

European parliament approves anti-privacy laws

Mike Ingram
11 June 2002

In a vote last week the European parliament approved measures that will allow the 15 member states of the European Union to force telephone and Internet companies to retain detailed logs of their customers' communications for an unspecified period. The security services and the police can then access these records, which are presently kept for only a couple of months for billing purposes before being destroyed. The law will be formally adopted by EU governments within a few months and implemented by the end of 2003.

Although police will still require a warrant to intercept the content of electronic communications, the new legislation means that they will be able to build up a complete picture of an individual's personal communications, including who they have emailed or phoned and when, and which Internet sites they have visited. With access to mobile phone records police will also be able to map a person's movements because the phones communicate with the nearest base station every few seconds. In urban areas, the information is accurate to within hundreds of metres. With the next generation of mobiles, accuracy will increase to within a few metres.

This latest directive is the final element of new electronic communications regulations, which entered into force on April 24, 2002. These data retention regulations are contained in an amendment to a bill originally intended to improve the security of e-commerce transactions. The bill's original author, Italian independent MEP Marco Cappato has condemned the amendments. He rejected any responsibility for the outcome of the bill, saying they entailed massive restrictions on civil liberties.

"Looking at the results, it amounts to a large restriction on privacy and increases the power of the state," said Cappato, who tried to prevent the amended

clause being added.

The EU legislation is the latest in a series of measures introduced internationally that have utilised the September 11 terrorist attacks to implement massive attacks on democratic rights. The bill provides EU member states with the power to lift the protection presently covering data privacy in order to conduct criminal investigations or safeguard national or public security when this is a "necessary, appropriate and proportionate measure within a democratic society." Opponents of the bill warn that police forces will use the collected information as a database to trawl through for suspicious activity rather than act on a case-by-case basis. Casper Bowden, executive director of the Foundation for Information Policy Research (FIPR), told the *Guardian* newspaper that the law allows for even a minor incident, such as joyriding near a military base, to be linked to terrorist activity.

A coalition of 40 civil liberties groups issued a joint statement warning that some of the proposed amendments could have "disastrous consequences for the most sensitive and confidential types of personal data."

Tony Bunyan, editor of *Statewatch*, said, "This is the latest casualty in the war against terrorism as far as civil liberties are concerned. The problem with wanting to monitor a few people is that you end up having to keep data on everybody."

John Wadham, director of Liberty (formerly Britain's National Council of Civil Liberties), said of the amendment: "This violates a fundamental principle of privacy, which is that data collected for one purpose should not be used for another. The police and other authorities will be able to trawl through all the details of the communications of millions of innocent people merely because there is a possibility that they might

come across something suspicious.”

The British government, which introduced its own Anti-Terrorism, Crime and Security Act (ACTS) last December, played a key role in pushing through the new measures and will now press ahead with the introduction of similar data retention measures contained in the ACTS. The European vote was welcomed by the Home Office, which said, “The UK is very pleased that the [European] council and parliament have reached agreement on a text that will ensure that the fight against terrorism and other crime will be given the appropriate weight. It is, of course, very important to protect people’s fundamental rights and freedoms, but, as the tragic events of September 11 show, this must be balanced with the need to ensure that the law enforcement community can do its job.”

In fact the British legislation has nothing to do with September 11 and was on the cards since April 2000. This was confirmed in a document written by the National Crime Intelligence Service on behalf of the government’s main electronic surveillance centre, GCHQ, and other agencies, which was leaked in December 2000. With the tragic events of September 11 came an ideal opportunity to push through the planned legislation.

As late as November 2001, the European Parliament had voted to uphold the right to privacy. The initial bill to which the amendment was attached had also tried to strengthen privacy safeguards by calling for data storage to be conducted only in exceptional circumstances. This was criticised by member states, particularly Britain, which wanted greater power to monitor the Internet. US officials also criticised the bill, claiming that the request to erase data would hinder the prosecution of criminals.

In the hysterical climate produced by US President Bush’s war against terrorism, the amendment could be pushed through in order to bring European legislation into line with British policy. Both the British ACTS and the new European legislation could still be challenged under the European Convention on Human Rights.



To contact the WSWS and the
Socialist Equality Party visit: