that encryption is now supervised by the Ministry of Defense and an encryption commission, while requests for a license are to be sent to the National Agency for Electronic Certification (ANCE), "including a detailed description of the means of encryption and a manual explaining how to use and program the encryption technology" [Source: 2005 HRW report False Freedom].

Turkey [Sources 1, 5]

1. Export/ import controls
Wassenaar controls (pre-December 1998), including the General Software Note.

2. Domestic laws and regulations
Source [1] did not find domestic regulations, but other reports suggest there may be restrictions.

3. Developments to restrict cryptography
Source [1] did not find developments to restrict cryptography.

Ukraine [Source 5]

1. Export/ import
Ukraine has signed the Wassenaar Arrangement. Export and import are subject to licensing, according to the Law On Licensing Certain Types of Economic Activity of 1 June 2000. Licenses are issued by the Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine (SBU). (Source: presentation (Word) by Russian-Ukrainian Legal Group.)

2. Domestic laws and regulations
Production, trade and use of cryptography are subject to licensing, according to the Law On Licensing Certain Types of Economic Activity of 1 June 2000. Licenses are issued by the Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine (SBU). A joint order, No. 88/66, of the State Committee for Regulatory Policy and Entrepreneurship and the SBU’s Telecom Department regulates the use of encryption and contains an application form to request a license. (Source: presentation (Word) by Russian-Ukrainian Legal Group.)

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM
United Kingdom [Sources 1, 3, 4, 5, 8]

1. Export/ import controls

Export is controlled in accordance with the EU dual-use regulation and the Wassenaar Arrangement in The Dual-Use Items (Export Control) Regulations 2000 (SI 2000/2620), amended several times (see DTI's legislation page, in particular the DUEC page). This includes export of crypto software to other EU Member States. Crypto export by intangible means (i.e., over the Internet) is now also covered by the regulation (contrary to earlier regulations).

There is a personal-use and Community-Licence exemption through the Open General Export License of 1 May 2004, for crypto goods. (This revoked the earlier OGEL of 28 September 2000.) This general license allows export of any controlled item (except functionally cryptanalytic tools) to most countries for personal use or for use by subsidiaries or collaborators in the course of "their own commercial cryptographic product development activities".

At the OECD meeting of December 1995, Nigel Hickson of DTI stated that export controls for approved products should be lifted. The policy Paper on regulatory intent concerning use of encryption on public networks of June 1996 announces that export controls will remain in place, but that the government would try to simplify export controls for encryption products used by licensed TTP's. This announcement was repeated in the Consultation Paper of 19 March 1997 on Licensing of Trusted Third Parties for the Provision of Encryption Services. In the April 1998 policy announcement, DTI commits itself to working internationally on the "updating and streamlining" of export controls, and this is repeated in the March 1999 consultation document.

The House of Commons Trade and Industry Select Committee, in its report of 18 May 1999 on this consultation document, recommended "that the Government consider the case for a review of the rationale for the continuation of export controls on cryptographic products, in the light of their widespread availability, and the procedures by which such controls are implemented."

The 1996 House of Lords Agenda for Action (at 6.39) wants the government to join other EU states in putting pressure on the US government to relax its export controls. In July 1998, DTI released a White Paper on Strategic Export Controls, which at 3.2 proposes to extend the controls on exporting crypto software to intangible transfers. Under such a policy, also exports by fax and email should fall under the export controls.

See also section 5.5 of Simo-Pekka Parviainen's thesis.

2. Domestic laws and regulations


The power can be given:

- if an intelligence service, the police, or the customs and excise have lawfully obtained encrypted data (art. 49 (1)), and
- if decryption is necessary in the interest of national security, crime prevention or detection, or the UK's economic well-being, or if it is necessary for the effective exercise or proper performance of a statutory power or duty, and if requiring decryption is proportionate and the only reasonably practicable means (art. 49 (2) and (3)), and
- if the person addressed is believed to be in possession of the decryption key (art. 49 (2)(a));
- in principle, by requiring the person to decrypt himself (art. 50 (1)), or, in special circumstances, by requiring the person to provide the decryption key (art. 50 (3)(c) jo. art. 51) - but not a key that is only used as an electronic-signature key (art. 49 (9));
- special cases apply for people working in corporate bodies or firms (art. 49 (5-6)), and for cases where multiple keys can be used to decrypt (art. 50 (4-7)); if the person required to decrypt no longer has the key, he must disclose all information that he does have to facilitate retrieval of the key (art. 50 (8-9)).

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
A person who knowingly fails to comply with the order is punishable with up to two years' imprisonment (art. 53 (1) and (5)). The provision on evidence and burden of proof in this penalisation are particularly complex. Someone is supposed to have the key if the prosecution shows that he had it at any time in the past, unless the suspect shows he no longer possesses it. The suspect can show this by raising an issue with respect to his ability to decrypt, but he also succeeds in exonerating himself if his ability to decrypt is not proved beyond a reasonable doubt (art. 53 (3)). The latter provision would suggest that there is no burden-of-proof reversal, but the earlier provision (that former possession of the key is sufficient evidence for current ability to decrypt) carries the impression of a burden-of-proof reversal. The Home Office, however, demystified that there is no reversal of the burden of proof.

If the suspects complies too late, he can put up a defence that he decrypted as soon as it was reasonably practicable to do so (art. 53 (4)).

Part III furthermore contains provisions on tipping-off (violation of a duty to keep secret is punishable with up to five years’ imprisonment) (art. 54), safeguards that the officials who order disclosure must take into account (art. 55), and definitions (art. 56).

On 10 July 2000, a Preliminary Draft Code of Practice on Investigation of electronic data protected by encryption etc was published, to provide guidance for public authorities on use of the decryption powers. In 2006, the Home Office held a consultation on a Draft Code of Practice for the Investigation of Protected Electronic Information covered by Part III of RIPA. The consultation closed on 13 September 2006. Parliament approved a revised Code of Practice, which came into force on 1 October 2007.

In R. v S and A, [2008] EWCA Crim 2177 (9 October 2008), the Court of Appeal ruled that an order to deliver encryption keys under art. 53 RIPA did not violate the privilege against self-incrimination. The lower court had argued that an encryption key does not fall under the privilege, as it exists independently from the suspect's will (refering to the ECtHR case of Saunders), or that if it did, it was legitimate and proportionate. The Court of Appeal noted that, even if the key exists independently of the will, it nevertheless may fall under the privilege against self-incrimination in that "the fact of the appellants' knowledge of the keys may itself become an incriminating fact" (§21), but only if the encrypted material is, indeed, incriminating (§24). Given RIPA's purpose, safeguards, and limitations, together with the fact that the trial judge can always exclude evidence like the defendant's incriminatory knowledge of the key, the Court of Appeal concludes that the privilege has not been violated in this case.

For more information, see the Home Office's RIPA information page as well as the RIP Information Center by the Foundation for Information Policy Research. Cf. a BBC story on a November 2007 application of the decryption order.

Electronic Communications Act 2000

Section 14 of the Electronic Communications Act 2000 (2000 Chapter c.7), which received Royal Assent on 25 May 2000, is entitled "prohibition of key escrow requirements". It determines that nothing in the Act shall confer any power on the government to "impose a requirement on any person to deposit a key for electronic data with another person." Subsection 2 contains two arcanely worded exceptions to this: requirements may be made to deposit a key with the intended recipient of data, and key recovery may be required for records "kept in pursuance of any provision made by or under any enactment or subordinate legislation".

