Briefing for Members of the European Parliament on Data Retention

September 26, 2005

Dear Members of the European Parliament,

We would like to take this opportunity to address you regarding the current proposals on communications data retention. As you are well aware, both the Council and the Commission have put forward proposals on data retention. It now appears that the policy is finally shifting to the first pillar away from the third. This does not mean that the policy has improved. Despite many edits over the last two years, both the Council and the Commission proposals continue to be invasive, illegal, illusory and illegitimate.

These proposals continue to require the collection and logging of every telecommunication transaction of every individual within modern European society. Almost all human conduct in an information society generates traffic data. Therefore traffic data can be used to piece together a detailed picture of human conduct.[1] Under the various proposals, this data will be kept for between six months and four years.

There are clear challenges for these proposals with respect to the European Convention on Human Rights, the European Charter on Fundamental Rights and national constitutions. The case still has not been made that retention is necessary in a democratic society.[2] The claimed need for harmonisation is premature at best and challenges democratic process.

Invasive

The Council and the Commission both acknowledge that the retention of traffic data is an intrusion upon the privacy rights of the individual. Over the years the proposals have been modified in recognition of this intrusion.[3]

The type of data collected under the proposed retention schemes will create a map of all of our contacts and relationships over a period of at least one year. Information will be retained on every phone call we make, every location we travel to, every communications service we use,

---

[1] The Commission claims that traffic data is the digital equivalent of fingerprints. But our fingerprints are not retained by default; nor do they pinpoint our networks of friends, colleagues, activities, and movements.

[2] The European Data Protection Supervisor reached a similar conclusion in his assessment, "Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM (2005) 438 final)", available at http://www.edps.eu.int/legislation/Opinions_A/05-09-26_Opinion_data_retention_EN.pdf

[3] Some may now argue that the mere collection and retention of this data is not an intrusion upon the private lives of individuals and instead only access to this information is problematic. Such an argument would not reflect the law, nor does it reflect the clearly stated positions of both the Council and Commission proposals.

every email we send and receive, and possibly more. This information will be kept to make a future judgement about us.

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 demanding that data be retained for one year, though Member States may demand longer periods up to four years. The Commission proposal establishes two retention regimes, with one year for telephone and mobile services, and six months for Internet services.

The UK Presidency has promised that with respect to the Internet the Council proposes only to collect data regarding log-ins and log-offs. The Commission definition is far more invasive than the Council proposal. The Commission defines 'communication' as involving "any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service". Therefore the Commission is proposing the tracing of all forms of Internet transactions. This means that communications service providers could be compelled to store their mail server logs, web cache logs, and IP flow logs[4] for six months without any regard to necessity or proportionality.

Illegal

The privacy of communications is given a high standard of protection in international human rights instruments and in many national constitutions. Communications secrecy is necessary for a functioning society.

All parties agree that the collection and retention of information creates challenges for the right to privacy enshrined in Article 8 of the European Convention on Human. Proponents of retention emphasise that safeguards are only required for access to this data. That is, they do not believe that the act of retention is an intrusion upon the privacy rights of individuals. The European Court of Human Rights appears to disagree with this interpretation.

Article 8 guarantees every individual the right to respect for his or her private life, subject only to narrow exceptions where government action is imperative. This interference with the privacy rights of every user of European-based communications services cannot be justified under the limited exceptions envisaged by Article 8 because it is neither consistent with the rule of law nor necessary in a democratic society. The indiscriminate collection of traffic data offends a core principle of the rule of law: that citizens should have notice of the circumstances in which the State may conduct surveillance, so that they can regulate their behaviour to avoid unwanted intrusions. Moreover, the data retention requirement would be so extensive as to be out of all proportion to the law enforcement objectives served.

The European Court of Human Rights has ruled that the recording of traffic data is a violation of Article 8 rights.[5] The Court also found that the storing of records on past activities constituted an interference.[6] The Court also deems surveillance as unlawful if it was indiscriminate and lacked

---

[4] This involves both packet level data on source, destination, traffic type, etc. and the flows of these packets. It is common to collect this data for short periods (and often on a statistical basis) in order to spot denial of service attacks, to assess link usage and other network management reasons. Even though this information is collected and kept for a short period of time, under the Commission proposals it would have to be kept for six months.

