Cybercrime: A European Perspective

THE COUNCIL OF EUROPE is reaching final agreement on its Cybercrime Communication. As well as dealing with issues such as copyright infringement, the Communication also prohibits internet service providers from being a conduit for illegal material or programmes which might deface websites. The treaty details for how long ISPs should retain connection data from subscribers, and tackles other measures to ensure co-operation between ISPs and local police.

Draft 25 of the Treaty was discussed at a meeting in Strasbourg, in December 2000 and the text was submitted to the Parliamentary Assembly in April 2001. The text will be subject to a further revision by the European Committee on Crime Problems (CDPC) which is then expected to approve it at its next Plenary session in June 2001. The text then will be submitted to the Committee of Ministers for adoption.

This document, provisionally the *Council of Europe Draft Convention on Cybercrime*, will be the first ever international treaty, the Council says, to address criminal law and procedural aspects of various types of criminal behaviour directed against computer systems, networks or data and other types of similar misuse.

However, it has attracted some criticism. In a letter to the Council of Europe, the Global Internet Liberty Campaign wrote: "To our dismay and alarm, the Convention continues to be a document that threatens the rights of the individual while extending the powers of police authorities, creates a low-barrier protection of rights uniformly across borders, and ignores highly regarded data protection principles." Many privacy groups and others are urging countries to refuse to sign the treaty when they are asked to do so.

As from 14 February 2001, the text of the draft explanatory memorandum has been made public to help readers of the draft Convention better understand the scope and meaning of its provisions, as intended by the drafters. Explanations provided in this document should, therefore, be read in conjunction with the draft treaty's provisions. Any comments on this draft Explanatory Memorandum would also be welcome.

EUROPEAN COMMISSION

At a conference organised in Brussels on March 7th, the European Commission proposed future legislation on child pornography, hacking and denial of service. It also proposed the creation of a Forum for discussing such issues. There was consensus that the EU does have an important role in trying to harmonise Member States' approaches. However, less certain was how such initiatives would mesh with the Council of Europe's Cybercrime Convention, now nearing completion (see above). On the main theme of the day, - retention of traffic data – there was no consensus. The law enforcement agencies insist that such data is important for fighting crime, but fail to appreciate business' concerns relating to cost and privacy. Nonetheless the Confederation of British Industry was successful in getting agreement from the Commission on having a business voice on the Forum.

ARTICLE 29 WORKING PARTY

On March 22nd 2001, the Article 29 Working Party adopted its Opinion 4/2001 on the Council of Europe Draft Convention on Cybercrime. It also reserved the right to issue further comment. It regretted the very late release of relevant documents and called for an extension and broadening of the debate to include all parties concerned. This Opinion comments on the text of the draft convention as published on December 22nd 2000 (version 25 public), and not on the explanatory memorandum.

The Working Party recognised the efforts being made in many areas to combat cybercrime. However, it nevertheless, gives a strong message that a fair balance must be struck between anti cybercrime efforts and the fundamental rights to privacy and personal data protection of individuals. It argued that most provisions of the draft Convention have a strong impact on fundamental rights to privacy and personal data protection.

The Working Party's suggestions for revising the draft Convention were extensive. It did, however, agree with the provision in the current draft convention that signatories not be

obliged to compel service providers to retain traffic data of all communications. This provision, the Working Party says, should remain as it is.

The Working Party stressed the Council of Europe's important role as guardian of fundamental rights and freedoms. In promoting international co-operation in matters of cybercrime outside its own membership, the Council of Europe needed to pay particular attention to the protection of fundamental rights and freedoms, especially the right to privacy and personal data protection.

The Working Party:

• called for clarification of the draft Convention because its wording was often vague and confusing. This wording might not qualify as a sufficient basis for relevant laws and mandatory measures that lawfully limit fundamental rights and freedoms. Explanations in the explanatory memorandum, the Working Party argued, cannot replace legal clarity of the text itself.

• called for a more substantial justification for the measures envisaged in terms of necessity, appropriateness and proportionality. It noted that some elements of the draft Convention are completely new and their impact on the right to privacy and data protection may not have been sufficiently evaluated by the committee of experts on crime in cyber-space (PC-CY). One of the basic questions in this respect was whether a measure is necessary in a specific case. If it is, is the measure appropriate, proportionate and not excessive?

• strongly recommended that the draft Convention contain data protection provisions outlining the protections that must be given to those whose information will be processed. These would help to codify and clarify the requirements of necessity, appropriateness and proportionality required by the "acquis"* of the Council of Europe and EU Member States.

• suggested that signatories to the Convention be invited to sign Convention 108 on the Protection of Individuals with regard to Automated Processing of Personal Data.

The Working Party also identified a discrepancy in treatment of Council of Europe countries and others because Council of Europe members have to respect their obligations: Human Rights, Convention 108, relevant Council of Europe Recommendations, the EU Charter on Fundamental Rights, the EU Data Protection Directives and relevant national legislation. Under the current draft Cybercrime Convention, countries outside the Council of Europe do not have the same or similar obligations.

Finally, the Working Party regretted that no provision is made in the draft Convention on the "incrimination of violations" of data protection rules. It also called for signatories to the Convention to ensure that the fundamental rights of individuals are adequately protected once data concerning them have been received from the European Union and Council of Europe member countries.

The Working Party maintained that a large number of the deficiencies it highlighted appeared to result from the Council of Europe's failure to make the best possible use of the expertise available in data protection matters. The Working Party invited the Council of Europe, and especially the EU Member States, to consult their data protection experts before finalising their position on the draft Convention.

**"acquis" shortened from "acquis communautaire" meaning all the legal provisions of the relevant institutions binding their members.*

The Global Internet Liberty Campaign's letter can be found at: http://www.gilc.org

The 24th draft of the Cybercrime Convention is at: http://conventions.coe.int/treaty/EN/cadreprojets.htm

The Working Party opinion can be found at the following website: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

Continued from page 10

that rules would be needed soon for what he called the "Wild West that's out there" in new surveillance technology. He also conceded the increased risk of privacy invasion but cited growing American criticism of "our extremely porous border" and Canada's reputation as "a gateway for illegal immigration, which has certainly raised the political temperature in the US."

Morden said Canada's borders must tighten even while budgets are cut. Biometric techniques like face-scanning seem a ready-made answer because they require fewer staff and thus save money.

Canadians may be ready to accept some applications of the technology. Already some businesses are reportedly using face scans to confirm customers' identity, including as a security check at some automated banking machines. But general use of face scanning is unlikely to pass muster of either existing privacy laws or individuals' privacy sensibilities.

A copy of the report is available on the Commissioner's website at http://www.ipc.on.ca