The Electronic Communications Act also contained provisions for registration and requirements of cryptography service providers, in Chapter c.7, part I, but these never entered into force and were consequently repealed on 25 May 2005 due to the sunset clause of art. 16(4) of Chapter c.7.

History

1999 Electronic Communications Bill


Article 10 of the draft bill contained a power to require disclosure of a crypto key. For encrypted material lawfully obtained, a written notice can be given to a person who appears to be in the possession of the key, to provide the encrypted information in intelligible form (that is, in the condition in which it was before any encryption or similar process was applied to it), or, if the notice explicitly orders so, to disclose the key. A notice cannot require disclosure of keys intended only for authentication that have not in fact been used for other
(i.e., confidentiality) purposes. The notice needs to be authorized by the appropriate authority (depending on the powers under which the encrypted material was obtained), such as the Secretary of State, a judge, or a senior police officer. Failing to comply with such a notice is an offence punishable with up to five years’ imprisonment. It is a defence to show that you do not have the key, if you give sufficient information to enable possession of the key; likewise, it is a defence to show that it is not reasonably practicable to disclose the key, if you show that you provided it as soon as this was reasonably practicable.

If the notice to provide a key requires secrecy of the giving of the notice, of its contents and of the things done in pursuance of it, tipping off someone about this is punishable with up to five years’ imprisonment (with several defences, such as informing a legal adviser). Various safeguards were proposed to limit the use of the keys obtained through a notice. A Code of practice will be issued about the exercise of this power, and a Commissioner will be appointed to oversee the use of this power. The government also decided to establish a Technical Assistance Centre, which helps law enforcement, among others, in gaining access to decryption keys under proper authorization. Although key escrow was not contained in the draft bill, concerns were raised that a key-escrow requirement might feature in secondary legislation, as a condition for approval as a Registered Cryptography Service Provider. Eventually, a provision to prevent this was included in section 14 of the Act (see above).

Because of the many critical reactions to the crypto proposals, the decryption power provisions were lifted from the Electronic Communications Bill in November 1999, in order to be reinserted in the Regulation of Investigatory Powers Bill.

2000 Regulation of Investigatory Powers Bill
On 9 February 2000, the draft Regulation of Investigatory Powers Bill was presented to the House of Commons. Part III contains the decryption-power provisions that were lifted out of the draft Electronic Communications Bill (see above), with a few modifications. The new proposal adds proportionality and goal requirements (required to comply with the European Convention on Human Rights), stating that the decryption command must be necessary for national security, crime prevention or detection, or for the UK’s economic well-being, or must be likely to be of value for the exercise of a statutory power.

The penalisation of not complying with the decryption order is extended with the requirement that a person is guilty only if he has or has had possession of the decryption key. (As I read it, this means that the burden of proof lies with the Prosecutor to show that the addressee (at one time) possessed the key, while (presumably after this has been argued) the burden of proof to show inability to decrypt lies with the addressee.) The tipping-off offence is limited by adding that the police can only require secrecy if the police obtained the encrypted material at stake through a means that it is reasonable for law-enforcement to keep secret.

3. Developments to restrict cryptography

DTI 1996 paper
In June 1996, DTI announced a crypto policy in the Paper on Regulatory Intent Concerning Use of Encryption on Public Networks. According to this paper, the government intends to introduce legislation for licensing and regulating Trusted Third Parties (TTPs). These licensed TTPs would be required to release to the authorities the private encryption keys of clients under similar safeguards to those which already exist. The licensing policy would aim to preserve law-enforcement access, and so willingness to cooperate with law enforcement would likely be a requirement for TTPs to be licensed. The paper was welcomed by the House of Lords in its Agenda for Action (at 6.38).

The policy paper stated that the Government does not intend to regulate the private use of encryption (but rather corporate use) seemed to be contradicted at a 27 June 1996 meeting discussing the policy. The Department of Trade and Industry (DTI) confirmed at the meeting that escrowing of confidentiality keys would be mandatory. Fortune 500 companies, however, would be trusted to manage their own keys, because their concerns are supposed to be too high to risk not cooperating with law enforcement anyway.

This policy was already indicated at the OECD Meeting of December 1995, where the UK delegation said it approved a voluntary (private) Trusted Third Party scheme with judicial access to stored keys under a judicial warrant. The TTPs would probably need licenses to be able to provide digital signature services. It was realized that numerous questions, such as liability, remained yet unresolved.

Red Pike
A preview of the proposed key escrow legislation was also found in the proposal for the National Health Service to adopt a crypto system, Red Pike, with a key recovery scheme. The 1996 (?) booklet The Use of Encryption and Related Services with the NHSnet' was quoted by Julian Assange as: "HMG had, for a number of years, been developing its ideas for a national Public Key Management Infrastructure having what is known as Key Recovery (KR) facilities. HMG’s interest in Key Recovery is driven by its Law Enforcement needs. (...) It is expected that eventual national policy in these areas, supported by legislation, will involve the use of KR capabilities”.

Labour policy
In its 1995-1996 policy on the information superhighway, Communicating Britain’s Future, Labour stated it did not approve of escrowed encryption: "attempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks.” Labour wished authorities to have the power to demand decryption under judicial warrant. It seemed, then, that Labour intended to penalize a refusal to comply with a demand to decrypt under judicial warrant. (This might be an extension of the Police and Criminal Evidence Act 1984, according to which the power of seizure in...
certain cases includes the power to require any information contained in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible.) In 1998, however, Labour's policy document was removed from the World Wide Web, which could indicate that Labour had changed its mind in favor of the DTI policy (see below).

On 18 February 1998, the Annual General Meeting fo Scientists for Labour passed a resolution endorsing the Labour encryption policy of Communicating Britain's Future in reaction to rumours that the Labour government would back away from this and announce a restrictive policy in line with the DTI consultation paper.

**1997-1998 DTI consultation process**

The Department of Trade and Industry (DTI) launched a Consultation Paper on Licensing of Trusted Third Parties for the Provision of Encryption Services on 19 March 1997 for a two-month comment period. The paper follows the June 1996 paper on regulatory intent (see below), extending it from use of encryption on public networks to encryption use in general (including stored data). The general aim of the legislation would be to engender trust in TTP services. The processing of the consultation process took a long time; the resulting policy was announced in April 1998 (see below).

The proposed legislation would regulate the licensing by DTI of Trusted Third Parties (TTPs) that offer cryptographic services - Certification Authorities, Key Escrow Agencies, and other TTPs. All cryptographic services offered (by organizations, not by individuals) to the public and business fall under the regime (except for intra-company TTPs and except for encryption services which are an integral part of another service, such as pay-TV). Services offered from abroad also require a license, including services via the Internet (this would require TTPs that offer online crypto services available in the UK either to get a license or to take measures to not render the service to UK citizens, e.g., by including an exception in the advertisement). The offering of services without a license will be prohibited.

TTPs would be required to render escrowed private encryption keys under a lawful warrant issued by the Secretary of State, under safeguards broadly similar to current wiretap warrants. Only confidentiality keys have to be handed over, not signature keys (although the paper does not say how to distinguish between (dual-use) keys). Note that the paper involves key escrow (not key recovery by sending along accessible session keys), and that law enforcement would receive the private encryption key, not session keys; no explicit safeguards are mentioned to assure the agency will destroy the private key on expiry of the warrant. For legal access to keys stored with TTPs abroad, there will have to be agreements with other countries on the basis of dual legality. TTPs will be liable for the protection of the private keys, and there will be strict liability for TTPs for compromise or disclosure of private keys. The requirement for releasing private keys upon a lawful warrant only addresses licensed TTPs who are able to comply, i.e., Key Escrow Agencies, not Certification Authorities (CAs).