[5] in the case of *Amann v. Switzerland*

[6] in *Rotaru v. Romania*

a specific regime of regulation.[7] Lawful surveillance can only take place when there are effective safeguards in place to ensure minimum impairment to privacy, and alternative means are exhausted.[8]

Data retention necessarily involves an intrusion upon the private life of an individual; 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.

One of the greatest flaws of these retention proposals is that the grounds for accessing the retained data remain obscured. In the Council's Framework Decision, it is promised that this data will be accessed in accordance with national law in a proportionate manner. But the Framework Decision does not prescribe any guidelines for national law nor a proportionality test. This data is stored for the wide set of purposes of "investigation, detection and prosecution of crime and criminal offences including terrorism", leaving little constraint of national law. This is consistent with existing national policies on retention. For instance in the UK traffic data may be accessed by almost every government body, including local councils and the environment agency.

On the other hand, the Commission proposes that the stated purpose of retention is to ensure that data is available for the "prevention, investigation, detection and prosecution of **serious** criminal offences, such as terrorism and organised crime". What constitutes 'serious crime' leaves much to the imagination, particularly as Commission documents note that retention will be of use for cybercrime investigations, international investigations that are renown for lacking dual criminality tests[9] and for investigating "intellectual copyright infringements" (sic).[10]

Even as the Commission moves forward on harmonisation of retention it doesn't appear to have produced the necessary research to understand the variety of existing access powers within Member States. Before the Parliament approves a measure that would vastly increase the data stores at the disposal of government departments across Member States, we would expect an evaluation of the differences in national laws and practices.

The indiscriminate retention of vast stores of information on everyone in Europe with unclear safeguards and limited means of regulating access leaves the Commission's proposal in problematic legal territory. It is likely that an EU policy on data retention will lead to a number of court cases in Member States and EU courts.

Illusory

Though there are vast amounts of information generated by activity on modern communications networks, linking this information to individuals' actions is not simple. The illusion of benefits to security must be confronted with some realities. First, traffic data does not easily link to individual conduct. Second, this policy is linked with the increased identification requirements. Finally, there are also significant technological and financial ramifications.

---

[7] *Kruslin v. France*, *Amann v. Swizerland* and *Kopp v. Switzerland*
[8] *Foxley v. United Kingdom*
[9] This is why the Council of Europe Convention on Cybercrime enables the power of expedited preservation.
[10] Commission Staff Working Document, Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, EXTENDED IMPACT ASSESSMENT, {COM(2005) 438 final}, page 5.

Linking an individual to a set of actions, recorded in logs, is increasingly difficult. Both the Council and the Commission propose the retention of tracing data, but tracing the individual log data back to the individual is increasingly difficult particularly as use increases of pre-paid mobile phones, open wire-less hubs, and countless smaller devices to interact with others across jurisdictions. It is increasingly difficult to ensure that communications data retention has investigative and evidentiary value. To ensure its value 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 (banning the use of Gmail, Hotmail, and other such services).

The ever-increasing volume of telecommunications data is one of the reasons why there has been no serious data retention proposal made in the US. National Security Agency director Lt. General Michael Hayden noted in 2001 that "Today there are over 180 million computers — most of them networked. There are roughly 14 million fax machines and 40 million cell phones, and those numbers continue to grow."[11] Realising the extensive burden this would place on US industry, the US Department of Justice has instead adopted powers allowing for the preservation of specific information on specific users under investigation.

The Commission and Council proposals would therefore place European residents and industry at a global disadvantage. EU-based mail providers would have to retain logs of e-mails sent and received while US-based providers would not. Multi-national service providers may not invest in European infrastructure due to the additional costs.

The Commission documentation claims that industry is demanding harmonised retention policy. This is an absurd claim. To date we have not seen lobbyists from communications service providers calling for the implementation of retention rules in countries that are currently without. No amount of harmonisation will solve the problem that companies outside the EU will not have to comply with retention requirements.

There are additional burdens on industry within both proposals. The Council proposal foresees retained data being accessed by all EU Member States upon request for investigation into any criminal activity, yet also requires that the data be kept secure with 'technical and organisational measures' to protect against accidental or unlawful access, loss, or destruction. The Commission proposal requires that this data is stored "in such a way that it can be transmitted upon request to the competent authorities without undue delay". These regulatory and design burdens will involve substantial costs.

