
**PRIVACY INTERNATIONAL**

# MEMORANDUM OF LAWS CONCERNING THE LEGALITY OF DATA RETENTION WITH REGARD TO THE RIGHTS GUARANTEED BY THE EUROPEAN CONVENTION ON HUMAN RIGHTS

**10th October 2003**

**Prepared by Covington & Burling**
**for Privacy International**

## EU DATA RETENTION LEGISLATION: A VIOLATION OF RIGHTS GUARANTEED BY THE EUROPEAN CONVENTION ON HUMAN RIGHTS

### Executive Summary: The United Kingdom

1. This Memorandum was commissioned to provide an indication of the legality of measures being undertaken throughout the EU to require the retention of communications data. The advice relates to the retention of data in a mandatory regime. The document is intended as a framework for the development of analyses more specific to national legal environments.

2. 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 behavior 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. Under the case law of the European Court of Human Rights, such a disproportionate interference in the private lives of individuals cannot be said to be necessary in a democratic society.

3. These and related protections are clearly affirmed in such cases as *Klass v. Germany, Amann v. Switzerland, Rotaru v. Romania*, *Malone v. United Kingdom, Kruslin v. France*, *Kopp v. Switzerland* and *Foxley v. United Kingdom*.

4. A number of countries in the EU have taken steps to create a legislated requirement on communications providers to store their customers' communications data for a minimum period. This analysis establishes that the fact of this blanket retention contravenes the European Convention on Human Rights.

5. Two Statutory Instruments currently before the UK Parliament would (a) establish a voluntary regime for retention and (b) extend a sunset clause within the Anti-terrorism, Crime and Security Act that would give the government authority to replace this voluntary scheme with a mandatory regime. It appears probable that such a scheme will be subject to similar, if not identical, constraints under the Convention.

6. This analysis establishes that it is the fact of blanket retention that is key to assessing the legality of the UK SI's. The impact of either a universal voluntary scheme or a mandatory regime on such guarantees as Accessibility and Foreseeability will in all likelihood bring the UK proposals into conflict with the Convention.

The text of the Memorandum begins overleaf.

## A. Summary

In the 1990s, Europe led the way in recognising how emerging technological trends threatened individual privacy and in providing countervailing protections. Since September 2001, however, security concerns have driven the European Union to water down these protections, in particular by granting Member State authorities discretion to gather data for security and criminal investigation purposes. A draft Framework Decision on data retention under discussion by EU Justice and Home Affairs Ministers would accelerate this trend dramatically. The proposed measure would oblige Member States to require communications providers to retain for up to two years traffic data relating to every communication carried, in case of need in a subsequent criminal investigation or prosecution. Some Member States already have taken matters into their own hands, and enacted data retention laws in their own right.

The data retention regime envisaged by the Framework Decision, and now appearing in various forms at the Member State level, is unlawful. Article 8 of the European Convention on Human Rights (ECHR) guarantees every individual the right to respect for his or her private life, subject only to narrow exceptions where government action is imperative. The Framework Decision and national laws similar to it would interfere with this right, by requiring the accumulation of large amounts of information bearing on individuals' private activities. 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 behavior 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. Under the case law of the European Court of Human Rights, such a disproportionate interference in the private lives of individuals cannot be said to be necessary in a democratic society.

If the Framework Decision is adopted, it would mark a dramatic departure from the European Union's formerly protective and cautious attitude towards personal privacy and data retention. Most recently, Community legislators enacted Directive 2002/58/EC[1] in mid-2002 to regulate the processing of personal data, including traffic data, on electronic networks. That Directive sensibly and prudently only permitted retention measures where "necessary, appropriate and proportionate" within a democratic society. The notion of unrestricted, blanket data retention was expressly rejected. The Framework Decision, on the contrary, would compel European

[1] Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002 O.J. (L. 201) 37-47. Directive 2002/58/EC replaced Directive 97/66/EC, which also addressed traffic data among other things.

businesses to retain communications data, thereby creating a regime far more intrusive than anything previously known in the EU or even in comparable democratic societies. By requiring the accumulation of huge stores of data traffic, containing countless items of private and personal information, it would generate opportunities for abuse by public authorities or private actors, such as hackers. Further, the additional regulatory burdens imposed by such a regime would be costly and would adversely affect the competitiveness of telecommunications and network service providers in Europe.