The paper confirmed that use of licensed TTPs is voluntary, and that there would be no restrictions on the use of cryptography. However, since users need CAs, and CAs fall under the licensing regime, it was not clear to what extent the government would allow a Public Key Infrastructure to be set up without requiring escrowing of private keys. If the licensing of CAs was restricted, there might be an effective regulation of encryption use after all. Moreover, the "Government recognises that further legislation may be required in the future to enable the appropriate authorities to obtain private encryption keys other than those held by licensed TTPs."

See a list with the responses to the DTI discussion paper, including Charles Lindsey's critique of the consultation paper. See also Yaman Akdeniz' page with more background on the UK policy and a critique by Cyber-Rights and Cyber-Liberties. The Summary of Responses on the consultation paper released by DTI in April 1998 showed that there were 260 responses, only a few of which approved the proposals without qualifications. The general idea of licensing TTPs was welcomed, but major concerns were raised over the mandatory nature of the licensing process, the linking of licensing to lawful access to keys, the nature of lawful access to keys as such, and the ineffectiveness of key escrow.

See also the general outline of British policy up to this point in chapter 6 of Bowden & Akdeniz' article Cryptography and Democracy: Dilemmas of Freedom.

**1998 policy announcement**

On 19 February 1998, a new policy announcement was expected to be made at the London ICX conference to follow up the DTI paper and the responses to it. It was expected to be largely similar to the DTI paper, but to refrain from linking certification of digital signature keys to mandatory deposits. However, the announcement was postponed. Nigel Hickson of DTI stated at the ICX conference that the likely timetable is a policy announcement "soon", consultation in the summer of 1998, and legislation in the 1998/9 parliamentary session.

The policy announcement was finally made on 27 April 1998 by Barbara Roche, Parliamentary Under Secretary of State at DTI, together with the publication of a Summary of Responses to the Consultation Paper. The policy follows the discussion paper, with some major changes to meet concerns raised in the consultation process. The licensing of TTPs will be voluntary, and so, crypto service providers are free to seek or refrain from licensing. There is also a better policy differentiation between digital signatures and confidentiality encryption. Thus, the policy distinguishes Certification Authorities from Key Recovery Agents. Organizations providing confidentiality encryption services (such as key recovery or key management services) are encouraged to seek licenses; licensed service providers will be required to make recovery of keys possible "through suitable storage arrangements", which indicates a key-escrow rather than a key-recovery technology (on this terminology, see my key recovery page). Legislation will be enacted to enable law-enforcement agencies to obtain a warrant for lawful access to encryption keys (which does not include keys used solely for digital signature purposes). The legislation to yield access to crypto keys will apply both to (licensed and unlicensed) crypto service providers holding keys and to crypto users. (The latter seems an implementation of the initial Labour policy intention to demand decryption under
judicial warrant.)

These policy principles were reiterated in Barbara Roche's speech at the International Commerce Exchange Conference of 19 October 1998. She announced then a consultation document detailing the thinking outlined in April. Among the details are the announcement that OFTEL will be the licensing authority for cryptographic services. The policy would be effected in an Electronic Commerce Bill "as soon as parliamentary time permits".

1999 consultation document

The consultation document "Building Confidence in Electronic Commerce" was published on 5 March 1999. It built upon the earlier proposals, with some changes. Confidentiality service providers are no longer obliged to provide key escrow or key recovery, although they are encouraged to do so. Legislation focuses on enabling the authorities to require plaintext or keys. Thus, the policy has three key elements:

1. Establish a power to require any person, upon service of a written notice, to produce plaintext or a decryption key (or password protecting a key). The ability to serve a written notice will be ancillary to powers for wiretapping or searching and seizing. This does not apply to encryption keys used solely for digital signatures. The power would apply to both providers and users, but it does not imply a requirement to store keys. According to the government, this power does not infringe the privilege against self-incrimination (but compare my FAQ on this issue). The government is considering how these provisions will apply to Scotland and Northern Ireland, where different wiretap and search laws apply. Safeguards would be introduced to protect delivered keys, as well as oversight and complaint mechanisms. To ensure compliance, the government would make it an offence not to comply with the terms of a written notice without reasonable excuse. Moreover, "tipping off" someone about an authorisation to demand encryption would also be penalized.

2. The use of key escrow and key recovery is encouraged. A TTP wanting to be licensed as a Key Recovery Agent must demonstrate that it can provide, electronically, key-recovery information to law enforcement when presented with the appropriate authority.

3. The government will "work with industry and other interested parties to find other ways of mitigating the effects" of crypto use by criminals.

Comments on the consultation document could be submitted until 1 April 1999 (sic). A summary of the 246 comments is available at DTI. The House of Commons Trade and Industry Select Committee published a report on 18 May 1999, stating, among others, their disappointment "that the Government should still hold a candle for key escrow and key recovery."

1999-2000 EC and RIP Bills, RIPA 2000

For the subsequent legislative history of the decryption power in the RIPA 2000, see under 2.

Back to the Table of Contents

United States of America [Sources 1, 2, 4, 5, 7]

1. Export/ import controls

Import

There are no import restrictions on cryptography.

Export

The US has signed the Wassenaar Arrangement, but does not implement the (pre-December 1998) General Software Note and generally maintains stricter controls.

Export Administration Regulations (EAR)

Cryptography export used to be controlled by the International Traffic in Arms Regulation (ITAR). At the end of 1996, cryptography export was transferred to the Export Administration Regulations (EAR) of the Department of Commerce, 15 C.F.R. Parts 730-774 (see in particular sections 740.13, 740.17 and 742.15). The export policy was relaxed to favor export of data-recovery cryptography. This initiative was announced in a statement by the Vice President of 1 October 1996, and further elaborated in a November 15, 1996 executive order and memorandum, and in the Commerce Department draft EAR of December 30, 1996. The Department of Justice is now included in crypto export decisions. (Incidentally, the Commerce Department has "borrowed" three export control and crypto specialists from the FBI and NSA to help process license applications.)

Making available cryptography on the Internet or a BBS is considered export, unless appropriate measures are
taken to prevent foreigners from accessing the cryptography.

The export rules distinguish between five categories of "encryption items" (EI).

1. Certain mass-market encryption software may be released from EI controls after a one-time review.
2. "Data recovery" crypto (meaning that government can access keys or plaintext with a lawful warrant) will be eligible for an export license to non-embargoed countries. The procedures for data-recovery licenses were simplified in September 1998, when also "recoverable products" were released for export (a recoverable product means that an operator can access plaintext without the user noticing).
3. After a one-time review, (up to) 56-bit cryptography can be granted a six-month export license, provided the exporting business commits itself to incorporating a data recovery feature in its products within the next two years. This provision was changed in December 1998, when all 56-bit crypto was released for export after a one-time review, with no requirement of data recovery.
4. All other encryption items may be eligible for encryption licensing arrangements; items not authorized under a licensing arrangement will be considered on a case-by-case basis.
5. Encryption "technology" may be licensed for export on a case-by-case basis.