The Commission proposal does call for the reimbursement for compliance with the draft directive. This would not account for an increased cost of operation, higher compliance risks, and challenges to smaller enterprises. The money disbursed will still come from European citizens, while gains are unclear and unsubstantiated.

In the Commission's impact analysis the reported costs for retention continue to vary widely, ranging from hundreds of thousands of euros for each telephone and mobile phone provider according to government estimates to hundreds of millions of euros for each network provider according to industry estimates. More research is required before the Parliament even considers a proposal that could affect European industry and users so greatly.

---

[11] James Bamford. Eyes in the Sky, Ears to the Wall, and Still Wanting. New York Times, 8 September 2002. Available from http://www.mindfully.org/Reform/2002/Terrorism-Dumb-Luck-Technology8sep02.htm

Illegitimate

Data retention is not a new policy. In fact it has been tried and has failed in a number of jurisdictions around the world. Now the European Parliament is being asked by the Commission to be complicit in the act of policy laundering: to pass laws at the EU level that failed in Member States.

The UK Government failed to achieve a mandatory regime in Britain after September 11, but is now seeking such a regime at the EU level. The German Parliament and the Dutch have voted to prevent their interior ministers from agreeing to the Council proposals. The Irish Justice Minister admitted that he was waiting for the 'EU cavalry' to come to his aid but when it did not, he was forced to rush telephone data retention through the Irish Parliament.[12]

The Commission argues that harmonisation is the key purpose for the directive. However, the majority of Member States do not have mandatory data retention obligations. Even fewer have functioning regulatory regimes for actually implementing data retention.[13] Existing retention periods vary widely (between three months and four years) as does the scope of retention, where some require just pre-paid mobile, others just telephone, etc. Yet the European Commission seems intent on harmonising a failed and yet broad policy. And the Commission is asking for the European Parliament's approval in this venture.

When the Council of Europe was drafting its cybercrime convention it specifically avoided data retention. There is no data retention in the United States and Canada. In fact, data retention policy seems mostly limited to Europe. Although Argentina has passed a retention law, the Argentinean government suspended that law in May 2005. Retention is an unpopular policy that few countries have and fewer want.

The European Commission contends that it performed a consultation and the results were in favour of retaining data for six months. For years the Commission has been discussing retention, and for years the opposition to the regime has prevented its implementation. Last year the Commission consulted on the Council's Framework Decision and received many responses, including one response that was endorsed by 190 industry and non-governmental organisations. That response was clear in its opposition to data retention. The Commission then reported that these responses all supported a six-month regime.

Both the Council and the Commission proposals are sullied by unaccountable and undemocratic procedures. The Council proposal acknowledges that some countries may retain data for four years and others only for six months. If countries opt for six months, however, the Council **requires** a 'national procedural or consultative process' and a review every five years. No national consultation is required to implement retention for one to four years. Meanwhile, the Commission proposal enumerates the data to be retained but proposes the creation of a Committee that will in the future decide what additional types of data must be retained because of the 'fluid nature' of technology.

The European Parliament is thus being called on to approve a policy that has failed elsewhere. Deliberation on data retention has not often occurred at the national level, and little debate has occurred at the level of the EU. Where these debates have taken place opposition was high, and

---

[12] Mr. Michael McDowell: "There is no EU cavalry coming down the hill to help me. I must sort out this conflict." Stated in Seanad Debate, Volume 179 No.4, February 3, 2005.

[13] less than half, according to impact assessment, p.6.

the arguments against were reasoned and justifiable. The Commission and the Council are sweeping these concerns aside and are promoting bad behaviour by calling for harmonising measures to increase surveillance while failing to harmonise safeguards against abuse.

Concluding Remarks

Data retention is a large and complex policy. In this briefing we have highlighted four problematic areas. But data retention is not just invasive, illegal, illusory, and illegitimate. It is bad policy with no clear goals.

Clear and open debate and deliberation has proven problematic for the governments who are seeking retention. This is why a harmonising measure is now being sought: in order to overcome all prior opposition and place blame on the 'unaccountable institutions' of the EU. Governments will return to their national parliaments claiming that they are compelled to introduce the illiberal practice of data retention because of EU obligations.

