

Chapter 5. A survey of cryptography laws and regulations

*So far key escrow products are enjoying less than stellar sales.
(Bruce Schneier, Applied Cryptography)*

Governments increasingly worry about the threat of criminals using cryptography to thwart law enforcement. Several governments have taken steps to address this issue; many are still studying potential lines of action. In this chapter, I describe the various existing and envisaged laws and regulations on cryptography in several countries, focusing on cryptography used for confidentiality purposes.¹ I will briefly go into export regulations in general (5.1); since these are not intended to safeguard law enforcement (they are targeted at hostile foreign powers and terrorists), the details fall outside the scope of this book. After a description of the major international initiatives on crypto policy (5.2), I will outline the encryption policies of Belgium, Denmark, Germany, France, the Netherlands, the Russian Federation, the United Kingdom, and the United States (5.3). Together, they cover the full spectrum of crypto regulations to date (5.4), and so, they provide a good source to look for directions on how to address the crypto conflict.

5.1. Export and import controls

5.1.1. COCOM and Wassenaar Arrangement

The export of cryptography has long been restricted. Evidently, governments have wanted to avoid strong cryptography from falling into the hands of foreign powers, which would have thwarted their ability to do intelligence work. Cryptography has long been regarded as a weapon, and it is still featuring on lists that control the export of munitions. The main international agreement on export controls, the treaty of COCOM,² the Coordinating Committee for Multilateral Export Controls, was replaced by the Wassenaar Arrangement in 1996.

1 For this survey, I have made use of several studies, including [Chandler] and [Kuner]. This chapter covers the state of affairs as of 1 July 1998; for a more elaborate and up-to-date overview, see my online Crypto Law Survey [Koops]. Most of the documents I refer to in this chapter are available online and can be found through a link from this website, so I have not added the references here. See also [Baker 98b].

2 The 17 COCOM 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, South Korea, Sweden, Switzerland, and Taiwan.

COCOM 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, regulating all kinds of cryptography. In 1989, COCOM decontrolled password and authentication-only cryptography. 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 others, such as the United States, maintained separate regulations.

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 terrorists, such as Libya, Iraq, Iran, and North Korea. Exports to other countries were usually allowed, although states often required a license for these.

COCOM was dissolved in March 1994. 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 treaty were finished in July 1996, and the agreement was signed by 33 countries.³ 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. The provisions are largely the same as COCOM regulations. The General Software Note excepts mass-market and public-domain crypto software from the controls; five countries (Australia, France, New Zealand, Russia, and the US) deviate from the GSN and control the export of mass-market and public-domain crypto software. Export via the Internet does not seem to be covered by the regulations. The Wassenaar Arrangement is scheduled to be revised in late 1998.

5.1.2. United States

The United States of America has restricted cryptography export more severely than COCOM and Wassenaar. Crypto exports were controlled under the International Traffic in Arms Regulation (ITAR) until 1996; at the end of that year, they were transferred to the Department of Commerce under the Export Administration Regulations (EAR). ITAR restricted export of 'dual-use' cryptography by placing it on the Munitions List. For (relatively strong) products that can encipher data, an export license is 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, currently 40 bits for symmetric crypto) can also be exported.

In June 1996, the National Research Council released a long-awaited study on cryptography policy [NRC]. It recommended that export controls be relaxed, but not eliminated. Export of 56-bit symmetric encryption products (such as DES) should be allowed, whereas export of cryptography using more than 56 bits should be exportable if the users agree to provide the US government access to decoded information. The NRC

3 Initially, 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, Romania, the Russian Federation, Slovakia, South Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. Later, Bulgaria and Ukraine also signed the treaty.

recommendations have not (or not yet?) been implemented. Although exports for financial institutions have been gradually relaxed, the export controls remain largely as they are. To promote the administration's key-recovery policy (see 5.3), export of 56-bit crypto is allowed if the producer pledges to incorporate key recovery in its products within two years.

