

Annual Report on Loss of Privacy Since September 11

Governments around the world have restricted privacy and increased surveillance in response to the terrorist attacks of September 11, according to a report released by Privacy International and the Electronic Privacy Information Center (EPIC). The 393-page annual report covers 50 nations and is the first survey of the changes to worldwide privacy rights since the September 11 attacks.

Titled "Privacy and Human Rights: An International Survey of Privacy Law and Practice," the report details four major trends affecting privacy rights and civil liberties: increased communications surveillance and search and seizure powers, weakening of data protection regimes, increased data sharing, and increased profiling and identification.

According to the report, almost every country that reacted to the terrorist attacks increased police and government powers to intercept communications and to engage in searches and seizures. Due process requirements were loosened in Canada, and in the United States, the USA PATRIOT Act, passed on Oct. 26, 2001, extended federal wiretapping laws and eased the use of Carnivore-style Internet surveillance technology. (See "The USA PATRIOT Act: How Patriotic Is It?" in the Winter 2002 *Silha Bulletin*.)

In Australia, attempts to pass a law that would allow police to intercept e-mail and voice mail messages without a warrant failed, although the Government plans to continue to push for this type of provision in future legislation. In addition, the report observes that France expanded police search powers to allow warrantless searches of private property and Germany expanded police authority to intercept communications.

Data protection laws in Europe were also weakened, the report states. The European Union adopted the Electronic Communications Privacy Directive in June 2002, which allows EU member states to enact laws requiring Internet Service Providers to retain communications data. Such data includes mobile phones, text messaging, land-line telephones, faxes, e-mails, chat rooms, the Internet, and any other electronic communications device. Several countries have adopted such laws, including Belgium, France, Spain and the United Kingdom. (See "European Union and Web Site Users," in the Summer 2002 *Silha Bulletin*.)

Data sharing also increased, the report observes, both within and across government agencies, and within the private sector. In the United States, data sharing has increased between the Federal Bureau of Investigation and the

Central Intelligence Agency. Efforts to increase data sharing also occurred in Canada and the United Kingdom. The report notes that "Germany has recommended to the European Union the creation of a database of "known trouble-makers."

Profiling and identification efforts have also increased, in tandem with the increased data sharing, says the report. Some airports have installed face-recognition technologies, and identification cards have been proposed in both the United States and the United Kingdom.

The report singles out Great Britain because of what it calls an "anti-privacy 'pathology' within government," and reported mass surveillance of the general population in that country.

Privacy is not suffering worldwide, according to the report. Efforts to pass data protection laws and amend current laws to strengthen protections continue in Eastern Europe, Asia, and Latin America. The report also documents the bolstering of workplace privacy laws within the past year. Finland, Sweden, the United Kingdom, the European Union and Hong Kong have either passed or are working on laws that will protect privacy in the workplace.

EPIC is a public interest research center in Washington, D.C. Privacy International is a human rights group based in London. The survey is available online at <http://www.privacyinternational.org/survey/phr2002/>.

— Kirsten Murphy
Silha Fellow