Proponents of retention believe that they have made the case for this policy. When the UK Presidency of the EU attempted to justify retention policy it pointed to cases of terrorism, murder, and torture. The UK Presidency argued that retention is used in serious crimes and cases involving terrorism, but failed to note that the language of the Framework Decision, and UK law, permitted its use for all investigations by many government departments. In all but one of the example cases presented by the UK Presidency, investigators would have had access to the data without any need for a retention policy.

Both the Commission and the Council cite a recent study on retention that although the vast majority of the retained data sought for investigations was less than six months old, "where data between 7 and 12 months old was required, it was used to investigate the most serious crimes, mostly murder". They both fail to clarify whether the sought data was conclusive evidence for the investigations or merely useful. With the billions of euros that will be required to implement data retention stronger evidence is required on the likely effectiveness of the scheme.

But it is not just a matter of cost-benefits. Despite the illusory gains described above, the retention of communications traffic data may be of use in some investigations. This is true of any invasive collection and retention of any form of personal information, whether fingerprints, DNA, medical records, financial records, religious information, travel details, sexual preferences, etc. All of this information could be kept indefinitely to aid the police in investigations, and the data would likely be of some assistance.

Therefore the European Parliament now faces a crucial decision. Is this the type of society we would like to live in? A society where all our actions are recorded, all of our interactions may be mapped, treating the use of communications infrastructures as criminal activity; just in case that it may be of use at some point in the future by countless agencies in innumerable countries around the world with minimal oversight and even weaker safeguards.

These proposals before you now are less invasive than previous versions. But they allow retention policies to be changed with minimal democratic scrutiny to include greater information storage. This is not a matter of the 'slippery slope' or 'thin end of the wedge'; but this will transform European law in an unprecedented manner. If the European Parliament approves data retention with even the strongest safeguards, it cannot prevent future Parliaments from undoing those safeguards.

We are already seeing Member State law that abandons the proposed safeguards. For instance, it is unlikely that the UK government will follow demands from the Commission to change existing British law to enhance safeguards on access to information. However, it is likely that the UK government will introduce mandatory data retention in accordance with EU obligations when it previously only managed to convince Parliament on a voluntary regime.

We the undersigned therefore call on the European Parliament to reject the Council and Commission proposals as an infringement of the civilised values and respect for human rights that underpin the European Union.

Gus Hosein, Privacy International

Sjoera Nas, European Digital Rights

Endorsing Organisations

Association Electronique Libre, Belgium
BBA Switzerland
Bits of Freedom, the Netherlands
Chaos Computer Club, Germany
Computer Professionals for Social Responsibility - ES, Spain
Digital Rights, Denmark
EFFi, Finland
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung, Germany
Foundation for Information Policy Research, UK
GreenNet, UK
ISOC-Bulgaria
Open Rights Group, UK
Privacyblog.net, Slovenia
Netzwerk Neue Medien, Germany
quintessenz.org, Austria
Stand.org.uk, UK
Statewatch, UK
Stop1984, Germany
Swiss Internet User Group, Switzerland
VIBE!AT, Austria

Appendix: Comparison of Council Framework Decision and Commission Directive

Council Proposal	Commission Proposal
Data to trace and identify the source and destination • telephone and mobile services: calling phone number, user name and address • internet access and internet communication services: User IDs allocated, User ID and telephone number, name and address of subscriber/user and the IP address and telephone number at the time of communication	Data to trace and identify source and destination • telephone and mobile services: calling number and subscriber information • internet access, internet e-mail and internet telephony: IP address, UserID of source, connection label/telephone number associated to any communication entering the public telephone network; subscriber details
Data to identify date, time and duration, including internet log-in and log-off	Data to identify date, time duration, including log-in and log-off of internet sessions
Data to identify type of communication, including the services used	Data to identify the type of communication, including voice, conference call, fax, SMS
Data to identify users' communication equipment "or what purports to be their equipment", including IMEI, IMSI, and MAC address	Data to identify communications device, including IMEI, IMSI, and MAC address
Data necessary to identify the location of mobile equipment • location label (CELL ID) at start and end • data identifying by reference to cell IDs the geographic location of cells during the period for which communications data is retained	Data necessary to identify the location • Cell ID • data mapping between cell ID and geographical location