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

Regulation of Investigatory Powers Act 2000

On 28 July 2000, the Regulation of Investigatory Powers Act 2000 (2000 Chapter 23) received Royal Assent. Part III of the RIPA contains a power to order disclosure in cases of encrypted data. Part III entered into force on 1 October 2007, after a lengthy process to establish the Code of Practice (see below).

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)).

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.

A section 49 decryption order is given regularly in practice, in cases involving for example child indecency, terrorism, insider dealing, theft, and evasion of excise duty. Data are provided by the Chief Surveillance Commissioner's Annual Reports (note that in the following, data from one period may include cases from a previous period, so the numbers do not add up precisely for each period). In the period April 2008 - March 2009, the National Technical Assistance Centre (NTAC) declined one application for a decryption order and approved 26 applications. 17 of these were forwarded for court approval, which was granted, leading to 15 decryption orders being given. 11 individuals failed to comply with the order. Seven of them were charged, and two convicted, under the Act. Between April 2009 - March 2010, 38 orders were approved by NTAC, 22 received court permission, 17 were served, of which six were complied with and seven were not complied with (the others were pending). Five non-compliers were charged under the Act, leading to one conviction, in a case involving child pornography; the other cases were pending at the time of the report. Unfortunately, the reports provide no information about the penalty for the convictions of failing to comply with the decryption order. Between April 2010-March 2011, 26 out of 30 orders were approved by NTAC, 17 received court permission, 12 were served; 4 orders were complied with, 2 were not complied with; 3 non-compliers were prosecuted, and 1 person was convicted. Between April 2011-March 2012, all 57 requested orders were approved by NTAC, 33 received court permission (the report does not say what happened to the other 21 for which court permission was sought), 20 were served; 9 orders were complied with, 15 were not complied with; 9 non-compliers were prosecuted, and 2 persons were convicted.
The punishments meted out in cases where people were convicted for not complying with the decryption order, are not mentioned in the Surveillance Commissioner's reports. News reports suggest that in one terrorism case, someone was convicted to 9 months' imprisonment ('UK jails schizophrenic for refusal to decrypt files', The Register 24 November 2009), while in a child-pornography case, a sentence was given of 16 weeks ('Teen jailed over failure to hand over computer password', Out-law.com 6 October 2010).

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

On 23 July 1999, the government published a draft Electronic Communications Bill, together with a new consultation document "Promoting Electronic Commerce. Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report", which also contained the Explanatory Notes to the draft 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 two 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 soons 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 in cryptography regulation

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 statement 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 TTP's 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 TTP's 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.