The restrictions on cryptography hamper US enterprises, not only those that make crypto products, but also those that make products in which cryptography is a tool, such as web browsers or e-mail programs. Because for some businesses it is inefficient or impractical to make two versions of their products, the export restrictions may also have had the effect of weakening domestic crypto products, as producers may have chosen to make a single, exportable product. Many people feel the EAR rules to be outdated. Strong crypto products incorporating US-made cryptography (or derivatives thereof) are widely available around the world, often online, and sometimes as shareware [TIS]. Several initiatives have been taken to relax the export controls, both in court and in Congress, but they have to date not been successful, with the exception of the *Bernstein* decision. In this case, Daniel Bernstein sought the ability to export his encryption algorithm; the district and federal courts judged the export regulations to be too restrictive. They found the licensing system an unconstitutional prior restraint on free speech (having ruled earlier that crypto source code was protected by the First Amendment). The decision is on appeal. Another case, *Junger v. Daley*, rejected this reasoning and held that encryption export is not protected under the First Amendment.

5.1.3. Import restrictions

As the main goal of export restrictions is to prevent foreign rogues and spies from obtaining cryptography, they usually have no pendant in import restrictions – the more strong cryptography imported, the better. On the other hand, countries with restrictions on *domestic* crypto use generally do apply import restrictions, to prevent the internal market regulation from being disrupted by foreign cryptography. The most notable countries that have import restrictions are France and the Russian Federation. Other countries restricting cryptography import include China, India, Kazakhstan, and South Korea.

5.2. International developments

5.2.1. OECD

The OECD (Organisation for Economic Co-operation and Development) have developed 'guidelines' for a crypto policy, after extensive discussions throughout 1996. The OECD started discussing and drafting policy 'guidelines' in December 1995 with an Ad-hoc Meeting of Experts on Cryptography Policy. The 'guidelines' were discussed and revised in several meetings in 1996, leading to the adoption of the *Recommendation of the Council concerning Guidelines for Cryptography Policy* on 27 March 1997 [OECD 97]. The 'guidelines' are non-binding recommendations to Member governments, meaning that they are not 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*: market forces and government regulation should foster user trust in cryptographic methods.
2. *Choice of cryptographic methods*: users should have the right to choose any cryptographic method, subject to applicable law.
3. *Market-driven development of cryptographic methods*: the market should determine the development and provision of cryptographic methods, including international standards.
4. *Standards for cryptographic methods*: international and interoperable standards for cryptographic methods should be developed; national standards should be consistent with international ones.
5. *Protection of privacy and personal data*: national cryptography policies and the implementation and use of cryptographic methods should respect the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data.
6. *Lawful access*: national cryptography policies may allow lawful access to plaintext or cryptographic keys.
7. *Liability*: the liability of crypto users and of crypto service providers should be clearly stated.
8. *International cooperation*: governments should cooperate to coordinate cryptography policies; governments should remove, or avoid creating, unjustified obstacles to trade.

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.” The balance basically has to be struck between the first five (crypto-friendly) principles and the sixth (police-friendly) principle, lawful access. This crucial and most controversial principle reads: “National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.” Interestingly, the most crypto-friendly principle, free choice, was adapted at the final stage. Where the earlier version read that crypto users should have a right to choose any crypto method, this was extended with the restriction “subject to applicable law”, thus opening the door for a prohibition of cryptography.

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 individual states with the task of finding a balance themselves between, roughly speaking, information security/privacy and law enforcement/ national security – a balance the OECD could not find.

Terminology	
Several governments are studying crypto systems that involve some form of law-enforcement access to keys (LEAK). I will explain these systems in 7.4 and 7.5, but I will already use the terminology here.	
data recovery	all-encompassing term for retrieving the plaintext of encrypted data if the key for decryption is not available, through key escrow, key recovery, or plaintext recovery; the TTP providing data recovery can give private keys, session keys, or plaintexts
KEA	Key Escrow Agent, TTP which provides key-escrow services
key escrow	generic term for crypto systems that provide government (and authorized-user) access to keys by having people deposit their private (or supersymmetric) keys with a TTP
key recovery	originally a term for a crypto system which provides LEAK by having people tag along to messages a recoverable session key rather than deposit their private keys; is increasingly used, irrespective of the technology, as a generic term for LEAK and a replacement for 'key escrow' which has become a too negative term; I use it in the original sense: recovering session keys
LEAK	Law-Enforcement Access to Keys, a generic term for key escrow and key recovery for law-enforcement purposes
TTP	Trusted Third Party; a trusted, independent organization which offers cryptography-based services that enhance the reliability of electronic data interchange and storage, such as key certification, distribution, revocation, and time-stamping; the term includes Certification Authorities, Key Escrow Agents, and Data Recovery Agencies

5.2.2. European Union

The 1993 draft *Green Book on the Security of Information Systems* [DG XIII], which has not been officially adopted by the European Council, posed a case for the provision of 'Public Confidentiality Services' (which would somehow offer Law-Enforcement Access to Keys).