In August 1997, a 25 July interagency draft Encryption Items Rule modifying the EAR was published on the Internet, although the Department of Commerce declined to check its authenticity. It would implement the government's key recovery policy, and clarify several issues, e.g., that electronic export to Canada is not controlled, the personal-use exemption (see below), that support documentation is not required for exports of technology or software (and removing this requirement for export to most Eastern European countries), and that export of non-key recovery financial-specific cryptography is allowed if it can be design only be used for financial applications. The regulation would also require Web server operators that allow people to download encryption software to seek an advisory opinion from the Bureau of Export Affairs. See also an article by Peter Wayner on the draft.

The Bureau of Export Administration (BXA) (now: Bureau of Industry and Security, BIS) has reviewed the export controls to determine whether they should be modified, rescinded or extended. On 8 October 1997, it released a statement "seeking comments on how existing foreign policy-based export controls have affected exporters and the general public." On 15 January 1998, it published an interim rule revising the Commerce Control List, necessary to implement the (pre-December 1998) Wassenaar Arrangement. The interim rule also imposed new reporting requirements on persons that export certain items to non-Wassenaar countries.

Two major reviews of the export controls were announced in July and in September 1998 by BXA. The 7 July announcement, which was implemented in an interim rule of 22 September 1998, introduced a licensing policy for banks and financial institutions (notably, brokers, credit-card companies, and securities firms). Non-voice crypto products can be exported by banks and financial institutions after a one-time review, with no data-recovery requirement, to 45 countries (members of the Financial Action Task Force or countries that have money-laundering laws) (Anguilla, Antigua, Argentina, Aruba, Australia, Austria, the Bahamas, Belgium, Barbados, Brazil, Canada, Croatia, Denmark, Dominicana, Ecuador, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Italy, Japan, Kenya, Luxembourg, Monaco, the Netherlands, New Zealand, Norway, Poland, Portugal, St. Vincent and the Grenadines, St. Kitts and Nevis, Seychelles, Singapore, Spain, Sweden, Switzerland, Trinidad and Tobago, Turkey, the UK, the US, and Uruguay). To other countries, their export-license applications will be viewed with a "presumption of approval".

On 16 September 1998, a major relaxation of export controls was announced, which was implemented in a 31 December 1998 interim rule. This entailed the following.

- All crypto products of up-to 56 bits are released for export after a one-time review, except to the (currently seven as defined by the US) terrorist countries. This includes DES, 56-bit RC-2/4/5, 56-bit CAST. Also, asymmetric crypto of up to 1024 bits is released for export. For export to military or government end-users, semi-annual post-facto reporting is required.
- Export to subsidiaries of US companies is permitted (except to those located in the seven terrorist countries) under license exception. For export to strategic partners, "favorable treatment" under license will be extended.
- Export to health, medical, and insurance companies (in the strict sense) is permitted to the same 45 countries as export by banks and financial institutions is allowed (see above). Biochemical and pharmaceutical producers excluded from this permission.
- Export to online merchants is allowed, under license exception, for "export of client-server applications (e.g., SSL) and applications tailored to on-line transactions" to online merchants located in the 45 countries of the bank list (see above). The export is "limited to those that facilitate secure electronic transactions between merchants and their customers." Export to other countries receive a policy of approval under export licensing arrangements.
- "Recoverable" products (which allow recovery of the plaintext without assistance or knowledge of the end
user) can be exported to foreign commercial firms for internal company proprietary use only, located in most of the 45 countries listed above, with a semi-annual post-export reporting requirement of end users.

- For exporting key-recovery products, the review of foreign key-recovery agents is eliminated.

After the President's Export Council Subcommittee on Encryption advised in "Liberalization 2000" to ease the export controls, the government announced further relaxation of export controls on 16 September 1999. (At the same time as this announcement, the government announced the Cyberspace Electronic Security Act (CESA) 1999 to meet the perceived effects of the export changes on law enforcement and national security.) The changes were to be implemented by 15 December 1999, but were subsequently postponed. The new regulations were finally published on 12 January 2000 (the press release is less specific but much more readable). The major components of the updated policy are the following.

- Any crypto of any key length can be exported under a license exception, after a technical review, to non-government end users in any country except the seven "terrorist countries". Exports to governments can be approved under a license.
- Retail crypto (i.e., crypto which does not require substantial support and is sold in tangible form through retail outlets, or which has been specifically designed for individual consumer use) of any key length can, after a technical review, be exported to any recipient in non-terrorist countries.
- Unrestricted crypto source code (like most "open source" software) and publicly available commercial source code (like "community source" code) can be exported to any end-user under a license exception without a technical review. BXA (BIS) must be given a copy or the URL of the source code. All other source code can be exported under license exception after a technical review to any non-government end-user. One may not, however, knowingly export source code to a terrorist country, although source code may be posted on the WWW for downloading without the poster having to check whether it is downloaded from a terrorist country.
- Any crypto can be (re)exported to foreign subsidiaries of US firms without a technical review. Foreign nationals working in the US no longer require an export license to work for US firms on encryption.
- The regulations implement the December 1998 Wassenaar changes (notably, export of 56-bits and 64-bits (for mass-market products) crypto to non-terrorist countries).
- Post-export reporting is required for exporting certain products above 64 bits to non-US entities.

Since 19 October 2000, a further liberalization of export controls is effective, triggered by changes in the EU export regulations (see the Federal Register Vol. 65, No. 203, pp. 62600-10). The liberalization was announced on 17 July 2000. A license exception is introduced for export of any crypto product to any end user (so, the distinction between government and non-government end users is dropped) in the 15 EU countries, Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, and Switzerland. Also, US exporters can ship products immediately after filing a commodity classification request, without waiting for the technical-review results or the previously used 30-day delay period.

On 6 June 2002, a further liberalization was published (Federal Register Vol. 67, No. 109, p. 38855). Mass-market crypto with key length exceeding 64 bits can now be exported after a 30-day review by the Bureau of Industry and Security (BIS) (without having to report after export, and without national-security review). To EU countries and the 8 other countries (Australia, Czech Republic, Hungary, Japan, New Zealand, Norway, Poland, Switzerland), mass-market crypto can be exported immediately after the review request has been registered with BIS. Publicly available source code can be exported to most destinations after notification. The rule also clarifies that no review or notification is required for export to US companies and subsidiaries for internal company use; for products with short-range wireless encryption; and for items with limited encryption use.

See the fact sheet of the rule at BIS.

On 9 December 2004, BIS published a further 'streamlining' of export procedures. A uniform 30-day review period was now implemented for most encryption items that need review. Moreover, the 'license-free zone' to which mass-market crypto can be exported immediately after a review request has been registered, was expanded with the new EU member states (effectively adding Cyprus, Estonia, Latvia, Lithuania, Malta, Slovakia, and Slovenia). The word 'retail', which caused confusion because it was used beside 'mass-market', was deleted from the regulations. 'Publicly-available' crypto software placed on the Internet under the relevant notification procedures can be modified without additional notification, provided it remains at the same URL. Finally, procedures for beta-test software and procedures for increasing key lengths of previously reviewed and authorized products have

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
been simplified.
See the fact sheet of the 9 December 2004 rule at BIS.

**Terrorist countries**
The "terrorist countries" are: Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria.

See BIS' Wassenaar and BIS' encryption page. See also the encryption excerpts of BXA's 1997 Annual Report.

