Joint Declaration on Data Retention

As representatives of citizens, professionals and businesses in Europe and world-wide,

Convinced that the recognition of inalienable human rights is the foundation of freedom, security and economic prosperity,

Concerned that in the fight against terrorism and crime we are giving up the values we are trying to protect, namely freedom and democracy,

Considering that current plans to record information on every citizen's communications, movements and use of media may constitute the most serious threat yet to our right to live self-determined and private lives,

we declare the following to be our profound belief:

1. The systematic collection or retention of personal data regarding our communications, movements or use of media ("data retention") beyond what is necessary for business purposes is unacceptable. We demand that any plans to introduce data retention be halted immediately.

2. The following reasons have led us to this conclusion:
   - Data retention is too invasive to personal privacy. It obstructs professional activities (e.g. in medicine, law, religion, journalism) as well as political and commercial activities that rely on confidentiality.
   - Data retention does not prevent terrorism or other types of crime; it is unnecessary and easy for criminals to circumvent.
   - Data retention violates the human right to privacy and control of personal information.
   - Data retention is expensive and burdens the economy.
   - Data retention discriminates against users of telephones, mobile phones and the Internet.

3. Any legal rules on the handling of communications data must be subject to prior parliamentarian consent. Providers must be reimbursed for additional costs they incur in complying with law enforcement-related obligations.

~

Explanatory Notes

1. Data retention is too invasive to personal privacy; it obstructs professional activities (e.g. in medicine, law, religion, journalism) as well as political and commercial activities that rely on confidentiality

1.1. Data retention creates detailed records of our private lives

The storage of communications data allows whoever has access to it, to establish who has electronically communicated with whom and at what time. In the case of mobile phones, the geographical movements of the owner can be tracked as well. As far as the Internet is concerned, all information viewed, downloaded or submitted by a particular person can be re-established. The systematic collection of communications data is likened to a police agency that follows us around the clock and notes who we telephone and at what times, which places we go with our mobile phones in the pocket, and what we do on the Internet.

In view of the privacy implications of communications data, current EU legislation permits the retention of communications data only where it is needed for billing purposes. Citizens, professionals and businesses can therefore prevent or minimize the storage of communications data by using flat rate tariffs, pre-paid or free services. However, EU proposals are now being considered which would result in the mandatory systematic retention of communications data concerning all kinds of telecommunications for a period of six months or more, in order to permit possible access by law enforcement and security agencies (“data retention”).

Today, a great amount of social interaction is taking place via telecommunications networks. Retaining all communications data would create a detailed map of our private lives. Communications data reflects an important part of our daily actions, habits and routines: which friends, professionals or businesses we contact, which places we visit, which information we read on the Internet. It may also reveal information about our political, financial, sexual or religious stance. Besides our habits, changes in our routines and other unusual behaviour can be detected as well.

Since the information value and usability of communications data is so high, its systematic retention has been labelled ”CCTV inside your head” or ”electronic diary”. Systematically storing communications data, as envisioned by the EU, would create the most comprehensive records in history of the private and professional lives of millions of citizens in the EU.

1.2. Retained data can cast suspicion on every citizen

Data retention can adversely affect every one of us. Anyone with a remote connection to a criminal or a suspected criminal can become a suspect themselves and, as such, be subjected to interrogation, to observation, to neighbourhood and employer questioning, to searches and to arrest. Communications data has, in the past, led to all of these measures being taken against innocent citizens. For example, there have been cases of criminals using mobile phones or Internet accounts of innocent citizens and thus linking these citizens to crimes. As communications data is readily accessible to the authorities, its systematic retention would provide a multitude of links to any crime, leading to a major increase in the risk of innocent citizens being erroneously subjected to police measures. Data retention, therefore, constitutes a real risk to every one of us.

1.3. Data retention harms relationships of trust and has a chilling effect on sensitive activities

The creation of massive databases on our communications, movements and use of media would entail a substantial danger of abuse by government agencies, government officials, telecommunications companies' personnel and others. The fact that illegal access to communications data has repeatedly happened in the past proves that the large-scale collection of sensitive data inevitably leads to abuse. There have been cases of police officers and telecommunications companies' employees selling private information to unauthorised persons and agencies. In the U.S., private investigators are openly offering communications data for sale.

Data retention would subject citizens to constant fear that sensitive information regarding their private lives may at some point in the future be used against them. Anonymity is essential in many situations, which is why data retention would have a chilling effect on a wide range of activities:

1.3.1. Effect on political activities

Communications data is extremely useful for political control. It can be abused by the police or intelligence agencies to monitor the activities of any group that may come into conflict with the state or the state's opinion, even if it is merely engaging in legitimate protest. In the past, the UK police have used anti-terrorism powers against groups opposed to the war in Iraq and protesters at an arms fair. U.S. intelligence agencies have spied on legitimate activities of NGOs such as Greenpeace and the American Civil Liberties Union.

1.3.2. Effect on confidential communications with doctors, lawyers, members of the clergy, journalists etc.

Confidential telecommunications is essential to many professions and services. For example, patients consult their doctors by telephone, people who are in difficulty consult the crisis line or drug counselling web sites on the Internet. The risk of confidential relationships and contacts being exposed later on would have a deterring effect and seriously hamper activities that rely on confidentiality. Physicians, psychologists, psychotherapists, professional counsellors, social workers, members of the clergy, lawyers, accountants and journalists would be among those affected by data retention and potential dissemination of private information. As citizens can often not avoid using telecommunications and carrying mobile phones, data retention is likely to seriously obstruct the work of such professionals. Criminal investigations often depend on information given anonymously as well.

1.3.3. Effect on business activities

Communications data is extremely useful in gathering economical intelligence by foreign governments. Businesses transmit confidential data via telecommunications networks daily. The success of negotiations on major contracts or mergers often depends on the secrecy of the process. The systematic retention of communications data would entail the risk of confidential contacts or actions of business people being exposed to competitors.

1.3.4. Effect on public safety

In the event of unauthorised access to retained communications data, information on the private life of prominent members of the public could be obtained. This information could be used to blackmail or otherwise bring harm to a government official, for example. Alternatively, it could be used by stalkers or criminals to investigate potential victims. Even information regarding the communications and movements of the police, intelligence agencies and the military could be obtained.

1.3.5. Effect on society

Where data retention takes place, citizens constantly need to fear that their communications data may at some point lead to false incrimination or governmental or private abuse of the data. Because of this, data retention endangers open communications in our society. Individuals who have reason to fear that their communications could be used against them in the future will endeavour to behave as unsuspiciously as possible or, in some cases, choose to abstain from communicating altogether. This would be detrimental to our democratic society, as any democracy relies on the active and unprejudiced involvement of its citizens.

2. Data retention does not help prevent terrorism or other types of crime; it is unnecessary and easy for criminals to circumvent

2.1. Data retention is easy for criminals to circumvent

Individuals involved in organised crime and terrorism would easily find a way to prevent their communications and movements from being traced. For example, it is simple for criminals to use mobile phone cards that have been registered in the name of another person; likewise, pay-as-you-go phones, Internet cafés or offshore e-mail accounts can be used to escape detection. The President of the European Confederation of Police, Heinz Kiefer, announced in 2005 that "he is sceptical as to whether [data retention] will actually help criminal investigations. [...] [I]t remains easy for criminals to avoid detection through fairly simple means, for example mobile phone cards can be purchased from foreign providers and frequently switched. 'The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them'".

2.2. Data retention is not necessary

Effective mechanisms for the investigation of crime are already in place, including, in the field of telecommunications, the availability of a wide range of communications data. The recording of additional communications data can be ordered where needed in specific investigations. The current availability of communications data has proved sufficient in the investigation of both the 2004 Madrid and the 2005 London terrorist attacks. A need for systematically retaining all communications data is not recognised by the U.S., where some providers destroy all such data immediately after it has been generated. In a report published recently by Erasmus University in Rotterdam, researchers reviewing 65 relevant police investigations concluded that data retention was unnecessary. In just about every case, police could use existing account and billing information from service providers. Considering that serious criminals can easily prevent their data from being traced, the systematic retention of all communications data would at best be useful in the investigation of few and generally less important crimes.