Since 1996, the European Commission has been working 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 TTPs. Although primarily meant for establishing an infrastructure for the use of public-key encryption, the initial proposal also tried to address the legal-access problem, e.g., through key escrow. The studies conducted did not address data recovery in-depth, but concentrated on issues related to establishing a public-key infrastructure for digital signatures. The report on the results of the 1995 TTP projects said that data-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."

With the release of the *Communication Towards A European Framework for Digital Signatures And Encryption* [COM (97) 503], however, the European Commission has chosen a direction away from data 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, although it is much less explicit here than it is on digital-signatures 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 harmonization 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 data-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. An EU expert meeting was organized in Copenhagen, on 23-24 April 1998, to initiate a broader debate on encryption issues; the meeting exuded a reserved attitude towards data recovery.

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

ETSI (the European Telecommunications Standardisation Institute) is developing a standard for Trusted Third Parties. Part of the standard would relate to lawful access to encrypted data. Great Britain has pushed here for its Royal Holloway key-escrow scheme (see 7.4.3) to be used as a basis for the standard, but this was not adopted, as several EU countries opposed the mandatory key-escrow approach.

5.2.3. Other European initiatives

On 11 September 1995, the Council of Europe⁴ issued a *Recommendation Concerning Problems of Criminal Procedure Law Connected with Information Technology*, which 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.” [CoE 95] 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”. Although some have interpreted the recommendation as leading to mandatory key escrow, the text does not imply this at all.

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 that 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 data recovery).

4 The Council of Europe is a 40-member intergovernmental organization (not to be confused with the European Council, which is a body of the 15-member European Union). Its treaties are not directly applicable in national law, but its recommendations induce members to adapt their legislation accordingly.

5.3. Domestic crypto laws per country

5.3.1. Belgium

In January 1996, Belgium all of a sudden discovered that it had a law which some interpreted as prohibiting the use of unescrowed encryption. The law had been passed in December 1994 as part of a larger law and had gone unnoticed at the time. The law adds a condition under which telecoms equipment may be seized, namely when end equipment renders tapping ineffective.

According to this law, crypto systems had to be agreed by the Belgian Institute for Posts and Telecommunications (BIPT), and the law could be interpreted as allowing a phone to be disconnected when it uses cryptography. It could also enable the establishment of a system of mandatory key deposits at BIPT, where the judiciary could access them. [Clerk]

Two legislation proposals were submitted in June 1996 to drop the contentious provisions of the 1994 law. One of these, by 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 was necessary for the investigation.

The law was amended on 19 December 1997 to clear the confusion. A new 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 BIPT. 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 key deposits. The new law does not mean that the government has abandoned every desire to gain access to coded messages in the future: "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".

5.3.2. Denmark

The Danish Technology Council, in an October 1995 report [Stripp], 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 the Danish government should cut expeditiously.

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.

A departmental Expert Committee, appointed in the summer of 1996 in preparation for a final decision on the crypto issue by the government, released its *Report by the Expert Committee on Cryptography* in April 1997 [ECC]. The Committee, under pressure of time, rather unrealistically 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 (sale) should be introduced presently. It further recommended that it continue

its work, in order to carry out an analysis of the possibilities and consequences of introducing incentive schemes to induce people to use key-recovery crypto. The Committee was allowed to continue its work, and in June 1998, it recommended that the government should refrain from restrictions on crypto use, including incentive schemes to induce people to use key recovery. If, however, international developments should lead to other countries generally favoring key recovery, the government should reconsider this position. On the basis of the Committee's recommendations, the government was supposed to take a stand on the crypto issue after the summer holidays.

5.3.3. France

France has long restricted the import, export, use and marketing of cryptography. The regulation distinguishes between cryptography that can be used *only* for authentication, and cryptography that can (also) be used for confidentiality purposes.