**Personal-use exemption**
In February 1996, the ITAR rules were amended as regards personal use of cryptography. Temporary export of products for personal use was exempted from the need of a license, provided the exporter take normal precautions to ensure the security of the product, including locking the product in a hotel room or safe. The product must not be intended for copying, demonstration, marketing, sale, re-export, or transfer of ownership or control. In transit, the product must remain with the exporter's accompanying baggage. The exporter must keep records of each export for five years. Export to embargoed countries (e.g., Cuba, Libya, Syria) is prohibited.

Under the new EAR, the ITAR personal use exemption is replaced by license exception TMP and BAG (see the EAR at 15 CFR 740.4 and at 740.14 and the original ITAR version). The Department of Commerce announced in February 1997 it would revise the new regulations to, among others, clarify the personal use exemption for laptop computers.

**Export Administration Act**
The Export Administration Act expired in August 1994, but it was extended by Executive Order 12924 by the president with the authority under the International Emergency Economic Powers Act (50 USC 1701ff). The president most recently extended the state of emergency in an order of 10 August 1999. On 9 August 1999, Senators Gramm and Enzi published a draft Export Administration Act of 1999 to reauthorize the EEA, which would maintain controls, except for items easily available abroad.

Michael Froomkin (in It came from Planet Clipper) argues that the government has no authority to steer industrial crypto policy through export regulation, and that the subsequent orders to extend the EAA can hardly be justified with a reference to a state of emergency this long.

**Export case law**

- In August 2001, two men were arrested and accused of attempting to illegally export encryption devices to China (news report).
- In February 2002, the Commerce Department fined a San Diego firm $95,000 for illegally exporting 128-bit encryption software to South Korea (news report).

**Export Council Subcommittee**
In April 1997, the President's Export Council Subcommittee on Encryption was established to advise the Secretary for Export Administration on the implementation of crypto export policy; it consists of approximately 25 members from the exporting community and government agencies.

**ITAR**
The International Traffic in Arms Regulation (ITAR) restricted export of "dual-use" cryptography (that is, cryptography that can serve both civilian and military purposes) by placing it on the Munitions List. For (relatively strong) products that can encipher information, an export license was usually issued only for use by foreign branches of American enterprises and for use by financial institutions.

"Weak" cryptography (e.g., with a certain maximum key-length) could also be exported.

Export of cryptography that served only authentication or integrity purposes was already ruled by the Export Administration Regulations. Some types of public-domain software were decontrolled and on the Commerce Control List.

In 1995, the Administration proposed a mitigation of the export controls. Cryptography using keys up to 64 bits (as opposed to the current maximum of 40 bits) would be exportable, provided it implements key-escrow. Criteria for exportable cryptography were discussed at two meetings in September and December 1995; criteria for the escrow agents were handed out at the December meeting.

Back to the Table of Contents

**Initiatives to relax export controls**
Several initiatives, as yet unsuccessful, have been taken, both in Congress and by the public, to try to mitigate the
Karn, Bernstein, and Junger cases
A federal district court in Washington, DC, on March 22, 1996 rejected the claims of Phil Karn, stating that the case presented a political question for the two elected branches to decide. It held that the export restrictions did not violate the First Amendment. The defense appealed; on 6 November 1996, the Department of Justice filed a brief on appeal. On 21 January 1997, the appeal court remanded the case to the district court in light of the transfer of the export controls to the Department of Commerce; it did not reach the constitutional issues. In August 1997, the Department of Commerce ruled that certain programs Karn sought to export were controlled by the EAR and subject to prior licensing. Karn challenged this classification in a law suit against the DoC; in March 1998, the government moved to dismiss this law suit. On 18 February 1999, the D.C. District Court granted Karn's request for discovery and an evidentiary hearing. However, following the January 2000 revisions of the export regulations, which effectively made publicly available source code freely exportable, Karn allowed his case to be dismissed as moot. See more information on this case.

Contrary to the 1996 Karn decision, a Northern California district court, in a December 18, 1996 decision in the case of Daniel Bernstein, who sought the ability to export his encryption algorithm, judged the export regulations to be too restrictive. The district judge found the licensing system an unconstitutional prior restraint on free speech - having ruled earlier that crypto source code was protected by the First Amendment (see the decision of April 15, 1996, in which she denied the government's motion to dismiss the case). The judge called the licensing system a "paradigm of standardless discretion", given its lack of decision time limits, of standards for denial and of appeal provisions. The ruling does not relate to object code. On December 30, 1996, Bernstein's lawyers asked the government to delay enforcement of the new export rules until they are reviewed for constitutionality. On 25 August 1997, the federal district court affirmed its earlier decision, declaring that the Export Administration Regulations and all rules promulgated thereunder insofar as they apply to cryptography are in violation of the First Amendment on the grounds of prior restraint and are, therefore, unconstitutional. The judge enjoined the government from further enforcement of the regulations, including prosecution of "anyone who uses, discusses or publishes or seeks to use, discuss or publish [Bernstein's] encryption program and related materials." The government, on 28 August 1997, requested a stay of the Court's order pending appeal, which was granted for the most part; Bernstein could, however, publish his program on the Internet after 8 September. See the decision of August 25, 1997.

On 6 May 1999, the Court of Appeals for the Ninth Circuit held (two to one) that the EAR are an unconstitutional prior restraint on free speech in violation of the First Amendment, arguing that source code is expressive speech entitled to First Amendment protection. Judge Nelson dissented. The government filed a motion for reconsideration on 21 June 1999, which was granted on 30 September. An 11-judge "en banc" panel of the Court was to re-examine the case on 21 March 2000, but, as requested by Bernstein on 3 March, the Court of Appeals on 12 April remanded the case back to the district court for reconsideration in light of the January 2000 revisions of the export regulations. Eventually, however, due to repeated assurances by the DoJ attorney Coppolino that the government would not enforce several portions of the regulations, the case was dismissed. So, in October 2003, Bernstein announced that the case had come to an end (for now). See the Bernstein archive.

In August 1996, law professor Peter Junger filed suit to challenge the ITAR regulations, saying they restricted his ability to teach a cryptography course, as foreign students are attending his classes; he wants to publish his class materials on the WWW server. Following the Bernstein decision (see above), Junger filed an amended complaint against the EAR regulations. On 2 July 1998, in Junger v. Daley (N.D. Ohio, 1:96-CV-1723), the US District Court for the Northern District Court of Ohio dismissed Junger's claim, arguing that encryption source code is not sufficiently expressive to merit First Amendment protection. Therefore, crypto export is not protected conduct under the First Amendment, and export regulation passes constitutional muster. On appeal, this decision was reversed. In Junger v. Daley, 2000 FED App. 0117P (6th Cir.) of 4 April 2000, the Court of Appeals for the Sixth Circuit stated that computer source code merits First Amendment protection, since it is a means of expression among cryptographers: "for individuals fluent in a computer programming language, source code is the most efficient and precise means by which to communicate ideas about cryptography". Thus, the case was remanded to the District Court to further consider the crypto export regulations (as revised in January 2000) under the Constitution.