A practical way of improving access to communications data is to implement mechanisms of "expedited preservation" of communications data (so-called "quick freeze") as provided for in the international Convention on Cybercrime and successfully practised in the United States. Improving international co-operation in obtaining communications data stored or generated abroad is another option. In the fight against global terrorism and organised crime, improving international co-operation promises to be much more effective than taking unilateral steps in Europe that can easily be circumvented by criminals.

2.3. Data retention does not help prevent terrorism or other types of crime

The potential of data retention to help prevent terrorism or crime is virtually non-existent. The proposed EU framework decision on data retention does not even mention crime prevention as a purpose. Massive restrictions on our civil liberties in the name of fighting crime can be acceptable only when measures are proven, by scientific and independent research, to effectively improve our safety. There is no evidence to indicate that data retention directly or indirectly lowers crime rates. In the contrary, scientific studies have repeatedly failed to find a correlation between the extent of police powers and crime rates. What can and must be done against crime and terrorism is specifically targeting its root causes, not only by repressive but also by social and political means. Substantial programmes to that end could be implemented by using only a fraction of the funds data retention would consume. Also, international co-operation is particularly important where international terrorism and organised crime are concerned.

Despite all efforts, experience has shown that the means available for preventing terrorism and crime are limited. Not only has the phenomenon of crime existed in all societies. Crime rates in western societies have also remained relatively stable for the past decades. In other words, the threat of crime we face today is roughly equal to the threat we have faced in the past, and to the threat we will likely face in the future. By creating a police and surveillance state, we would give up our liberties without improving our safety. States such as the German Democratic Republic have demonstrated that even with unlimited powers of surveillance, states cannot suppress crime. In the aftermath of the 2005 terrorist attacks on the London underground, British Prime Minister Tony Blair acknowledged that ”all the surveillance in the world" could not have prevented the bombings.

This means that we must resign ourselves to the possibility of terrorism and crime as one of the risks inherent to life. Fortunately, statistics prove that we are virtually safe from crime. According to Eurostat less than 0.002% of Europeans die as a result of crime and terrorism per year. We are far more likely to die in traffic accidents, in accidental falls, or as a result of an unhealthy lifestyle (unhealthy diets, lack of exercise, alcohol and tobacco consumption) than at the hands of a criminal or terrorist. Likewise, risks such as illness, poverty, unemployment or natural disasters are far more likely to affect us than crime.

3. Data retention violates the human right to privacy and control of personal information

Weighing the conflicting rights and interests proves a significant disparity between the possible benefit of data retention and its negative effects, both on individuals and on society as a whole. Data retention is a disproportionate and illegal restriction of the right to privacy as guaranteed in Article 8 of the European Convention on Human Rights. The

systematic retention of communications data threatens to inflict great damage on society, while its potential benefit is marginal. It is excessive to record information on everybody's communications and movements when only a small fraction (0.0004% according to statistics by a large German Internet provider) of this data could be of use in future criminal investigations. This assessment applies irrespectively of retention periods and the types of data to be retained. Of the innumerable telecommunications taking place every minute, the probability of a particular communication needing to be re-visited and established as fact by law enforcement is minuscule. 99.9% of the citizens affected by data retention would be completely innocent warns Peter Schaar, chairman of the EU's Data Protection Working Party.

The European Court of Human Rights confirmed that the importance of maintaining public safety "does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such as law poses of undermining or even destroying democracy on the ground of defending it, confirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".

Privacy NGOs are rightly pointing out the following: "[Of course] 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".

One lesson the past has taught us is that protecting human rights by maintaining the historical balance of state powers and individual rights ultimately serves freedom, peace and justice in the world better than pursuing short-term gains by extending police powers. Extensive police powers create a climate of fear, distrust and hostility, especially with minorities, and provoke resistance. On the other hand, respect for freedom and privacy strengthens society's inherent mechanisms for maintaining peace and justice. In the fight against crime, we will not give up the values we cherish. Terrorists wish us to live in fear, and fundamentalists want us to give up freedom and democracy. We will not allow them to achieve their aims.

