BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

E.U. Data Retention Proposals in the Headlines

Daniel Cooper, Special Counsel, and
Robin Blaney, student-at-law,
Covington & Burling, London

Reprinted from the July 2005 issue of BNA International's
World Data Protection Report

www.bnai.com

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

Security & Surveillance

E.U. Data Retention Proposals in the Headlines

By Daniel Cooper, Special Counsel, Covington & Burling, London and Robin Blaney, student-at-law, Covington & Burling, London. The authors may be contacted at dcooper@cov.com and rblaney@cov.com, respectively.

E.U. legislation on data retention, the maintenance of telephone and e-mail records, has been mooted for several years now, but the terrorist bombings in London on July 7, 2005 catapulted this issue to the top of the U.K. political agenda. The United Kingdom's presidency of the E.U. Council has simultaneously ensured that the issue is now a priority at E.U. level. Following an emergency meeting of E.U. Justice and Home Affairs Ministers on July 13, 2005, the E.U. Council has established a deadline of October 2005 to agree on its proposed Framework Decision. This article describes that proposal and highlights the many controversies – political, technical and legal – that surround it.

Background

Post-9/11

In the 1990s, Europe led the way in the recognition of how emerging technological trends threatened individual privacy and in the provision of countervailing protections. Following the terrorist attacks in the U.S. on September 11, 2001, however, the political climate in Europe and throughout the world altered radically and perhaps irrevocably. E.U. lawmakers have been forced to re-evaluate the tension between security concerns, on the one hand, and civil liberties, on the other, and increasingly they are erring on the side of security.

In mid-2002, E.U. legislators enacted Directive 2002/58/EC to regulate the processing of personal data, including traffic data, on electronic networks. Although that Directive provided that, in principle, traffic data should not be retained once it was "no longer needed for the purpose of the transmission" (Article 6), it did allow derogations from that principle to safeguard public security and for the "prevention, investigation, detection and prosecution of criminal offences" (Article 15). Any such restriction, however, was to be "necessary, appropriate and proportionate", a prerequisite that did much to assuage the concerns of privacy advocates, industry and others who feared that Member States might be tempted in the wake of Directive 2002/58/EC to adopt broad-reaching data retention laws. Article 15 went on to say explicitly that Member States were entitled to adopt legislative measures providing for the retention of data for a limited period. The Directive therefore did not mandate data retention throughout the European Union, but granted individual Member States a limited right to enact local laws on the issue, which many already had done.

At around the same time as the Directive was adopted, and much more controversially, Belgian officials circulated a Draft Framework Decision that would oblige communications providers to retain all traffic data for a period of between 12 and 24 months.[2] That proposal encountered vociferous opposition from human rights and privacy advocates when it became publicly known. Partly as a consequence of this opposition and perceived difficulties in securing approval from each Member State, the Council of Ministers allowed the proposal to fall quickly by the wayside, so that, by November 29, 2002, the Council could issue a formal denial that any such Framework Decision was even under consideration.[3]

Madrid

Following the controversies surrounding the Belgium proposal, no significant developments at the E.U. level occurred between the summer of 2002 and March 11, 2004, when terrorists perpetrated an attack on the transport system in Madrid, killing substantial numbers of people. Once again, the Council responded quickly and issued a statement on March 25, 2004, condemning the atrocities.[4] In its published Declaration, the Council urged the adoption of a number of legislative measures to deal with the perceived terrorist threat in the EU, including "proposals for establishing rules on the retention of communications traffic data by service providers". These proposals were stated to be a priority, with a view to adoption by June 2005.

Then, on April 28, 2004, the French, Irish, Swedish and U.K. governments jointly tabled a new proposal for a Framework Decision on traffic data retention, revisiting the very issue so controversially raised by Belgium back in 2002.[5] The proposal is a so-called "Third Pillar" initiative, relating to "Police and Judicial cooperation in Criminal Matters". As a result, the European Parliament is entitled to give a non-binding opinion on the proposal, but has no further input in the legislative procedure. The Decision can be adopted only with the unanimous support of the 25 Member States in the Council.