### B. The Framework Decision & National Laws

The European Union's Council of Ministers is considering a measure that would require communications providers to retain for up to two years data related to every communication they carry. The "Draft Framework Decision on the Retention of Traffic Data and Access to this Data in Connection with Criminal Investigations and Prosecutions" is a Belgian proposal, that had been under discussion in the EU's Third Pillar, devoted to Justice and Home Affairs issues. If approved by the Council, and subsequently ratified by the European Parliament, the Framework Decision would require Member States to adopt national legislation mandating data retention by providers operating from their territories.

The EU has not yet made the proposed legislation public. However, the text has been made available on the Internet by one non-governmental organisation concerned about the legislation's likely impact on civil liberties.[2] The proposal would require communications providers to retain for a minimum of 12 months and a maximum of 24 months, data necessary to follow and identify the source of every communication, and to identify the time a communication was made, its destination, the subscriber name and the communications device involved. The Framework Decision defines a communication as all information exchanged or routed between a finite number of parties via an electronic communications network accessible to the public. The data retention requirement would therefore apply to all means by which individuals relate to each other remotely, including land-based telephones, mobile telephones, pagers, data text messaging and electronic mail. The data retained would subsequently be made available as needed to law enforcement agencies in the course of the investigation and prosecution of criminal offenses.

Possibly reflecting the altered mindset that led to the proposed Framework Decision, a number of European Member States separately have moved to enact national legislation that similarly would compel the retention of traffic data. These efforts are gathering pace. At least nine of the 15 Member States either have, or intend to enact, legislation calling for mandatory traffic data retention, and the large majority Member States have expressed broad support for an EU-measure calling for mandatory data retention. While authorities in a few states like Germany and Finland remain skeptical, authorities in Greece, Denmark, Austria, Spain, Belgium and most of the rest of Europe are supportive. Where legislation already has been enacted, it typically calls

---

[2] *See* Draft Framework Decision on Data Retention and Access for Law Enforcement Agencies, *available at* http://www.statewatch.org/news/2002/aug/05datafd.htm.

for retention of traffic data for up to 12 months, although at least one Member State has set a 3-year retention period. These trends are worrying, and we would argue, violate of fundamental privacy rights embedded in European law.

### C. The Right of Privacy in the European Convention on Human Rights

The European Convention establishes basic rules regarding fundamental rights and liberties that are applicable throughout its Contracting States. The Contracting States include every EU Member State, as well as numerous other members of the Council of Europe. Each Contracting State is obliged to ensure that everyone within its jurisdiction, without regard to nationality or place of permanent residence, enjoys the rights guaranteed by the Convention. In many Contracting States, these obligations may be enforced through national courts, on which the Convention is directly binding. To provide further assurance that the rights will not be abridged, the conduct of Contracting States is also subject to review by the European Commission on Human Rights and thereafter by the European Court of Human Rights. In addition to the obligations of individual Member States under the ECHR, European Union law also explicitly incorporates the standards set out in the Convention.[3]

Article 8 of the ECHR guarantees the individual's right to respect for his private and family life.[4] The Article specifies that public authorities may only interfere with this right in narrowly defined circumstances. In particular, any interference must be in accordance with law and necessary in a democratic society, in view of such public interests as national security and the prevention of crime.

