Stop data retention

Reject the 'Directive on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services'

Съхраняването на данни не е решение! Pastrarea datelor de trafic nu este o solutie! Сохраненние данных – это не решение! Hramba prometnih podatkov ni rešitev! La retenció de dades no és la solució! Η κατακράτηση τηλεπικοινωνιακών δεδομένων δεν είναι λύση!Datuen gordetzea ez da konponbidea!

I. The Directive *invades* the privacy of all Europeans.

II. The Directive is *illegal* under the European Convention on Human Rights.

III. It *threatens* consumer confidence.

IV. It *burdens* European industry and harms global competitiveness.

V. The Directive *requires* more invasive laws.

De bewaarplicht is geen oplossing! La rétention de données n'est pas une solution! Teletietojen tallennusvelvollisuus ei ole ratkaisu! Data retention är inget svar!

December 6, 2005

Open Letter to all Members of the European Union,

We the undersigned are calling on you to reject the 'Directive of the European Parliament and the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC' when it comes to a plenary vote on December 12, 2005.

Adopting this Directive would cause an irreversible shift in civil liberties within the European Union. It will adversely affect consumer rights throughout Europe. And it will generate an unprecedented obstacle to the global competitiveness of European industry.

A Directive Fraught with Problems

In the Information Society every human action generates transaction logs. Our movements, our purchases, and our interactions with others can be routinely logged in public and private sector databases. In recognition of this, the European Union led the world in establishing a data privacy regime to limit the collection, processing, retention, and accessing of this information. Now the Council is demanding that the European Parliament reverse its position and lead the world in introducing mass surveillance of our activities.

Under existing EU law many of these logs are already available for law enforcement purposes for as long as the telecom industry service providers retain them for business purposes. Justice and Home Affairs officials are pushing to make available even greater stores of information.

More than 58,000 Europeans have signed a petition opposing the Directive. A German poll revealed that 78% of citizens were opposed to a retention policy.

The Directive proposes the collection of information on everybody's communications and movements. The storage of such "communications traffic data" allows whoever has access to it to establish who has electronically communicated with whom and at what time and at which location, over months and years.

In recent meetings with the Justice and Home Affairs Council on 1 and 2 December 2005, it appears that the European Parliament suddenly agreed to the collection of information on everybody's communications and movements for very broad law enforcement purposes, in spite of having rejected this policy twice before.

An Illegitimate Process

Proponents of retention policy are sweeping these concerns aside and are harmonising measures to increase surveillance while failing to harmonise safeguards against abuse. European opposition has been high, and the arguments against reasoned and justified. The continued life of this policy in Europe is inexplicable save for the illegitimate policy process that is being pursued by the policy's proponents.

These proponents claim that retention is spreading across Europe. In fact, less than five countries have some form of mandatory data retention in place, and even fewer apply the practice to internet services.

The Council is demanding that the European Parliament approve a regime that parliaments in the Member States have already rejected. For instance the UK Presidency is proposing a policy that has already failed in the UK Parliament. The Council is trying to make the Parliament complicit in this act of policy laundering.

A Key Moment

As the EU embarks on this unprecedented policy, we are facing a momentous decision as to whether we wish to set in motion a chain of events that will lead to a surveillance society.

Once a surveillance regime begins it always expands. As the European Data Protection Supervisor has stated in his opinion, the mere existence of data might lead to increased demands for access and use by industry, law enforcement authorities, and intelligence services. Already, restrictions agreed on in the Committee for Civil Liberties were pushed aside in secret negotiations with the Council.

Though the Council claims retention will combat terrorism, for years it has rejected limiting the legislation to such investigations. Even if access to this data were limited by the Parliament to a list of serious crimes nothing prevents the expansion of this list: already the Copyright Industry has called for access to this data to combat file-sharing online.

Any reimbursement of costs to service providers, like most other surveillance cost-recovery experiments, will likely be temporary. Eventually the costs and burdens generated by this policy will be seen as 'the cost of doing business' and will be passed on to individual consumers as 'the cost of communicating in Europe'.

The only way we can prevent this chain of events is by following the example of other countries around the world and to reject this policy in its entirety.

Promises are Not Enough

The European Data Protection Supervisor and the Article 29 Working Party of European Privacy Commissioners, as well as the European Parliament itself, have repeatedly stated their convictions that the case for retention has not been made. And their calls for standards and necessary safeguards have gone unheeded. The concerns of civil society and the telecommunications industry have also not been adequately addressed.