Before 1996, delivery, export, and use of cryptography were subject to:

- previous declaration if the cryptography could have no other object than authenticating communications or assuring the integrity of transmitted messages;
- previous authorization by the Prime Minister in all other cases.

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

On 18 June 1996, France passed a law slightly liberalizing these restrictions. The law was published on 27 July 1996 and is referred to as the 26th July law. Decrees on the application of the law (which had to be promulgated for the law to be applicable) were delayed significantly, to be published only in February and March 1998. They covered, among others, the conditions of declarations and authorizations, and the conditions for key-escrow agencies.

Cryptography that does not provide for confidentiality can be used without restriction (the previous requirement of declaration is canceled); supply of authentication-only cryptography still has to be declared. Use and supply of confidentiality cryptography require authorization. A decree specifies categories of cryptography which do not require declaration or authorization, or which require only prior declaration rather than authorization (e.g., cryptography for video-scramblers or ATMs, and cryptography with a key length of up to 40 bits). A supplier is exempted from the formalities for use exclusively for developing, validating or demonstrating cryptography, if he informs SCSSI (the government body responsible for crypto policy) at least two weeks in advance. No authorization is given for cryptography for use by radio amateurs. A supply authorization for collective use exempts users from acquiring a use authorization.

The law furthermore introduces Trusted Third Parties (TTPs), or rather, Key Escrow Agents (KEAs). If a KEA and its key-escrow scheme have been approved, users who escrow their keys with the KEA will be able to freely use the cryptography scheme with these keys. The KEAs will be required to hand over keys to law enforcement under certain conditions. Currently, the only approved KEA is (surprise!) SCSSI itself.

Decree 98-102 specifies the conditions for KEAs. It addresses, among others, the duration of a license to operate, the information the KEA has 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 a KEA ceases its activity. KEA employees are required to have a French security clearance.

The action plan on Electronic Commerce, 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” [Lorentz]. It urged a rapid implementation of the new law, and it proposed further 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 and key deposits, and 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. Given the quite restrictive decrees published afterwards, however, one wonders whether the government as a whole is “committed to a liberal reading”.

It is unclear to what extent the present regulation is being enforced in practice; it is rumored to be widely ignored. It seems difficult for individuals or enterprises to obtain authorization for ‘strong’ cryptography.

5.3.4. Germany

In the February 1996 policy document *Info 2000: Germany’s Way into the Information Society* [BfW], the German government supported the European Commission’s ETS initiative. A focal point is 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”.

Several politicians have expressed a desire to regulate cryptography (see [Moeller] for an overview). There have been many conflicting rumors on the imminence of a crypto regulation, while the government continued to state it was still forming its opinion.

The German federal government is, in fact, itself divided over the issue. Federal Interior Minister Kanther stated, in a speech on 28 April 1997, that he wants to control encryption by allowing only technologies whose manufacturers agree to provide keys to law enforcement (this seems a requirement for crypto providers to build in LEAK). 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. Use of certified products would be voluntary. In October 1997, parliamentarian Tauss revealed that Kanther favors 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 (the government agency for IT security) stated that the chip did not contain a backdoor.

Contrary to Kanther, the Minister of Economic Affairs Rexrodt opposes 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 opposes a restrictive crypto regulation. The initiative on Electronic Commerce, from 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 LEAK 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.

By mid-1998, it was generally expected that the issue would, if at all, be decided after the September 1998 elections. The recent government statements show that it is generally leaning towards a stimulating rather than a restrictive approach to cryptography.

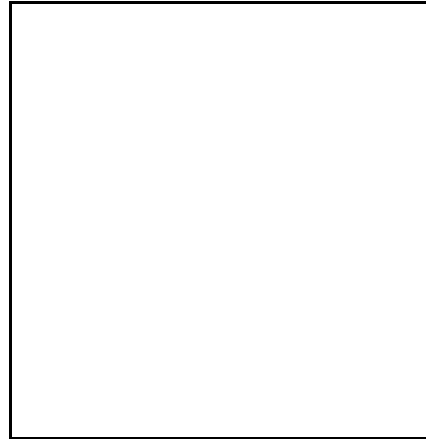
5.3.5. The Netherlands

In the early 1990s, when the Netherlands discussed a Computer Crime Act, it was recognized that the power to search in computers would be useless if the files in the computer were encrypted. Therefore, a power was introduced to demand decryption (art. 125k para. 2 DCCP). If encrypted data are 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 data. The command cannot be given to suspects, respecting the privilege against self-incrimination.