These provisions have been interpreted in a series of decisions by the European Court of Human Rights. In these cases, the Court adopts a three-part test for assessing the legality under the Convention of a governmental measure affecting individual privacy:

> first, the Court asks whether a right protected by Article 8 has been interfered with;

---

[3] *See* Treaty on European Union, Article 6(2), *available at* http://europa.eu.int/abc/treaties_en.htm ("The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms").

[4] In complete text, ECHR Article 8 provides as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence."
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

next, it asks whether the interference was in accordance with law. This enquiry requires not only that there be a basis in domestic law for the interference, but also that the legal basis accord with the principle of the rule of law - that it be accessible and that its operation be foreseeable by all citizens;

finally, the Court asks whether the interference was necessary in a democratic society.

The European Court of Human Rights has not previously ruled on a legal challenge to data retention legislation. But the Court has on numerous occasions decided cases involving analogous governmental surveillance of its citizens, frequently finding such regulation to be in violation of Article 8. Analysis of those cases shows that the data retention regime proposed by the draft Framework Decision and now reflected in certain national laws would interfere with the Article 8 right to privacy. Moreover, indiscriminate retention of personal data is not in accordance with law because it fails to distinguish between different classes of people and therefore denies citizens a foreseeable basis on which to regulate their conduct. Finally, such laws are not necessary in a democratic society because blanket retention of data is wildly disproportionate to the law enforcement aims that it seeks to advance.

### D. Data Retention Interferes with the Right to Respect for Private Life

The European Court of Human Rights has interpreted Article 8's reference to respect for private life expansively. Private life does not consist only of an individual's innermost thoughts—those that he chooses not to share with the outside world.[5] It extends to the right to establish and develop relationships with other human beings.[6] Intrusions into an individual's personal or business affairs that interfere with this right therefore fall within the protection of Article 8.[7]

An individual's use of communications services falls squarely within this zone of privacy. The telephone, the Internet and other communications services are quintessentially about bringing people together, in a personal or a business capacity. Government regulation that chills use of these services is accordingly an interference with the right to respect for private life protected by Article 8. Thus, in *Klass v. Germany*, the Court reasoned that because a law permitting interception of mail created a "menace of surveillance" for all users of the postal service, and because that menace struck at freedom of communication, the law therefore constituted an

---

5 *See* Niemietz v. Germany, 16 Eur. Hum. Rts. Rep. 97 (1993).

6 *See id.*; P.G. v. United Kingdom, No. 44787/98 (Eur. Ct. H. R. 2001), *available at* http://www.echr.coe.int.

7 In Niemietz v. Germany, the Court held that there was no reason why the notion of "private life" should be taken to exclude activities of a professional or business nature, since it is in the course of their working lives that the majority of people have a significant opportunity of developing relationships with the outside world.

interference with the right to respect for private life.[8] The indiscriminate retention of traffic data strikes at freedom of communication in the same way as the law at issue in *Klass*. By ensuring that use of communications services will generate a record of one's private activities, data retention requirements threaten all users of those services with the menace that this record will be abused, either by public or private actors. That menace is no less an interference with the right to private life than the generalised threat in *Klass* that one's mail may be intercepted by the authorities.

Retention of data by the authorities is an interference in private life, whether or not the State subsequently uses that data against the individual. In *Amann v. Switzerland*, the European Court of Human Rights found Article 8 applicable when State security services kept a record indicating that the applicant was a contact of the Soviet Embassy, after intercepting a telephone call from the Embassy to the applicant.[9] The Court specifically noted that storage of the information on an index card alone was sufficient to constitute an interference in private life and that the subsequent use of the stored information had no bearing on that finding. Similarly, in *Rotaru v. Romania*, the Court found that the storing of information by the security services on the applicant's past activities as a university student constituted an interference with his Article 8 rights.[10] The data retention envisaged by the Framework Decision and now seen in some Member State laws is of a far greater magnitude than that at issue in either of these cases. Under the EU proposal, for instance, at any given time a record would be in existence recording each and every person or entity with which an individual had communicated electronically over a one to two year period, as well as the time of the communication and the location from which it was made.