From its inception, the passage of the draft Framework Decision has been dogged by controversy. The E.U. Commission and Parliament strongly oppose the measure and it has encountered near universal resistance from human rights watchdogs, privacy regulators and the telecommunications industry. Perhaps as a result of this opposition, the Framework Decision has undergone seemingly continuous revision at a working group level, with new versions published by the Council on a fairly regular basis. Furthermore, about two weeks after the proposal was tabled, the German Parliament voted down a draft data retention law championed by the German Government. This precluded a quick adoption of the Council proposal since the German Government was no longer in a position to approve a Framework Decision calling for essentially the same result. After a year of insubstantial progress, it was questionable whether a final Decision ever would be agreed.

London

Once again, a terrorist outrage precipitated a change in the political climate. Following the London bombings of July 7, 2005, the issue of data retention has risen to the top of the U.K. political agenda. Charles Clarke, the U.K. Home

  WDPR ISSN 1473-3579

Secretary, has made clear the U.K. Government's commitment to the proposal and suggested that the issue of public security far outweighed an individual's right to privacy. Indeed, in an address to the European Parliament's civil liberties committee, he declared that the right to go to work "without being blown up" was as much a fundamental civil liberty as the right to privacy.[6]

The United Kingdom's presidency of the Council also ensures that the issue of data retention has now become a priority for the rest of the European Union. An extraordinary Council meeting of E.U. Justice and Home Affairs ministers, held on July 13, 2005, resulted in a commitment to agree the final Framework Decision by October 2005.[7] Whether the Council will be able to adhere to this self-imposed deadline remains to be seen, although the United Kingdom is likely to push hard for some result during the time that it retains the Council presidency. Meanwhile, some Member States already have enacted national data retention laws, without waiting for the Decision to materialise.

The Proposed Framework Decision

The draft of the Framework Decision under discussion at the time of the bombings in London was presented by the "Incoming Presidency" (*i.e.*, the United Kingdom) to the Working Party on Co-operation in Criminal Matters on June 29, 2005. Although the E.U. Council has yet to make this draft publicly available, a number of interested non-governmental organisations have published it on the Internet.[8]

Scope and Aim (Article 1)

The Framework Decision is intended to harmonise,

> "Member States' legislation on the retention of communications data, generated or processed by providers of a publicly available electronic communications service or a public communications network, for the purpose of investigation, detection and prosecution of criminal offences".
>
> Prior drafts included the additional aim of retaining data for the "prevention" of crime. This language was, and remains, one of the more controversial aspects of the draft Decision. Although the present draft now omits this language, a footnote states that the omission is "subject to scrutiny", suggesting that it may be added later if there is political consensus.

Article 1 explicitly excludes from the remit of the Decision the content associated with retained communications data. Notwithstanding that, the draft Framework Decision has potentially broad scope. For example, Article 1 does not limit the proposed retention mandates to European service providers or data located in Europe. In addition, the Decision fails to define "electronic communications service" and "communications network", so it is unclear precisely to whom this Decision will apply. Previous drafts, however, have referred to, among other things, telephony, short messaging services and Internet services. It appears likely that the Decision will apply not only to Internet service providers (ISPs), but possibly also providers of electronic services such as e-mail and instant messaging. This could mean that different service providers would be required to retain the same data regarding the same individuals.

Data Retention Obligations (Articles 2 and 3)

The crux of the draft Framework Decision continues to be its data retention provisions. The Decision requires Member States to mandate the retention of "communication data", namely "traffic", "location", "user" and "subscriber data". "Traffic data" and "subscriber data" are defined by reference to Directive 2002/58/EC as data processed for the "conveyance of a communication" or indicating the "geographic position of the equipment of a user". "User data" and "subscriber data" are defined as data relating to a natural or legal person using or subscribing to an electronic communications service.