In March 1994, a Dutch pre-draft 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; many interpreted this as a requirement to deposit keys with the agency. After many protests from those who would have been affected by the proposed regulation, the government somewhat sheepishly withdrew it.

As the power to demand decryption is rather useless in practice (in almost all situations, it is only the suspect who knows the key to the encrypted files, and the command can only be given *during* a search), the government has studied on additional means to solve the crypto problem for law enforcement. An envisaged legislative update, the draft Computer Crime Act II, proposes to extend the present decryption command to cover encrypted telecommunications as well. So, if the police encounters encryption in a wiretap, they could command the conversing parties to assist in decrypting. The draft Computer Crime Act II also proposes to extend the power of the police to demand decryption to be given after the search has ended, to allow the police to seize the hard disk for later analysis. Initially, the draft also proposed to give the command to suspects as well, in case of grave evidence against the suspect and if this is urgently necessary for finding the truth. The Explanatory Memorandum considered this in accordance with the privilege against self-incrimination as interpreted in European Court case law, but after protests from the legal community, the provision was removed. (See further Chapter 8 on this issue.)

The government is working on a Trusted Third Parties policy, intended to set preconditions for TTPs to operate. The final report on the TTP project, of March 1998, mentions lawful access to cryptographic keys as a desirable condition for TTPs offering authentication or confidentiality services.⁵ However, since most current TTPs do not store private keys, and because of the risks involved in requiring TTPs to store keys, the report suggests that it should not be mandatory for TTPs to store private user keys, although it recommends TTPs to do so. If the TTP does (in effect becoming a KEA), the police can access the keys with a warrant. [KPMG 98]



The government's policy document *Legislation for the electronic highway* of 12 February 1998 [25880, nrs 1-2], affirms that one of the premises for establishing law-enforcement powers is that the use of cryptography will remain free.

5.3.6. Russian Federation

On 3 April 1995, president Yeltsin issued a decree prohibiting unauthorized encryption [Указ]. State organizations and enterprises need a license to use encryption (for both authentication and confidentiality, for storage as well as transmission). Non-state enterprises and organizations using uncertified cryptography do not receive state orders. The Central Bank takes measures against commercial banks that do not use certified cryptography when communicating with divisions of the Central Bank. The development, production, implementation, or operation of cryptography without a license is prohibited. Licenses are issued by FAPSI (a successor of the KGB) based on internal regulations.

5.3.7. United Kingdom

The Department of Trade and Industry (DTI) has been working on a crypto policy since 1996. It proposed legislation in early 1998 after a consultation process with interested parties. After publishing a paper on regulatory intent in June 1996, 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 department took its time in studying the 260 reactions, publishing a summary of the responses in April 1998, together with an

⁵ The report suggests that the condition of lawful access does not hold for TTPs offering authentication services, but only if the TTP ensures "that the TTP service and the keys in question *can only be used* for authenticity and integrity." [KPMG 98, 15-16, emphasis added] In several crypto systems, signature keys can also be used for confidentiality encryption, and in fact, an authentication service can always facilitate confidentiality encryption (see 7.7.1). Therefore, this would imply that authentication TTPs would also have to provide lawful access to keys – which they usually will not be able to do since they do not have access to secret or private keys.

indication of envisaged legislation. The general aim of the legislation process would be to engender trust in TTP services, while at the same time addressing the law-enforcement problems caused by cryptography. In general, the UK government seems to favor a large-scale implementation of the Royal Holloway scheme (see 7.4.3); although it is not explicitly mentioned, the language of the papers suggests inspiration by the Royal Holloway configuration.

The legislation proposed in the 1997 consultation paper would regulate the licensing by DTI of TTPs that offer cryptographic services - Certification Authorities, Key Escrow Agents, and other types. All cryptographic services offered (by organizations, not by individuals) to the public and businesses would 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 would 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 would 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 would have to be handed over, not signature keys (although the paper does not say how to distinguish between (dual-use) keys). The paper involves key escrow (not key recovery), and 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 foreign TTPs, there would have to be agreements with other countries on the basis of dual legality. TTPs would be liable for the protection of the private keys, and there would be strict liability for TTPs for compromise or disclosure of private keys. The requirement for releasing private keys upon a lawful warrant only addressed licensed TTPs who are able to comply, i.e., Key Escrow Agents, not Certification Authorities (CAs).