See various documents in this case, and another page.
Congress Bills

Three bills were proposed in 1996 to ease export controls. Senator Leahy's bill, proposed on 5 March 1996, the Encrypted Communications Privacy Act (S. 1587), reintroduced 27 February 1997 (S. 376), would, among others, relax export controls, allowing generally available or public-domain crypto to be exported. At the same time, Representative Goodlatte introduced a similar bill, Security And Freedom through Encryption (SAFE) Act of 1996 (H.R. 3011), reintroduced on 12 February 1997 (H.R. 695). On 30 April 1997, the House Subcommittee on Courts and Intellectual Property unanimously approved the SAFE bill. On 14 May 1997, the House Judiciary Committee also unanimously approved the SAFE bill, after adopting three amendments (one to the criminal provision (ensuring that it only criminalizes crypto use with the intention to cover up a federal felony), one to correct a technical oversight, and one to direct the Attorney General to compile and maintain data on the instances in which cryptography hampered the investigation). On 24 June 1997, the House International Relations Subcommittee on International Economic Policy and Trade approved the SAFE act. The House International Relations Committee approved the bill on 22 July 1997, rejecting an amendment to reinstate strict controls if relaxation would turn out to harm national security. The House National Security Committee radically amended the Bill to include the Secretary of Defense in export decisions (Weldon/Dellums amendment), whereas the House Permanent Select Committee on Intelligence replaced the language of the bill with domestic controls (see below) as well as strengthening export controls (Goss/ Dicks amendment). The House Commerce Committee, on 25 September 1997, rejected an amendment by Oxley/Manton to strengthen export controls, and adopted a version by Markey and White to remove export controls. Given the many conflicting versions of the bill, the SAFE Act was not put to a vote, especially since the chair of the House Rules Committee, Solomon, stated to only move the Act to the floor if it contains (Oxley/Manton) mandatory key escrow. (See below on the re-introduced bill.)


The Kerrey-McCain bill, Secure Public Networks Act (see below), introduced June 1997, would allow export of 56-bit non-key recovery cryptography under a license. Key recovery cryptography would be exportable regardless of key length, under a license. An unofficial draft amendment circulating in the government by August 1997 would somewhat relax the export provisions of the bill (export of crypto with a recovery feature, regardless whether it is activated, would be granted; an Advisory Board would recommend to the President whether larger than 56-bit crypto could be decontrolled; and the power to prohibit any exports "contrary to US security interests" would be dropped). On 4 March 1998, the senators announced a new, largely similar, version of their bill.

The Computer Security Enhancement Act of 1997 (HR 1903) would require the Commerce Department, upon request, to take into account the foreign availability of comparable crypto in deciding the export of crypto products. The Act was cleared in the House on 16 September 1997.

On 12 May 1998, senators Ashcroft and Leahy introduced the E-PRIVACY Act ("Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace"). This would relax export controls, lifting the restrictions for exporting generally available crypto products after a one-time review by the Secretary of Commerce; this also valid for products if a like product of similar strength is commercially available outside the US from a foreign supplier, which is to be determined by an Encryption Export Advisory Board. The same holds for "interface mechanisms for interaction with other encryption products" which do not themselves provide encryption capabilities. For other crypto, an export advisory board would make recommendations on its exportability.

On 25 February 1999, Rep. Goodlatte reintroduced the Security And Freedom through Encryption Act (SAFE) (H.R. 850). The bill would limit export license requirements for generally-available or public-domain cryptography to a one-time, 15-day technical review. Export would be allowed for more specialized products to the 45 countries on the "financial export" list (see above) or if a similar product is available abroad without export restrictions. The SAFE Act was approved by the Commerce Committee on 23 June 1999 (with amendments) and by the International Relations Committee on 13 July 1999 (with amendments tightening certain provisions). The Permanent Select Committee on Intelligence amended and approved the bill on 15 July; the amendments will be viewed as suggestions only, since the Committee has no jurisdiction over the bill. The Armed Services Committee substantially amended and approved the bill on 21 July 1999; an amendment would permit the president, unsubjected to judicial review, to block export if it is contrary to national-security interests. Subsequently, the bill went to the Rules Committee to reconcile the competing versions into one that will be presented to the full House.

On 14 April 1999, Sen. McCain introduced the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999 (S. 798). This bill would allow unlimited crypto export to member states of...
NATO, OECD, and ASEAN, and limit export to other countries to 64-bit key-length crypto. An Encryption Export Advisory Board would periodically research foreign availability of cryptography and advise amendments accordingly. The Bill passed the Commerce, Science, and Transportation Committee on 23 June 1999.

On 9 August 1999, Senators Gramm and Enzi published a draft Export Administration Act of 1999 to reauthorize the EEA, which would maintain controls, except for items easily available abroad and mass-market items. On 27 July 1999, as an alternative to the SAFE Act, Rep. Goss introduced the Encryption for National Interests Act (H.R. 2616), which would, among others, remove key recovery as a factor in any export controls, and allow exports of up to 64-bit symmetric crypto (level to be increased every six months).

See for more information the Pro-crypto Legislation Archive.

On 5 September 1997, the California legislature passed a resolution asking for a revision of federal crypto export controls, supporting the proposed SAFE Act (the original version, see above).

Reports
The Department of Commerce recommended easing export controls after a joint study with the National Security Agency found that the export restrictions harm US business.

In June 1996, the National Research Council released its long-awaited study on cryptography policy. It recommended that export controls be progressively relaxed, but not eliminated. Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable; for today, this would mean allowing export of 56-bit symmetric encryption products. Export of stronger cryptography (i.e., today, using more than 56 bits) should be exportable on an expedited basis to a list of approved companies if the proposed user agrees to provide the US government access to decoded information.

According to a draft paper Enabling Privacy, Commerce, Security and Public Safety in the GII, the government is working toward a policy that will readily license export of key-escrow systems, once the needed infrastructure and government-to-government agreements are in place.

More information
See for more information and links the Cryptography Export Control Archives and John Young's Arms Control Essays.

2. Domestic laws and regulations

DMCA
The Digital Millennium Copyright Act (Public Law 105-304, H.R. 2281, also called WIPO Copyright Treaties Implementation Act) was approved on 12 October 1998 by the House and signed by the President on 29 October 1998. It creates penalties for circumventing copyright-protection systems. Although limited exceptions for circumventing such systems for the purposes of cryptography research were included in the Act, cryptographers were still concerned that crypto research and the development of cryptanalytic tools would be hindered. (Compare EPIC's testimony.) The Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works of the Copyright Office, effective from 28 October 2000 until 28 October 2003, contains two exemptions (related to filtering and malfunctioning software). Compare EFF's archive of DMCA cases.

Case law
In the case of United States v. Scarfo, the US District Court for the District of New Jersey held on 26 December 2001 that the federal wiretapping law and the Fourth Amendment allow the use of a "key logger" that intercepts a passphrase to an encrypted file, provided that the system does not operate while the computer is communicating with other computers. Because of a plea agreement, there will be no appeal in this case. See EPIC's Scarfo page.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM 2009-02-02
In the case of *United States v. Boucher*, 2007 WL 4246473 (29 November 2007), the District Court for the District of Vermont held that a password that protects encrypted files falls under the Fifth Amendment (the privilege against self-incrimination). Boucher was subpoenaed by a grand jury to give the password. The court held that a defendant cannot be compelled to give the password, since it exists in the suspect's mind and handing it over would provide testimonial evidence, in particular, the fact that the suspect knows the password and has control over the encrypted files. Cf. Susan Brenner's blog post.

### 3. Developments to restrict cryptography

**Escrowed Encryption Standard (Clipper)**

In 1993, the Clinton Administration announced the Escrowed Encryption Initiative (EEI), usually referred to as the Clipper Initiative, after its first implementation in the Clipper chip. A classified, secret-key algorithm, SKIPJACK, has been implemented in an Escrowed Encryption Standard (EES). The reported basic idea of the EEI is to provide citizens with a safe cryptosystem for securing their communications without threatening law enforcement. The EES procures law enforcement access by means of a Law Enforcement Access Field (LEAF) that is transmitted along with each encrypted message; the field contains information identifying the chip used. Law enforcement agencies wire-tapping communications encrypted with EES can decipher tapped messages by obtaining the two parts of the chip's master key that are deposited with two escrow agencies (National Institute of Standards and Technology and the Treasury Department's Automated Systems Division), provided they have a court order for the tapping.