Data retention is no less an interference in private life when it is limited to traffic data, rather than recording the content of individual communications. The European Court of Human Rights has repeatedly found the recording of numbers dialed from conventional telephones to constitute an interference with private life.[11] In an earlier technological era, the Court pointed out that the records of such metering contain information which is an integral element in the communications made by telephone.[12] Indeed, the information at issue in *Amann*—that the applicant was a contact of the Soviet Embassy—could have been inferred just as easily from traffic data as it was from interception of the content of the communication. Recent technological advances have blurred the distinction between traffic data and content still further. We now live in a world when mobile phone companies are able to record the exact location from which calls are made, Internet Service Providers can track every web page visited by their users, and the address lines of e-mails provide a wealth of data about the circle of people with which each individual interacts. All of this information, and more, would be stored under the terms of the Framework Decision; it

---

8 Klass v. Germany, 2 Eur. Hum. Rts. Rep. 214 (1980).

9 Amann v. Switzerland, 30 Eur. Hum. Rts. Rep. 843 (2000).

10 Rotaru v. Romania, No. 28341/95 (Eur. Ct. H. R. 2000), *available at* http://www.echr.coe.int.

11 *See, e.g.* P.G. v. United Kingdom, *supra* note 5; Valenzuela Contreras v. Spain, 28 Eur. Hum. Rts. Rep. 483 (1999); Malone v. United Kingdom, 7 Eur. Hum. Rts. Rep. 14 (1985).

12 *See* Malone v. United Kingdon, *supra* note 11.

is now being stored pursuant to a variety of Member State laws. As the case law of the European Court of Human Rights makes amply clear, this represents an interference of unprecedented proportions in the private life of every user of European-based communications services.

### E. Indiscriminate Retention of Data is Not in Accordance with Law

Of course, not all interferences with the right to private life violate Article 8 of the European Convention on Human Rights. Article 8(2) acknowledges that there are certain situations in which interference by the State is justified. But the Court has been clear that this paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be read narrowly.[13] The Court has accordingly interpreted Article 8(2)'s requirement that such interferences be in accordance with law, as meaning not only that there must be a law in place authorising the interference, but that it should meet the standards of accessibility and foreseeability inherent in the concept of rule of law. The data retention regime envisaged by the Framework Decision fails to meet these standards. Even if we assume that it was implemented by national laws that could be accessed by all citizens, the very idea of blanket data retention offends the standard of foreseeability as it has been developed by the Court.

The principle behind the foreseeability requirement is the simple notion that the State should give citizens an adequate indication of the circumstances in which the public authorities are empowered to interfere in their private lives.[14] When laws are foreseeable in this way, individuals can regulate their conduct accordingly, so as to avoid invoking unwelcome intrusions by the State. Laws that offer citizens no reasonable means of avoiding surveillance of their private affairs by the State are the hallmark of the police state.

The requirement of foreseeability is not satisfied by blanket regulations, such as those envisaged in the Framework Decision, that allow everyone to foresee that the State will interfere with their right to a private life. As the Court said in respect of secret surveillance in *Malone v. United Kingdom*, it would be "contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power."[15] Rather, what makes a law foreseeable is the extent to which it distinguishes between different classes of people, thereby placing a limit on arbitrary enforcement by the authorities. Thus, in *Kruslin v. France*, the Court found that a law authorising telephone tapping lacked the requisite foreseeability because it nowhere defined the categories of people liable to have their telephones tapped or the nature of the offenses which might justify such surveillance.[16] In *Amann v. Switzerland*, the Court reached the same conclusion with regard to a decree permitting the police to

---

13 *See* Klass v. Germany, *supra* note 8. The Court added that: "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."

14 *See* Kruslin v. France, 12 Eur. Hum. Rts. Rep. 547 (1990); Malone v. United Kingdom, *supra* note 11.

