# *European Parliament accepts report on ECHELON global interception system*

report by Eugene Oscapella

BUSINESSES IN THE EU, suspecting that their operations are being monitored, to their commercial disadvantage, by foreign intelligence services, have new reason to worry, according to a report released in July. The European Parliament voted to accept the report on September 5th.

The European Parliament's investigation of the global surveillance system known as ECHELON has resulted in a report and resolution. On July 5th 2000, Parliament decided to set up a temporary committee to examine ECHELON, the global communications interception system. Among its duties, the committee was to assess the compatibility of such a system with Community law. In particular, it was to address the following questions:

• Are the rights of European citizens protected against activities of secret services?

• Is encryption an adequate and sufficient protection to guarantee citizens' privacy or should additional measures be taken, and if so what kind of measures?

• How can the EU institutions be made better aware of the risks posed by these activities and what measures can be taken?

• Is European industry put at risk by the global interception of communications?

The lengthy Temporary Committee report, released on July 11th 2001, concluded that there was no longer doubt about the existence of a global system for intercepting communications operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UK-USA Agreement. Among the most important findings for businesses, the Committee reported that the purpose of ECHELON is to intercept private and commercial communications, and not military communications.

The temporary committee made the following additional findings:

1. The technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed. Nevertheless, it is worrying that many senior Community figures, in particular European Commissioners, who gave evidence to the Temporary Committee, claimed to be unaware of this phenomenon.

2. The surveillance system depends, in particular, upon worldwide interception of satellite communications. However, in areas characterised by a high volume of traffic only a very small proportion of those communications are transmitted by satellite. This means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals. However, inquiries have shown that the UK/USA states have access to only a limited proportion of cable and radio communications, and, owing to the large numbers of personnel required, can analyse only an even smaller proportion of those communications. However extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice.

3. If the system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the European Community Treaty. However, if the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition. If a Member State participates in such a system, it violates EC law.

4. Any interception of communications represents serious interference with an individual's exercise of the right to privacy. An intelligence system which intercepts communications permanently and at random

would be in violation of the principle of proportionality and would, therefore, not be compatible with the European Convention on Human Rights (ECHR). It would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible, or if they were so formulated that their implications for the individual were unforeseeable. Member States must act in a manner consistent with the ECHR.

5. As the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and since in some cases parliamentary monitoring bodies do not even exist, the degree of protection can hardly be said to be adequate. It is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services. But even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic rather than foreign intelligence services, since as a rule it is only the former which affect their own citizens. In the event of cooperation between intelligence services under the Common Foreign and Security Policy (CFSP) and between the security authorities in the spheres of justice and home affairs, the institutions must introduce adequate measures to protect European citizens.

6. The US intelligence services do not merely gather general economic intelligence, but also intercept communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery. Detailed interception poses the risk that information may be used as competitive intelligence, rather than combating corruption, even though the US and the United Kingdom state that they do not do so. At all events, it must be made clear that the situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country. Although it is frequently maintained that the global interception system considered in this report has been used in this way, no such case has been substantiated. The fact is that sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more frequently, by hacking into internal computer networks. Only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering.

7. Risk and security awareness in small and medium-sized firms is unfortunately often inadequate and the dangers of economic espionage and the interception of communications are often not recognised. Since security awareness is likewise not always well developed in the European institutions, immediate action is, therefore, necessary.

### POSSIBLE SELF-PROTECTION MEASURES

Firms must secure the whole working environment and protect all communications channels which are used to send sensitive information. Sufficiently secure encryption systems exist at affordable prices on the European market. Private individuals should also be urged to encrypt e-mails: an unencrypted e-mail message is like a letter without an envelope. Relatively user-friendly systems exist on the Internet which are even made available for private use free of charge.

The report made several recommendations directed at the commercial environment:

• The European Union and the USA should conclude an agreement on the basis of which each party applies to the other the rules governing the protection of privacy and the confidentiality of business communications which are valid for its own citizens and firms.

• EU Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.

• Member States and the US Administration are called upon to start an open US-EU dialogue on economic intelligence-gathering.

• United Kingdom authorities are called upon to explain their role in the UK/USA alliance in connection with the existence of a system of the 'ECHELON' type and its use for the purposes of industrial espionage.

• Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.

• The Commission and Member States are called upon to inform their citizens and firms about the possibility of their international communications being intercepted. This information must be combined with practical assistance in developing and implementing comprehensive protection measures, not least as regards IT security.

• The Commission, the Council and the Member States are called upon to develop and implement an effective and active policy for security in the

*continued on page 23*