Following criticisms on the choice of escrow agents, the government came up with commercial key escrow ("Clipper II"), a scheme in which the escrow agents can be independent organizations chosen by cryptography users.

The EES is a voluntary standard to be used in telephone communications. Privacy advocates fear that the government may declare escrowed encryption obligatory once it has captured a sufficient portion of the market. The EES has been generally rejected, though.

In March 1997, the Department of Defense announced that the NSA, developer of the Fortezza card (implementing the key-escrow system of the EES), would no longer implement the EES; instead, it would work to adopt key recovery as promoted by the US government (see below).

#### Key Management Infrastructure

In its May 1996 draft paper *Enabling Privacy, Commerce, Security and Public Safety in the GII* (referred to by opponents as Clipper III), the government proposes the establishment of a key management infrastructure (KMI) that incorporates key escrow. Participation in the KMI would be voluntary, and choice of encryption algorithms would be free. A Policy Approving Authority would certify Certification Authorities (CAs); it would also be responsible for setting CA performance criteria to meet law enforcement's needs. Users should escrow keys with an Escrow Authority (either the CA or an independent EA) before they can get a public-key certificate. Self-escrow is considered an acceptable option, if the corporate CAs can meet necessary performance requirements, including independence from the rest of the organization and handing over keys to law enforcement.

On December 5-6, 1996, a Technical Advisory Committee (website no longer available) to Develop a Federal Information Processing Standard (FIPS) for the Federal KMI held its first meeting. A report of the meeting expressed doubt on the viability of the process, due to the difference of opinion between business and government on the need for a key-recovery standard. Various subsequent meetings were held in 1997 and 1998. In mid-1998, the Committee announced it could not reach an agreement on a final FIPS recommendation. The charter of the TACDFIPSFKMI was renewed in August 1998 to continue work on the requirements for key-recovery products. It released a report on proposed key-recovery standards, for which comments could be submitted until 4 November 1999 (website no longer available).

#### Broad Encryption Policy

The 1 October 1996 statement by the Vice President, covering export controls, also refers to domestic crypto use. The temporary relaxation of export controls is part of a broader encryption policy, which claims to be broadly consistent with the NRC recommendations. Domestic use of key-escrow cryptography will be voluntary, and the choice of an encryption system remains free. The government will, however, promote key-escrow cryptography.
by expanding the purchase of key-escrow products for itself, promoting key-escrow cryptography in international discussions, and stimulating the development of innovative key-escrow products and services. The Administration will also seek legislation to facilitate commercial key-escrow, including liability issues for releasing keys.

**Crypto Ambassador**

On November 15, 1996, the government appointed ambassador Aaron as "special envoy for cryptography". He will promote international cooperation and coordinate US contacts with foreign governments on encryption matters. On 18 June 1997, the Electronic Privacy Information Center (EPIC) filed a lawsuit to seek public disclosure of the travel records of ambassador Aaron. EPIC acquired the travel records in January 1998.

**Annual report on criminal crypto use**

A 2 October 1996 law (HR 3723) includes an amendment requiring the US Sentencing Commission to report annually on the use of computer encryption to conceal criminal activity. Likewise, by law S. 1769 signed on 2 May 2000, section 2519(2) (b) (iv) of title 18 U.S.C. requires the Department of Justice to generally report on law-enforcement encounters with encrypted communications in the execution of wiretap orders. The President's Statement specifies that only general aggregate data on the total number of crypto encounters will be provided.

**Draft Key Recovery Legislation**

At the end of March 1997, a Draft Key Recovery Legislation dating from 12 March was published: the "Electronic Data Security Act of 1997". The Act would promote a Public Key Infrastructure with key recovery by registering (private or (foreign) government) Certification Authorities (CAs) and (private or government) Key Recovery Agencies (KRAs). A registered CA may only issue a public key certificate if the user provides a registered KRA with sufficient information to allow timely plaintext recovery by law-enforcement or national security. KRAs - both registered and unregistered - shall disclose recovery information to government agents with a warrant or upon receipt of a written authorization by the Attorney General. After complaints that use of a written authorization without judicial review could violate the Fourth Amendment, in May 1997, the government amended the draft law to clarify that the same legal criteria would apply for disclosing recovery information as for wiretapping. The facts of release of recovery information to government agencies may not be disclosed. Those who intentionally undermine certain provision of the Act (such as issuing public key certificates to persons while knowing they do have not provided sufficient information to a KRA) are subject to civil penalties; the penalties are limited for registered CAs and KRAs. Such activities are also criminally punishable with up to five years' imprisonment. Likewise, the use of encryption in furtherance of the commission of a criminal offense can be punished with six months' to five years' imprisonment (having used key recovery which is reasonably available to the government is an affirmative defense). People packaging encryption products must label them to inform the user whether the product uses registered KRAs. Finally, the President shall conduct negotiations with other countries on the mutual recognition of registered KRAs. The draft legislation affirms that use of any encryption shall be lawful except as provided in the Act or other law (which currently means any encryption use is lawful except in furtherance of a crime), and that use of the key recovery infrastructure is voluntary. The government is no longer seeking a sponsor for the draft bill.

The government's Framework for Global Electronic Commerce restates the (voluntary) key recovery approach. In a 4 March 1998 letter to Senatory Daschle, Vice-President Gore reiterated the government's commitment to encouraging voluntary key recovery; it reaffirmed that the administration will not pursue mandatory key recovery. Rather, the government will pursue a dialogue between industry and law enforcement.

**Cyberspace Electronic Security Act of 1999**

On 16 September 1999, together with the announcement of export relaxation, the government proposed a draft Cyberspace Electronic Security Act of 1999. This contains provisions on law enforcement accessing crypto keys stored with third parties, but there is no requirement for users to use key-recovery crypto. The FBI's Technical Support Center will be given $80 million over four years, to help law enforcement "in responding to the increasing use of encryption by criminals". Moreover, to ensure "that sensitive investigative techniques and industry trade secrets remain useful", there will be protections "from unnecessary disclosure in litigation and criminal trials involving encryption", which indicates that the prosecution should not have to detail how they obtained decrypted information; such protection should, however, be consistent with fully protecting defendants' rights to a fair trial.

An earlier version of this bill suggested the power to alter "hardware or software that allows plaintext to be obtained even if attempts were made to protect it through encryption", effectively allowing the government to perform secret break-ins and alterations in
computers. This was not reiterated in the final draft.

**Domestic Security Enhancement Act 2003 (Patriot II)**
A draft Domestic Security Enhancement Act 2003 (Patriot II) of 9 January 2003 leaked out in February 2003 (see the text, also in pdf). Section 404 would criminalize the knowing and wilful use of crypto to conceal a federal crime, with a punishment of up to 5 years for first offenses or 10 years for second or subsequent offenses. The explanatory report suggests that these "additional penalties are warranted to deter the use of encryption technology to conceal criminal activity". The bill has not been submitted to Congress.