15 Malone v. United Kingdom, *supra* note 11.

16 Kruslin v. France, *supra* note 14.

conduct surveillance, because the decree gave no indication of the persons subject to surveillance or the circumstances in which it could be ordered.[17] Data retention laws that fail to distinguish between different classes of people would have a more pernicious impact on individual privacy than the vague laws at issue in *Kruslin* and *Amann*. Whereas the latter left every citizen vulnerable to a risk of surveillance, blanket data retention would subject every citizen to the certainty of ongoing and unremitting interference in his or her private life.

Blanket data retention laws also offend the principle of foreseeability because they make no distinction for relationships that the State already recognises as sufficiently special to warrant a degree of protection. In *Kopp v. Switzerland*, the Court observed that a law authorising interception of telephone calls would in certain circumstances contradict other provisions of Swiss law according protection to confidential attorney-client communications. The Court found that the telephone tapping law failed to meet the standard of foreseeability, because it provided no guidance on how authorities should distinguish between protected and unprotected attorney-client communications. The Framework Decision and laws like it suffer from the same flaw. Confidential attorney-client communications, to take one example, enjoy a protected status throughout the EU. Yet the proposed data retention schemes make no effort to distinguish between such communications (and others like it) and "normal" communications.

### F. Indiscriminate Retention of Data is Not Necessary in a Democratic Society

Blanket data retention is the antithesis of a regime designed to achieve the minimum necessary impairment of rights. In order to retain information bearing on the very small fraction of the population involved in criminal activity or threatening national security, mandatory data retention gives rise to an indefinite and ongoing interference with the privacy rights of every individual who uses European-based communications systems. Such a broad interference with an established right exceeds the bounds of permissible interferences as set forth in the European Convention and enunciated by the European Court of Human Rights.

Article 8(2)'s limited exception to the right to respect of private life requires that any interference be no greater than is necessary in a democratic society. This condition is subject to the same narrow reading that the European Court on Human Rights applies to the rest of Article 8(2).[18] The Court has explained the principle underlying this requirement in terms of the need for any interference in Article 8 rights

---

[17] Amann v. Switzerland, *supra* note 9. According to the facts in this case, the Swiss government, following routine interceptions of communications of Soviet embassy personnel, recorded telephone communications between an Embassy worker and the applicant. Although the government found that the applicant's activities did not generate any national security concerns, the government nevertheless stored information in connection with the applicant for a long period after the investigation. The court found that the storage of information by a public authority relating to the individual's private life was an Article 8 interference, even though there was no subsequent use of that information.

[18] *See supra* note 13 and accompanying text.

to correspond to a pressing social need and to be proportionate to the legitimate aim pursued.[19] Mandatory data retention laws fail on this score as well. The distinguishing feature of a blanket data retention requirement is the absence of any reasonable relationship between the intrusion on individual privacy rights and the law enforcement objectives served.[20]

For a measure impairing individual rights to be proportional, the State must put in place safeguards ensuring that interference with those rights is no greater than necessary. In *Foxley v. United Kingdom*, for example, the Court found that interception of a bankrupt's mail violated Article 8 because of the absence of adequate and effective safeguards ensuring minimum impairment of the right to respect for his correspondence.[21]

European legislators can make no showing that such large-scale impairment of individual rights arising from mandatory data retention laws is the only feasible option for combating crime or protecting national security. Indeed, international practice points strongly in the opposite direction. For example, in the U.S., the authorities have much more circumscribed authority to require retention of traffic data.[22] And, as recently as 2001, all 15 Member States of the European Union signed a Council of Europe Convention providing for data to be retained on a selective basis, where the authorities have reason to believe that the information may be relevant to a criminal investigation.[23] Law enforcement requirements can be met without widespread interference with individual rights. In short, blanket data retention is unnecessary. The interference in individual privacy rights required by mandatory data retention laws cannot therefore be necessary in a democratic society.