The paper confirmed that use of licensed TTPs would be 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 were restricted, there might be an effective regulation of encryption use after all. Moreover, the "Government recognise[d] 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."

On 27 April 1998, Barbara Roche, Parliamentary Under Secretary of State at DTI, announced the definitive policy proposal of DTI, based on the responses to the consultation document. The policy follows the consultation 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. 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; see below.) Despite meeting several concerns raised in the consultation process, the final proposal still met with negative comments from UK citizens, notably on the mailing list ukcrypto. Legislation is scheduled for the 1998-1999 parliamentary session.

The new Labour government thus has not significantly altered the DTI policy proposals, contrary to prior hopes and expectations. After all, Labour had stated in its policy on the information superhighway, *Communicating Britain's Future*, that 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] Instead, Labour wanted authorities to have the power to demand decryption under judicial warrant.

5.3.8. United States of America

Escrowed Encryption Standard (Clipper)

In 1993, the Clinton Administration announced the Escrowed Encryption Standard (EES), usually referred to as Clipper, after its first implementation in the Clipper chip. In this initiative, law-enforcement agencies wiretapping communications encrypted with EES could decipher tapped messages by obtaining the two parts of the chip's master key deposited with two escrow agencies (National Institute of Standards and Technology and the Treasury Department's Automated Systems Division), provided they had a court order for the tapping. Following criticisms on the choice of escrow agents, the government came up with 'commercial key escrow' (soon dubbed 'Clipper II'), a scheme in which the escrow agents could be independent organizations chosen by cryptography users.

The EES was a voluntary standard to be used in telephone communications. Privacy advocates feared that the government would declare escrowed encryption mandatory once it had captured a sufficient portion of the market. Documents obtained by EPIC under the Freedom of Information Act show that already in 1993, federal agencies concluded that the Clipper initiative would only succeed if other crypto-systems were outlawed. FBI director Freeh stated in hearings on pro-crypto bills: “I believe that the [voluntary key-escrow] policy that is enunciated here is a doable policy, but there could come a point where that policy, the voluntary policy, is not a viable one. And then I would certainly look at more mandatory controls” [EPIC Alert 3.14, 1 August 1996].

The EES was generally rejected, though, and in March 1997, the Department of Defense announced that the NSA, developer of the Fortezza card (which contained 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). (See further 7.4.2 on Clipper.)

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 proposed the establishment of a key-management infrastructure (KMI) that incorporates key escrow [IWGCP]. Participation in the KMI would be voluntary, and choice of encryption algorithms would be free. A Policy Approving Authority would certify 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 Escrow Authority) in order to get a public-key certificate. Self-escrow would be considered an acceptable option, if the corporate CAs could meet necessary performance requirements, including independence from the rest of the organization and handing over keys to law enforcement.

Efforts to develop a Federal Information Processing Standard for a KMI have been slow. Despite ten meetings, the Technical Advisory Committee could ultimately not produce a definite FIPS recommendation due to conflicting requirements. [Davidson] The charter for the elegantly named TACDFIPSFKMI⁶ was renewed in August 1998 to continue work on the requirements for key-recovery products.

NRC report

The June 1996 National Research Council CRISIS study *Cryptography's Role In Securing the Information Society* [NRC], which was requested by Congress, favors widespread encryption. It says the government should promote extensive 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 many questions regarding key escrow were resolved, adoption of escrowed encryption (or of any other standard) should be voluntary.

Broad Encryption Policy

On 1 October 1996, Vice President Gore made a statement on export controls, in which he also referred to domestic crypto use. Domestic use of key-escrow cryptography would be voluntary, and the choice of an encryption system would remain free. The government would, however, promote key-escrow crypto by expanding the purchase of key-escrow products for itself, promoting key escrow in international discussions, and stimulating the development of innovative key-escrow products and services. The Administration would also seek legislation to facilitate commercial key escrow, covering, among others, liability issues for releasing keys.