The Framework Decision also stipulates the retention of, at least, communication data necessary to identify the source, destination, date, time, duration and type of the communication and to identify the communication device and the location of mobile equipment at the start and the end of the communication.

Data Retention Time Periods (Article 4)

The default position under the draft Framework Decision is that communication data should be retained for 12 months following its generation. Derogations allow Member States to mandate for longer periods of up to 48 months, provided such a period is "necessary, appropriate and proportionate" in a democratic society or for shorter retention periods of at least six months. In a significant development, the most recent draft contains a new provision that allows data to be retained for periods of less than six months, where that data ordinarily is retained for business purposes for less than seven days.

Data Security and Access (Articles 5 and 6)

Retained data must be protected pursuant to the framework Data Protection Directive 95/46/EC. Similarly, the following "data security principles" must be followed: (1) "retained data shall be of the same quality of those data on the network;" (2) "data shall be subject to appropriate technical and organizational measures to protect the data;" and (3) all data shall be destroyed at the end of the period for retention". The Decision sets out an additional set of rules that those accessing the data should adhere to. For example, data must be accessible for only "specified, explicit and legitimate purposes", and the "confidentiality and integrity of the data shall be ensured". These rules are, to a certain extent, duplicative of those contained in Directive 95/46/EC. The reference to the Directive and the additional security protections are in response to concerns raised by privacy advocates that the Decision represents an excessive intrusion into the private lives of individuals.

Data Sharing (Article 7)

The Decision requires Member States to execute requests from other Member States for the transmission of communication data. As presently drafted, however, cross-border access rights are not absolute, for the,

> "requested Member State may make its consent to such a request for communication data subject to any conditions which would have to be observed in a similar national case".

This provision is proving to be a bone of contention within the Council, with many Members fearing that the sentence "would allow for refusing requests for mutual assistance to a wider extent than provided under existing instruments".

Controversies Abound

Political

Over the past year, the Council's proposed Framework Decision has given rise to a political power struggle between the Council on one side and the Commission and Parliament on the other. At issue, among other things, is whether the Council has the authority to issue this Decision in the first place, and the Parliament has questioned publicly the proposal's legal basis.

The various E.U.-level treaties, which allocate power and responsibilities between the European Union and its Member States, are organised into the following three "Pillars":

- Pillar One addresses "Community policy";
- Pillar Two addresses foreign and security policy; and
- Pillar Three addresses police and judicial co-operation.

The proposed Framework Decision is a "Third Pillar" initiative because it deals primarily with "police and judicial cooperation in police matters". In particular, Article 34.2 (b) of the Nice Treaty allows Member States and/or the Commission to propose Framework Decisions addressing these matters. Such decisions are considered by the E.U. Council, which consists of ministers from all the Member States. Notably, Decisions can be adopted only with the unanimous support of all 25 Member States. Critically, the European Commission and European Parliament play marginal roles in the deliberative process attending the passage of such Decisions. For example, the Commission serves essentially as a logistical coordinator, while the Parliament is entitled to prepare a non-binding opinion on the proposal, its only opportunity to shape the legislation.

The date chosen by the French, Irish, Swedish and U.K. governments to table the data retention proposal, April 28, 2004, was not accidental, and seemed likely to raise Commission and Parliament hackles. Only two days later, on May 1, 2004, a transition phase of the Nice Treaty expired and Member States lost their right of initiative for such matters. In addition, as of May 1, 2004, Third Pillar initiatives with First Pillar ramifications – such as the proposed Framework Decision, which deals primarily with security but also impacts the E.U. internal market – are subject to the "co-decision procedure". The co-decision procedure provides the European Parliament and Commission with important roles in the legislative process. The proposal's release, therefore, was timed precisely to marginalise the powers of the Commission and Parliament in the deliberative process.