**Congress bills**
On 16 June 1997, Senators Kerrey, McCain, and Hollings introduced a bill largely similar to the government draft key-recovery legislation, the Secure Public Networks Act (S. 909). It has similar provisions on registration of CAs and KRAs, on criminalization of encryption in furtherance of a criminal offense, on release of recovery information (under broader conditions than the June amendment to the government bill), on international negotiations, and on the voluntary nature of the infrastructure. Additionally, it would require government use and government funding of encryption products to be based on key recovery crypto, establish an Information Security Board, and provide a waiver authority for the president in cases affecting national security. The bill was approved by the Senate Commerce Committee on 19 June 1997, including several amendments. See more information on the bill by CDT.

An unofficial proposed amendment to the Secure Public Networks Act, circulating in the government by the end of August 1997, would prohibit the manufacture, distribution, sale or import of non-key recovery cryptography (not its use or possession). The draft amendment contains several other changes, e.g., dropping the requirement for CA registration that the CA ensures recovery information to have been escrowed. In a 3 September 1997 Senate subcommittee hearing, FBI Director Freeh backed this draft legislation, but saying that key recovery should be mandatory, not voluntary; Commerce Undersecretary Reinsch commented that this was not the administration's policy. According to Jim Bidzos, President Clinton at a private dinner in September 1997 also stated not to support the domestic encryption controls being considered in Congress. In February 1998, Kerrey and McCain were said to circulate a somewhat revised version of their bill, requiring a court order for law enforcement access, and dropping the link between digital-signature-key certification and key recovery. On 4 March 1998, the senators announced a new version of the bill, which retains the establishment of an advisory board to decide upon easing export restrictions; in the new version, the board would consist of eight industry and four government representatives.

Goodlatte's SAFE Act (see above), aimed at relaxing export controls, was substantially amended by the House Permanent Select Committee on Intelligence, effectively imposing mandatory key escrow (the Goss/Dicks amendment). The House Commerce Committee, on 25 September 1997, rejected a similar amendment (Oxley/Manton); instead, it adopted an amendment by Markey and White to create a National Electronic Technologies (NET) Center, a federal information clearinghouse on encryption, which is to assist law enforcement by examining techniques to facilitate the efficient access to plaintext. Also, the amendment doubled the penalty for using encryption in furtherance of a felony. Goodlatte's prohibition of mandatory key escrow was maintained by the Commerce Committee. The SAFE did not make it to a vote in the House, given the many competing versions, and given that the chair of the House Rules Committee, Solomon, had declared to only move the Act to the floor if it contained a mandatory key escrow provision. The SAFE act was reintroduced in 1999, see below.

The Leahy bill (see above) would penalize the use of encryption in furtherance to a felony, if the encryption is intended to obstruct investigation. It creates a framework for key escrow agents, including strict requirements for law enforcement access; anyone is free to use non-escrowed cryptography. On June 27, 1995, Senator Grassley introduced the Anti-Electronic Racketeering Act (S.974), which, if enacted, would virtually ban encryption. Only the use of escrow-like software would be an affirmative defense for those prosecuted for using cryptography. The bill doesn't seem to have much support at present.

The E-PRIVACY Act of Ashcroft and Leahy, introduced on 12 May 1998, would also penalize using cryptography to conceal incriminating information in the commission of a federal felony with 5-10 years' imprisonment. Like the Markey/White amendment to the SAFE act (see section above), the bill would create a NET Center to assist law enforcement. The bill would prohibit the government from mandating key escrow or key recovery.

http://rechten.uvt.nl/koops/cryptolaw/CLS2.HTM
On 25 February 1999, Rep. Goodlatte reintroduced the Security And Freedom through Encryption Act (SAFE) (H.R. 850) (see above for Congressional developments). SAFE would safeguard everyone's right to use cryptography, prohibit the government from mandating key recovery, and it would penalize crypto use to conceal criminal conduct. The Commerce Committee, on 23 June 1999, amended the act, making it a crime not to comply with a decryption order, with penalties of up to ten years. The Permanent Select Committee (which does not have jurisdiction over the bill), on 15 July 1999, added a provision to permit law enforcement to gain access to decryption information with a warrant.

On 14 April 1999, Sen. McCain introduced the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999 (S. 798) (see above for Congressional developments). The bill prohibits the government from mandating key recovery. It does not contain a provision to criminalize the use of crypto to cover up a crime.

On 27 July 1999, Rep. Goss introduced the Tax Relief for Responsible Encryption Act of 1999 (H.R. 2617), which would offer a 15% tax credit for the costs of developing and producing recoverable cryptography (i.e., systems which can provide the government with plaintext without the user's knowledge). Also on 27 July 1999, as an alternative to the SAFE Act, Rep. Goss introduced the Encryption for National Interests Act (H.R. 2616), which would, among others, allow domestic use of all crypto, not mandate key recovery, and require a court warrant for accessing encrypted data or communications.

See the EFF Privacy, Security, Crypto, Surveillance Archive and the EPIC Key Escrow Page.

4. Developments favoring cryptography

Congress Bills
The Leahy bill (see above) affirms the right of citizens to use encryption without restrictions in the US (except in furtherance to a felony to impede law enforcement). The Burns bill (see above) also affirms the right to freely use encryption; besides, it would limit the authority of the federal government to set standards for encryption products used by businesses and individuals, particularly standards which result in products with limited key lengths and key escrow. The E-PRIVACY Act (see above) would similarly prohibit the government from mandating key escrow or key recovery.

Representative Markey introduced a bill on 19 June 1997, the Communications Privacy and Consumer Empowerment Act (H.R. 1964). The bill would prohibit restrictions on the use or sale in interstate commerce of encryption software, regardless of the medium used or length of encryption key. Further, the government would be prohibited from conditioning certificates of authority or certificates of authentication upon any key escrow system.

NRC report
The June 1996 National Research Council study Cryptography's role in Securing the Information Society, which was requested by Congress, favors widespread encryption. It says the government should promote widespread commercial use of cryptography. The government can explore key escrow systems for its own use, but it should not push others to use it; even if the current many unresolved questions regarding key escrow were resolved, adoption of escrowed encryption (or of any other standard) should be voluntary.

Advanced Encryption Standard
NIST has approved an Advanced Encryption Standard (AES), FIPS 197, the successor of DES. Minimum acceptability requirements, evaluation criteria, and submission requirements were discussed at a 15 April 1997 workshop. The object of NIST was to create a standard with significant advantages over triple-DES. The standard should use a strong algorithm, regardless of the legal climate, with a (possibly variable) large key length (at least 128 bits). On 12 September 1997, NIST put out a call for candidate algorithms. Fifteen proposals were narrowed down to five, of which on 2 October 2000 Rijndael was selected as the draft FIPS. A notice was published in the Federal Register on 28 February 2001, opening a 90-day public-comment period. After incorporating minor changes from submitted comments, Rijndael was officially approved and announced in the Federal Register, becoming effective on 26 May 2002.
Uruguay [Source 5]

1. Export/ import
Import is not restricted.

2. Domestic laws and regulations
There are no restrictions on crypto use.

Back to the Table of Contents

Venezuela [Source 5]

2. Domestic laws and regulations
There are no regulations on crypto use.

Back to the Table of Contents

Vietnam [Source 5]

1. Export/ import controls
Import of encryption technology for protection of confidential data requires a license from the Ministry of Trade. If the technology is telecommunications equipment, an additional license from the VN Post Office is required. There is a personal-use exemption for travellers with crypto software on a laptop.

Back to the Table of Contents

Please send comments, corrections, updates, additional information, and questions to E.J.Koops@uvt.nl.