This policy continues only due to secret processes, agreements established without scrutiny, and through fast-tracking of debate because the Council fears open and democratic discussion on these matters. This is evidenced by the lack of similar policies in Member States where Parliamentary scrutiny is constitutionally required.

The EU should follow the example of open and democratic countries that have instead chosen to implement a preservation regime where data is collected and retained only for a specific investigation and then is accessed through court orders.

We, the undersigned, call on Members of the European Parliament to recognise the significant threat to European civil liberties, consumers, and industry and to therefore reject the Directive on communications data retention.

Gus Hosein, Privacy International
Sjoera Nas, European Digital Rights
Foundation for a Free Information Infrastructure
Statewatch

Associação Nacional para o Software Livre (PT)
Association for Progressive Communications (International)
Bits of Freedom (NL)
BlueLink Information Network (BG)
Bürgerrechte & Polizei/CILIP (DE)
Bulgarian Institute for Legal Development (BG)
CPSR (International, Canada and ES)
Coopération-Solidarité-Développement (FR)
Deutsche Vereinigung für Datenschutz e.V. (DE)
Digital Rights Denmark (DK)
Digital Rights Ireland (IE)
Changenet.sk (SK)
Chaos Computer Club (DE)
Consumentenbond (NL)
EDRI-observer Aljaz Marn, privacyblog.net (SL)
Electronic Frontier Foundation (US)
Electronic Privacy Information Center (US)
Emancipation syndicale et pédagogique RP (FR)
European Federation of Older Persons (EU)
Fairfax County Privacy Council (US)
Fédération Informatique et Libertés (FR)
Fitug e.V. (DE)
FoeBuD e.V. (DE)
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (DE)
Foundation for Information Policy Research (UK)
Foundation Metamorphosis (MK)
Fundacio Escula Latinoamericana de Redes (Venezuela and IT)
GreenNet (UK)
Helsinki Foundation for Human Rights (PL)
Internet Society Bulgaria (BG)
Internet Society Poland (PL)
IP Justice (US)
IRIS - Imaginons un réseau Internet solidaire (FR)
ISPO, Internet Service Providers Association (NL)
Iuridicum Remedium (CZ)
Joint Declaration on Data Retention (DE)
Netzwerk Neue Medien e.V. (DE)
Öko-Referat, Ruhr-Universität Bochum (DE)
Open Rights Group (UK)
OpenSky (CH)
Option consommateurs (Canada)
Pangea.org (ES)
Privacy Activism (US)
Privacy Commissioner Schleswig-Holstein (DE)
Privacy Rights Clearinghouse (US)
PROSA - Forbundet af It-profesionelle (DK)
Public Interest Advocacy Centre (Canada)
quintessenz (AT)
Stand (UK)
Stichting Vrijschrift (NL)
Stop1984 (DE)
Strawberrynet Foundation (RO)
Swiss Internet User Group (CH)
ver.di Fachgruppenvorstand Banken (DE)
VIBE!AT (AT)
The Winston Smith Project (IT)
Transnational Radical Party
XS4ALL (NL)
Xtended Internet (NL)
Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (DE)
Unimondo Italy (IT)

KEY PROBLEMS

I. INVASIVE
The Directive calls for the indiscriminate collection and retention of data on a wide range of Europeans' activities. Never has a policy been introduced that mandates the mass storage of information for the mere eventuality that it may be of interest to the State at some point in the future.

II. ILLEGAL
It contravenes the European Convention on Human Rights by proposing the indiscriminate and disproportionate recording of sensitive personal information. Political, legal, medical, religious and press communications would be logged, exposing such information to use and abuse.

III. THREATENS CONSUMER CONFIDENCE
It will have a chilling effect on communications activity as consumers may avoid participating in entirely legal transactions for fear that this will be logged for years. This could damage nascent markets in services such as location-based services.

IV. HARMS INDUSTRY
Creates additional costs of hundreds of millions of Euros every year. These burdens are placed on EU industry alone. The U.S., Canada and the Council of Europe have already rejected retention. Repeated concerns from industry in the U.S. has led to an even stronger set of safeguards, while three court decisions have called for added safeguards to policy access to location data.

V. INCOMPLETE
To be effective, there will be calls for additional draconian measures including:
- identification of all those who communicate, requiring ID cards at cybercafés, public telephone booths, wireless hotspots, pre-paid services
- banning use of international communications services such as webmail (e.g. Hotmail and Gmail) and blocking the use of non-EU internet service providers and advanced corporate services.