Unsurprisingly, the European Parliament reacted negatively to this attempt to circumscribe their involvement. On the basis of a report prepared by its Committee of Legal Affairs (JURI Committee), the Parliament declared its rejection of the proposal and called on France, Ireland, Sweden and the United Kingdom to withdraw their initiative.[9] The rapporteur concluded that the proposal contained two distinct measures: one, covering access to and the exchange of data stored in the Member States, which properly could be regarded as a Third Pillar concern and one, imposing obligations on service providers to retain data, which was already an area of Community law, as reflected in Data Protection Directive 95/46/EC and Electronic Communications Data Protection Directive 2002/58/EC.

The rapporteur argued that the measures proposed logically must have "the same legal basis as the existing legislation". Accordingly, the co-decision procedure called for by Article 95 of the EC Treaty therefore would be the appropriate means of initiating this legislation. Any proposal disregarding this procedure would be an attempt to alter existing legislation unlawfully, in breach of Article 47 of the E.U. Treaty, and hence the Council's Framework Decision would be *ultra vires*. The Commission and also the Council's own Legal Service have endorsed, to a certain extent, this position. In response, the Commission announced that it would put forward its own proposal on data retention, and a September 2005 publication date has been set. In the meantime, the Council is pressing ahead with its Decision, setting it on a collision course with the Parliament and Commission.

Technical

The Framework Decision, as it currently stands, would require the retention and hence storage of a massive amount of data. The European Parliament estimates that a large Internet provider, even at today's Internet traffic levels, would accumulate an amount of data equivalent to 10 stacks of files each reaching from the Earth to the moon. Patently, the obligations imposed by the Decision would necessitate a significant investment in infrastructure by communications providers just to retain the relevant data. They likely also would need to make technical changes to their systems, in order to allow the generation and storage of the requisite data.

But not only must the service providers store the data, they must comply with the data protection principles and implement appropriate technical and organisational measures to guarantee the security of the data. Moreover, the service providers would have to develop some means of searching the data. The European Parliament estimates that, with a data volume so large and using technology available today, it could take upwards of fifty years to conduct a single search of the data in some cases. Evidently, significant investment will be required to enable the data to be accessible in any meaningful way.

Relatedly, far from harmonising pan-European data retention regimes, the Framework Decision could lead to markedly different regimes throughout Europe. By using the available derogations, a Member State could mandate a retention period of anywhere between six months and four years. At present, service providers may not keep much of the data covered by the Decision for more than a few minutes, let alone for months or even years. In such circumstances, Member States may chose to exercise their right of derogation to allow for retention periods of less than six months, but there is no guarantee that they will do so. Communications providers thus are likely to be subject to multiple and conflicting data retention requirements throughout the European Union, escalating their compliance burdens and hence costs.

Similarly, the Framework Decision contains no territorial restrictions, so potentially could apply equally to service providers based in North America or Asia, possibly subject to different data retention obligations in their own territory. Service providers frequently do not know in what country a particular user resides and so, in order to comply with the Decision, would have to ask each user to indicate his or her country of residence. Given that a user may decline to answer truthfully, service providers will be faced with a

difficult choice. They could retain all global data, on the basis that it might be covered by the Decision, risk non-compliance, by accepting the user's statement as true, or further invade the user's privacy by verifying independently the accuracy of the user's statement.

The European Parliament has estimated that, for a traditional telephone network operator, compliance with the Framework Decision would require an initial investment in the region of €180 million, with annual operating costs of up to €50 million. This inevitably would jeopardise the very existence of many small and medium-sized businesses. The costs for an Internet provider probably would exceed that multi-fold. And, the Framework Decision contains no consistent means for spreading the cost burden. Recital 16 of the Decision urges Member States to *consider* "making appropriate contributions towards the costs", but contains no compulsion for them to pay anything. Industry evidently will have to meet some of the compliance costs and may well end up being liable for the vast majority of them.