Proportionality also requires that interferences in private life take account of the specially protected nature of certain communications. Thus the Court has on occasion analysed the impact of State surveillance on the attorney-client relationship as part of its inquiry into whether a given regulation was necessary in a democratic society. In finding that the interception of a bankrupt's mail was not necessary in a

---

19 *See* Foxley v. United Kingdom, 31 Eur. Hum. Rts. Rep. 637 (2000).

20 *See* Common Industry Statement on Storage of Traffic Data for Law Enforcement Purposes, Joint Statement by the International Chamber of Commerce, the Union of Industrial and Employers' Confederations of Europe, the European Information, Communications and Consumer Electronics Technology Industry Association and the International Telecommunication Users Group (June 4, 2003) (*available at* http://www.iccwbo.org/home/news_archives/2003/stories/data.asp) (criticizing the overly broad definitions of data traffic in the draft Framework Decision and the excessive storage period involved, and describing mandatory data retention as an ineffective means of furthering criminal investigations).

21 Foxley v. United Kingdom, *supra* note 19.

22 For a general discussion of US law in this area, see Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, *available at* http://www.cybercrime.gov/s&smanual2002.htm.

23 Convention on Cybercrime, *opened for signature* 23 November 2001, ETS No. 185. *See* Art. 16-17, Expedited Preservation of Stored Computer Data.

democratic society, the *Foxley* decision, for example, accorded particular weight to the authorities' failure to distinguish between privileged communications from the applicant's lawyer and other items.[24] As already noted, blanket data retention falls short on this measure too. The Framework Decision, for instance, fails to take even the minimum steps necessary to ensure respect for attorney-client and other specially-protected communications.

### G. Data Retention Laws Are Regressive Legislation

The Framework Decision and comparable national laws represent the latest stage in the steady erosion since September 2001 of European privacy safeguards. EU legislation in force prior to that date prohibited communications providers from retaining data for any longer than necessary to resolve billing disputes.[25] A narrowly-worded exception allowed Member States to deviate from this standard to the extent necessary to safeguard national security and to investigate and prosecute criminal offences.[26] Reacting to the September 11 attacks, and under pressure from the U.S., the EU widened this exception substantially in 2002. Controversial new legislation that year permitted Member States to "adopt legislative measures providing for the retention of data for a limited period" for national security or criminal justice purposes.[27] The Framework Decision shifts the balance still further in the direction of security at the expense of individual privacy, transforming the permissive language of the 2002 legislation into an obligation on Member States to require data retention by communications providers. As noted above, the majority of Member States perhaps sensing this shift in orientation have since enacted, or are in the process of enacting, legislation that would mandate traffic data retention.[28]

The proposal to make blanket retention of traffic data mandatory throughout the EU has drawn criticism from data protection officials,[29] civil liberties groups[30] and

---

24 Foxley v. United Kingdom, *supra* note 19. *See also* Niemietz v. Germany, *supra* note 5.

25 Directive 97/66/EC of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

26 *Id.* at Art. 14(1).

27 Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), at Art. 15(1). *See also* Paul Meller, *EU Set to Weaken Net Privacy Regime*, International Herald Tribune, May 30, 2002 (describing the background and opposition to the data retention provisions of the 2002 Directive).

28 In connection with the Framework Decision, the General Secretariat of the Council of the European Union issued a questionnaire to Member States in 2002 seeking further information on their data retention laws. The Member State responses have been made available at: www.statewatch.org/news/2002/jan/12eudatret.htm.

29 *See* Statement of the European Data Protection Commissioners (Sept. 11, 2002), *available at* http://www.fipr.org/press/020911DataCommissioners.html (expressing "grave doubt as to the legitimacy and legality of such broad measures" as those contained in the draft Framework Decision).

