

Protecting Privacy in the Information Society



Communications Data Retention policies are invasive, illegal, illusory and illegitimate.

Privacy International

European Digital Rights

The Council has ordered the Parliament to pass a directive on "retention of data processed in connection with the provision of public electronic communication services". **But according to human rights groups and the European Data Protection Commissioners, the Commission's directive would be:**

Invasive

Information will be retained on every phone call we make, every location we travel to, every communications service we use, every e-mail we send and receive, and more. Never before have democratic governments had such information at their fingertips. And yet weak safeguards would apply to their use of this information. The Council is resisting attempts to ensure that this data is retained and accessed only in serious investigations into organised crime and terrorism.

Illegal

The European Convention on Human Rights guarantees every individual the right to respect for his or her private life, subject only to narrow exceptions where government action is imperative. Data retention results in the collection of vast dossiers on past activities of everyone, and does so in an indiscriminate manner even while alternative means of surveillance exist that are less disproportionate. Data preservation is the chosen policy of many other governments around the world, e.g. in the United States. This 'quick freeze' method preserves only

specified data on specific individuals under a specific investigation.

Vote no to protect the privacy of European citizens, and demonstrate the value of human rights within the European Union. More information is available from

www.edri.org

and

www.privacyinternational.org

Illusory

Tracing communications data back to the individual is increasingly difficult as use increases of pre-paid mobile phones, open wireless hubs, and countless smaller devices. To ensure its value this policy regime would require the registration of every Internet user, blocking of every open network, registration of the identity of all mobile phone users, the logging of ID numbers at cybercafés and libraries, and forcing Europeans to only use EU-based mail providers. We should be promoting the growth and development of the IT sector and use of telecommunications devices, not blocking it with burdensome policies.

These policies are also likely to be circumvented through something as simple as the sharing of Hotmail or Gmail accounts. As Heinz Kiefer, the president of EuroCop notes on data retention: "The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them."

Illegitimate

Data retention has been rejected by the U.S., Canada and the Council of Europe. European opposition has been high, and the arguments against reasoned and justified. European Digital Rights and XS4ALL have launched an online petition (with confirmed signatures) that already has attracted over 56,000 public signatures, see: www.dataretentionisnosolution.org.

The Commission and the Council are sweeping these concerns aside and calling for harmonising measures to increase surveillance while failing to harmonise safeguards against abuse. They claim that retention is spreading across Europe: less than five countries have some form of mandatory data retention in place. The Council is asking the European Parliament to approve a regime that parliaments in the Member States have already rejected.

This is the first time in history that human activity potentially generates such vast logs. Many of these logs are already available for law enforcement purposes as long as the telecom industry retains them for business purposes. Governments are now trying to ensure that even greater stores of information are made available, including internet data, thus registering all of our **movements, interests, and associations**. Yet the Council continues to reject safeguards such as restricting the scope of retention, minimising the harm to service providers, limiting access, ensuring judicial authorisation and adequate oversight.