Legal

Numerous human rights and privacy watchdogs argue that the proposed Framework Decision is incompatible with privacy principles contained in the European Convention on Human Rights, which all Member States have implemented and which E.U. law also explicitly incorporates.[10] Article 8 guarantees an individual's right to privacy.[11] Although this right is not absolute, any interference must comply with the European Court of Human Rights' interpretation of Article 8(2), which requires that any interference be laid down by law, be necessary in a democratic society and serve one of the legitimate purposes specified in the Convention.

To be in accordance with law, the measures not only must be stipulated by a law, but also should meet the standards of accessibility and foreseeability inherent in the concept of the rule of law. When laws are foreseeable in this way, individuals can regulate their conduct accordingly, so as to avoid invoking unwelcome intrusions by government authorities. According to some, the fact that blanket data retention laws offer citizens no reasonable means of avoiding surveillance of their private lives suggest that they fail to meet this standard.

Relatedly, others have noted that only limited evidence has been offered that data retention laws are needed in the fight against terrorism, or may even be of the slightest assistance. To be "necessary in a democratic society" a measure must correspond to a pressing social need and be proportionate to the legitimate aim pursued.[12] The phenomenal cost to industry arguably calls into question the proportionality of the obligations. Likewise, any technological impossibility of conducting a useful search of the retained data within a reasonable period of time suggests that the proposal may be more than unnecessary, it may be counterproductive. The measure simply will create a larger haystack for the same number of needles, according to one source.[13]

Political Prospects

In the past, politicians have responded quickly and emotively to terrorist atrocities, but then failed to convert that indignation into substantive legislation. The discussion, some four years on from 9/11, of a blanket data retention law is clear evidence of that. Given the strong opposition from so many different elements of society, from MEPs, from privacy regulators, from the telecommunications industry, one ordinarily would consider the proposal doomed to failure. But this time may well be different. The current U.K. Government has a consistent track record of prioritising security over civil liberties, as evidenced by its introduction of "control orders" (which effectively place a suspect under house arrest at the behest of the Home Secretary) and its support for identity cards. The U.K. Government understandably is determined to react strongly and swiftly to the London bombings and its presidency of the European Council may give the United Kingdom the necessary platform and impetus to persuade the rest of Europe to follow suit. The Framework Decision on data retention, in its current or a substantially similar form, now should be seen to be a very real possibility.

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.

2 The text of that proposal was not made public by the E.U., but was made available on the Internet by a non-governmental organisation. See Draft Framework Decision on Data Retention and Access for Law Enforcement Agencies, at *www.statewatch.org/news/2002/aug/05datafd.htm*.

3 See Draft Reply to Written Question, Doc. 14923/02, *http://register.consilium.eu.int/pdf/en/02/st14/14923en2.pdf*.

4 Draft Declaration on Combating Terrorism, Doc. 7764/04, *http://register.consilium.eu.int/pdf/en/04/st07/st07764.en04.pdf*.

5 Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism, Doc. 8958/04, *http://register.consilium.eu.int/pdf/en/04/st08/st08958.en04.pdf*.

6 See David Rennie, "The Right Not to be Bombed Outweighs Liberties, says Clarke", *Daily Telegraph*, July 14, 2005, at 6, available at *www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/07/14/nclarke14.xml*.

7 Press Release, Doc. 11116/05 (Presse 187), *http://ue.eu.int/ueDocs/cms_Data/docs/pressData/en/jha/85703.pdf*.

8 Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of investigation, detection and prosecution of crime and criminal offences including terrorism, Doc 10609/05, available at *www.statewatch.org/news/2005/jul/10609-05.pdf*.

9 See Draft Report, Doc. 2004/0813(CNS), *www2.europarl.eu.int/registre/commissions/libe/projet_rapport/2005/357618/LIBE_PR(2005)357618_EN.pdf*

10 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").

11 The complete text of 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 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.

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

13 Tony Bunyan, Statewatch, at *www.statewatch.org/news/2005/jul/05eu-data-retention.htm*.