The 'special envoy for cryptography', ambassador Aaron, appointed in November 1996, promoted international cooperation and coordinated US contacts with foreign governments on encryption matters. The 'crypto czar' traveled extensively abroad to lobby (largely unsuccessfully, as it turns out) for the US-favored key-recovery approach.

6 Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure.

Draft key-recovery legislation

At the end of March 1997, a draft Key Recovery Legislation 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 and (private or government) Key Recovery Agencies (KRAs). A registered CA could 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 – would have to disclose recovery information to government agents under the same legal criteria as those for wiretapping. The use of encryption in furtherance of the commission of a criminal offense would be punished with six months' to five years' imprisonment (having used key recovery which is reasonably available to the government would be an affirmative defense). Finally, the President should conduct negotiations with other countries on the mutual recognition of registered KRAs. The draft legislation affirmed that use of any encryption would be lawful except as provided in the Act or other law (which means any encryption use is lawful except in furtherance of a crime), and that use of the key-recovery infrastructure would be voluntary. The government stopped seeking a sponsor for the draft bill when developments in Congress seemed to lead to similar legislation.

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*. It had 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 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.

An unofficial proposed amendment to the *Secure Public Networks Act*, circulating in the government by the end of August 1997, would have prohibited the manufacture, distribution, sale or import of non-key-recovery cryptography (not its use or possession). The draft amendment contained several other changes, e.g., dropping the requirement for CA registration that the CA ensure recovery information to have been escrowed. In a 3 September 1997 Senate subcommittee hearing, FBI Director Freeh backed this draft legislation, but at the same time, he said 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, which required a court order for law-enforcement access and which dropped the link between digital-signature key certification and key recovery.

Also in 1997, Representative Goodlatte's *Security And Freedom through Encryption Act* (SAFE) was heavily debated. While aiming at relaxing export controls, it was substantially amended by the House Permanent Select Committee on Intelligence, effectively imposing mandatory key escrow (the Goss-Dicks amendment), and making it a quite different bill. The only provision of the original bill on domestic use had been a penalization of crypto use in furtherance of a criminal offense. However, the House Commerce Committee 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 would 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 the government mandating key escrow was maintained by the Commerce Committee. Given the many competing versions, the bill was not fit for voting, especially since 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.

Senators Ashcroft and Leahy, in May 1998, introduced the E-PRIVACY Act, a creative acronym for Encryption Protects the Rights of Individuals from Violation and Abuse in CYberspace. The bill would also penalize using cryptography to conceal incriminating information in the commission of a federal felony with five to ten years' imprisonment. Like the Markey-White amendment to the SAFE act, the bill would create a NET Center to assist law enforcement. The bill would prohibit the government from mandating key escrow or key recovery.

Conclusion

The US government has been trying to establish some form of more or less mandatory key-escrow or key-recovery policy, although lately, they have increasingly stressed the voluntary nature of their proposals. Such a policy is heavily debated, and citizens, privacy lobby groups, and industry generally fiercely oppose this approach. This is reflected in Congress, where many competing (versions of) bills have been and are being discussed, none of which seems currently to carry sufficient support to be enacted. Therefore, despite the heated debate, the US still does not have any domestic regulation of cryptography.

5.4. Concluding remarks

The survey of cryptography laws shows that regulations differ widely. Some countries have virtually prohibited cryptography (Russia, France). Others are looking at LEAKy solutions (in particular the US and the UK), but they face fierce opposition by their citizens. Moreover, other countries and the European Commission are wary of this approach. Some countries are looking at commanding people to decrypt as a solution. The Netherlands has enacted a law to that effect, which is currently under revision to enable the police to give a decryption command in more situations.

Most countries leave cryptography as yet unregulated – if not by a conscious decision, then at least by a failure to develop a viable and broadly supported policy. The complexity

of developing an acceptable crypto policy is also reflected in the international talks on the subject. Given the failure of the OECD 'guidelines' to steer international crypto policies, there is little hope that there will be an international or supranational agreement on addressing the crypto problem within the foreseeable future.

Failing international consensus, countries are thinking of taking steps on their own, driven by a growing concern for criminal crypto use. However, most governments are confused over the direction of a policy, and they seem to be looking at other countries to see what the emerging international direction will be. So, there is a general impasse in the crypto-controversy debate.