30 *Cf.* Letter to Pat Cox, President, European Parliament, from a coalition of civil liberties organizations (May 22, 2002) (*available at* http://www.gilc.org/cox_en.html) (urging Members of the European Parliament to vote against the "general and exploratory data retention" provisions of the 2002 Directive).

industry bodies.[31] As these groups have pointed out, mandatory data retention regimes such as that embodied by the Framework Directive have a major, and negative, impact on individuals and on business in the European Union and beyond:

> The requirement that communications providers retain traffic data for up to two years (and even longer under some national legislation) would effectively create a massive database reaching indiscriminately into the personal and business affairs of each and every user of EU-based communications services. Whatever national rules were developed to regulate access to traffic data by law enforcement agencies, the very existence of this database would put at the disposal of the State an unprecedented amount of information about the everyday activities of its citizens. This would be a significant departure from the traditional approach in societies based on the rule of law, where the State's ability to monitor individuals is strictly limited and regulated by such requirements as probable cause and a duly-authorised warrant. Interestingly, although the U.S. government has encouraged the European Union to adopt more extensive data retention powers,[32] U.S. law permits data retention by communications providers only in respect of specific investigations that are already underway.[33]
>
> The retention of traffic data by communications providers would also greatly enhance the risk that personal information could be stolen and exploited by third parties. Stored traffic data would present an attractive target for hackers, who would be able to access multiple personal details about individuals in one place. Moreover, because the information would be stored, hackers would be able to sort through stolen data at their leisure, rather than trying to intercept valuable personal details in real time, as at present. Thus, in the name of facilitating the investigation and prosecution of crimes, mandatory data retention laws would in fact make the job of the cybercriminal considerably easier.
>
> Concern about the misuse of sensitive personal information could undermine public confidence in electronic communications systems. A blanket requirement on communications providers to retain traffic data would give all users of electronic services reason to fear that stored data relating to their personal lives might be improperly accessed. As the 2002 EU legislation recognised, "the successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk."[34] A loss of public confidence could, in particular, retard the role of the Internet as a channel of social intercourse and a vehicle for electronic commerce. The failure of the Internet to live up to its potential in either respect would represent a significant loss for

---

31 *See* Common Industry Statement, *supra* note 20 (arguing that data storage requirements should not exceed that which is necessary to achieve law enforcement objectives and which cannot be achieved by alternative and less intrusive measures).

32 *See* U.S. Letter from Bush to E.U., 16.10.01, Statewatch Analysis No. 2, *at* http://www.poptel.org.uk/statewatch/news/2002/feb/useu.pdf.

33 *See supra* note 22.

34 Directive 2002/58/EC, Recital 5.

society at large, as well as for individuals in their capacities as both citizens and consumers.

Indiscriminate data retention requirements would raise the cost of electronic services to the consuming public. By requiring communications providers to retain data on every communication carried, this would create a need to store massive amounts of information, out of all proportion to the quantity of information law enforcement agencies actually need. Storage of this data for up to two years would impose significant additional costs on business, which would inevitably be passed on to consumers in the form of higher prices. This, too, would tend to retard the development of the Internet, and other electronic services, in Europe.

## H. Conclusion

The blanket data retention regime envisaged by the draft Framework Decision and now reflected in Member State laws represent a significant violation of the privacy rights of every user of European-based communications services. Even the obligations imposed under the Council of Europe Convention on Cybercrime do not go so far in constraining the right of an individual to privacy. These obligations limit data retention to those cases where there is a real reason to suspect relevance to national security or a criminal investigation. This approach would not only avoid the needless violation of privacy rights on a massive scale, it would also be more consistent with the EU's traditional concern for data protection. The vigorous opposition to mandatory data retention from such diverse groups as data protection officials, civil liberties groups and industry, is a powerful indication of the practical difficulties with blanket data retention requirements. The indiscriminate nature of mandatory data retention offends basic principles of the rule of law and democratic governance, and is contrary to established notions of privacy and human rights found in the European Convention on Human Rights.