4. Data retention is expensive and harms the economy

An obligation to systematically retain communications data would place enormous burdens on the companies compelled to retain the data. Costs would result from the processing and analysis of security authorities' inquiries, technical changes to systems for data generation and storage, and changes to firms' in-house processes for secure data archiving. For each major telecommunications company, set up costs are estimated in the European Parliament report on data retention to amount to €180 million, followed by running costs of up to €50 million per year. Internet service providers would have to bear costs several times those faced by telephone companies. Small and medium-sized businesses with limited budgets would be hit particularly hard by data retention obligations. Some of them could be forced to stop operations altogether, for example providers of advertisement-financed e-mail services that would not be able to recover additional costs.

Ultimately, consumers would have to bear the cost of data retention through higher prices for telecommunications services. A German poll revealed in 2005 that 78% of users are unwilling to pay for data retention costs. Price increases of 15-20% have been predicted for some services; privacy concerns are likely to lead to a further decrease in the use of electronic communications services. These factors mean that data retention threatens to damage Europe's telecommunications and Internet industry and obstruct E-commerce. Where companies could not recoup costs for data retention from their consumers, funds would be missing for the development of product innovations. Service providers could decide to move operations to countries without data retention obligations, which would threaten jobs in the EU. Data retention laws would substantially disadvantage European telecommunications companies in competing with U.S. companies, where no data retention obligation exists or is planned. Finally, as a wide range of business activities depends on confidential communications, the systematic retention of communications data could substantially harm various sectors of Europe's economy and damage its competitiveness in the global markets.

Reimbursing providers for data retention costs can reduce the financial impact on them. However, the need to process and analyse the increased number of security authorities' inquiries, to change systems for data generation and storage and to change processes for secure data archiving would still distract them from their core business and disadvantage them in global competition. Most importantly, the impact on citizens, professionals and businesses in general would not be reduced at all. The taxpayer would be obliged to spend heavily on data retention, withholding funds from targeted projects with a proven impact on citizens' safety.

5. Data retention discriminates against users of telephones, mobile phones and the Internet

Data retention would mean recording information on communications, movements and use of media just because telecommunications devices are used. A wide range of otherwise private activities would be recorded simply because we use a telecommunications device. While we can have conversations or send letters anonymously, details of our electronic communications would be retained. While we can use public libraries, bookshops and department stores anonymously, similar activities on the Internet would be recorded. While we can generally move unnoticed, the movements of citizens who need to carry a mobile phone would be registered. The sole reason for this discrimination would be that it is technically possible to record the use of telecommunications devices, and that it can be done without our noticing it. A scheme to systematically record our behaviour outside of telecommunications networks would be unrealisable as well as clearly unacceptable as such surveillance would be permanently visible to us.

It is not justifiable to record information on generally private activities, simply because telecommunications devices are being used. This is particularly so because we can often not reasonably avoid using a telephone, a mobile phone or the Internet. In the future, telecommunications devices are likely to become omnipresent, reducing our options to avoid using them.

6. The way forward

Instead of introducing data retention, the EU should explicitly ban member states from requiring providers to retain communications data. This is the best way of harmonisation, considering that only a minority of EU member states have a retention policy and even fewer (about 5 of the 25 member states) have actually implemented data retention obligations. In addition, a common regime for the storage and preservation of communications data in specific cases (data preservation) should be introduced, as successfully practised in the U.S. and in a number of EU member states. Improving international co-operation in obtaining communications data promises to be effective as well.

Balanced solutions can be found only by means of democratic discussion in parliaments. It follows that restrictions on civil liberties based on intergovernmental agreements without prior parliamentarian consent are unacceptable. This applies particularly to the EU ministers' plan to side-step the European Parliament in the process of deciding on the introduction of data retention. Any legal rules on the handling of communications data must be subject to prior parliamentarian consent.

Furthermore, providers must be reimbursed for any additional costs they incur in complying with law enforcement-related obligations. The prevention and prosecution of crime benefits society as a whole. Therefore, its cost must be borne by the state, rather than by providers or their customers.