EC plans encryption rules in bid to police information superhighway

Paris. The European Commission is to propose legislation to police the information superhighway that will include powers to decrypt confidential telephone and computer communication.

The commission's move follows concern over the perceived increase in the 'illegal' use of the Internet, including the proliferation of pornography and the unauthorized release of classified documents.

It also coincides with a similar proposal from the 34-nation-member Council of Europe. The proposals would, if passed into law, effectively end the Internet's status in the 15 member states of the European Union (EU) as an unregulated medium for the free flow of information.

But they have also raised questions about the possible violation of telephone and computer privacy, as well as the preferred choice of encryption/decryption system.

The proposal to introduce Europe-wide surveillance guidelines has been confirmed by a senior official responsible for encryption and data security in the French government. He says that Brussels is working closely with the Senior Officers' Group for Information Security Systems (SOGIS), a collection of experts from EU countries, chaired by the commission itself.

The commission is expected to publish its guidelines later this autumn, detailing the powers of enforcement to be given to regulatory authorities, as well as a preferred choice of decryption system. The guidelines will then be considered by the EU's Council of Ministers and the European Parliament.

But a spokesman for the commission's telecommunications directorate says that the decryption mechanism is likely to be based on a version of the 'key escrow system'. This refers to the policy under which users of encryption systems give copies of their decryption keys either to their government or to a third party that the government trusts. The keys can be handed over if the government, on production of a court order, wants to monitor encrypted information.

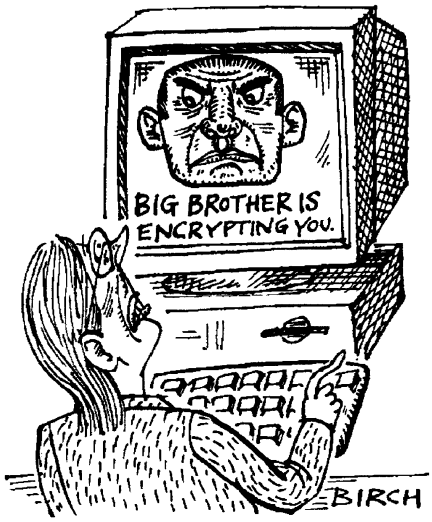
The system being considered by the commission will enable EU countries to monitor encrypted telephone and computer communications in member states. Thus if someone in Germany makes a call to Italy, agencies in both countries would possess the keys enabling them to decrypt the call.

Significantly, the commission will also propose that member states choose private 'trusted third parties' rather than government departments to regulate computer and telephone networks. It is thought to believe that this move will secure greater public support for the proposals.

But civil liberties groups remain sceptical, and maintain that the use of 'third parties' to police the Internet raises its own questions, one of which is deciding which party to trust and ensuring they all remain trustworthy. "It is difficult to trust these third parties," says Simon Davies from the organization Privacy International. "There is no guarantee that the keys [to decryption] will not be corruptly accessed within the 'trusted' organization."

Critics of the commission's proposals also include information technology specialists, although their concerns are different. Ross Anderson, a senior research associate in computer and communications security at the University of Cambridge's Computer Laboratory says that the Council of Ministers will need to iron out various issues before the key escrow system is fit for use.

One factor, says Anderson, is that such a system ironically falls victim to precisely what it is trying to protect — namely, national security. "If you are a banker doing a politically sensitive deal — such as renegotiating the Eurotunnel debt — then the UK government will certainly not want the French to get that key."



Similarly, the decryption key for a secure telephone bought in Britain will be kept at the government's General Communications Headquarters. But if it is taken into France and used to call someone in Germany, the French government "will inevitably want a copy of the key", says Anderson.

This direct conflict of national security priorities, adds Anderson, makes it hard to "specify a system which satisfies the curiosity of intelligence agencies, while still providing meaningful privacy to users".

A parallel proposal for decryption was announced earlier this month by the Council of Europe. Peter Csonka, head of the council's Crime Problems Division, said its 18 suggestions were long overdue following concern that "electronic information systems and electronic information may also be used for committing criminal offences".

The council's suggestions include giving investigating agencies the right to search computer networks and seize offending, unauthorized or illegal material. The proposals will also require providers of telecommunication networks to "avail themselves of all necessary technical measures that enable the interception of telecommunications by investigating authorities". **Jerome Thorel**

Royal Society opens rebuilt lecture hall

London. **Britain's Royal Society last week re-opened its 168-year-old lecture theatre (right), newly refurbished after asbestos was discovered in the ceiling in 1994. It is now named the Wellcome Trust Lecture Hall.**

The new facilities, according to a Royal Society spokeswoman, "blend the prestigious and elegant atmosphere of Carlton House Terrace, designed in 1827, with modern comfort and state-of-the-art technology".

The Royal Society itself was founded in 1660, by a group of 12 founding fellows including Robert Boyle. The lecture hall was opened on Tuesday with a quiz pitting a team from Trinity College, Cambridge, this year's winners of the television quiz show *University Challenge*, against a one made up of fellows of the society. □

© 1995 Nature Publishing Group