THE FEDERAL TRUST
for education & research
enlightening the debate on good governance
EuropeanPolicyBrief
Jan 2006 • Issue 21 • The Federal Trust, 7 Graphite Square, Vauxhall Walk, London SE11 5EE • www.fedtrust.co.uk

Civil Liberties and Democracy in the EU: Assessing the Data Retention Directive

In recent years, justice and home affairs has been the policy field which has seen the most intensive progress towards further integration in the European Union (EU). There is widespread agreement among commentators and politicians alike that problems such as terrorism, international crime and illegal immigration are more easily tackled at the European level. The legislative agenda of the Union over the past five years has reflected this consensus.

Nevertheless, two growing public concerns have accompanied the EU's greater involvement in matters of internal security. First, the European Union is sometimes criticized for its supposed tendency to see its justice and home affairs agenda predominantly in criminal and repressive terms, rather than seeking long-term political solutions to such new social phenomena as mass migration. Second, there is an oft-voiced fear that democratic control over European policy-making in this area has been insufficient. Little scrutiny is given in Europe's national media to legislation on internal security coming from European institutions, and the European Parliament (EP) – the only directly elected European institution – has much less influence on the EU's internal security agenda that over most other areas of EU activity.

The discussion surrounding the recent directive on mandatory data retention, adopted by the EP in December, clearly reflects these problems. Approval of the directive proved a long and controversial process, provoking an unusual coalition against it of human rights campaigners and industry associations. The latter argue that the directive imposes significant costs on telecommunications companies even though it is unclear whether the data stored will be of much practical use. Human rights campaigners for their part argue that the directive is an unnecessarily large infringement of civil liberties. Most worryingly, the manner of the directive's approval does not inspire confidence in democratic control over EU policy-making on internal security matters.

Background

On December 14, the EP approved a directive on mandatory data retention, scoring a major success for the UK Presidency in its closing days. The directive, which will be implemented over the next 18 months, requires so-called telephonic 'traffic data' to be stored for a period between six months and two years. This means that all numbers dialled, the length of calls made and the location of the caller at the time of the call will be recorded. Similar rules will apply to the internet, where the data stored will include the recipient, date and time of e-mails as well as information on internet access and internet telephony. No data related to actual content of communications, however, will be recorded under this new system.

The stated aim of the directive is to use this retained data to help detect, investigate and prosecute serious crimes. Each member state will define what exactly constitutes a 'serious' crime and will set up an independent national authority to monitor the use of

CONTINUED OVERLEAF

EDITOR's NOTE

This is the nineteenth in a series of regular *European Policy Briefs* produced by the Federal Trust. The aim of the series is to describe and analyse major controversies in the current British debate about the European Union.

We would welcome comments on and reactions to this policy brief. Other Policy Briefs are available on the Federal Trust's website www.fedtrust.co.uk/policybriefs.

Brendan Donnelly (Director, Federal Trust)

retained data. Law enforcement agencies will not gain access to the entire database, but will have to make applications to companies on a case-by-case basis. It is up to each member state to decide what financial contribution, if any, telecommunications companies will have to make to the expense of implementing the new system.

Is data retention worth it?

European governments maintain that data retention is an absolute necessity in the fight against international terrorism. The British Home Secretary Charles Clarke, in his address to the EP the day before the vote, argued that communications data has been vital in several investigations in order to 'trace the members of terrorist cells, to help identify murders and free kidnap victims and to deal with those who organise very serious crime.' Spanish officials have pointed out that the perpetrators of the Madrid bombings could not have been found without the retention of mobile phone data.

Supporters of the directive have also argued that it is essential that data retention laws be harmonised across Europe. As Charles Clarke stated, 'Variations in data retention practice mean that the ability of investigators and prosecutors to detect and prosecute criminals and terrorists ... is dependent on which communications service provider a suspect, a victim or witness has used or which member state they were in. That variation gives an open goal to our opponents in criminality.'

However, experts have been much more sceptical on the benefits of the new directive. For example, the committee of EU privacy commissioners – also known as the Article 29 Working Party – was not convinced by the case for data retention. In their report of 21 October 2005, they note that 'the circumstances justifying data retention, even though they are said to be based on the requests coming from the competent authorities in Member States, do not appear to be grounded on crystal-clear evidence.'

The President of the European Confederation of Police (EuroCOP), Heinz Kiefer, argued in June that the data retention law would not be of great use in the fight against organised crime. European police forces, he claimed, simply do not have the technological ability to search efficiently the wealth of data that would be provided under the directive by telecommunications companies. While recognizing that telephone data has sometimes proved useful to law enforcement agencies, especially for periods of up to one year, Mr. Kiefer saw little evidence that either longer retention periods or internet data would bring significant benefits.

Moreover, the retention rules seem very easy to circumvent. Mr. Kiefer also points out that, for example, mobile phone cards can be bought from suppliers outside the EU and switched regularly. On the internet, evading police surveillance would be even simpler, as e-mail services based outside Europe (of which there are many thousands) will not need to retain data. For the infrequent possibility of providing some useful information to the police, European providers will be forced to store information on the billions of spam e-mails sent out each day. The ease with which e-mails and web sites can be changed throw yet further doubt upon the benefits of retaining internet data for any substantial period of time.

All these considerations led a number of technology experts to criticize the directive, claiming it showed that European lawmakers had little idea of how the internet world works. As Richard Clayton of Cambridge University told *The Guardian*, 'I think the EU hasn't a clue what they're doing...they understand telephony but not the internet.' Carl Mühlner, head of Tiscali Germany, told the *International Herald Tribune* that, in his view, 'this law is definitely not going to hinder terrorism.' The opinion of the online world is simply that these new laws will not bring any tangible benefits to police investigations.

Finnish MEP Alexander Stubb came to a similar conclusion: 'I think we are chasing the wrong crooks, because if you are a crook who does not have the brains to use hotmail or prepaid mobile phone networks, then you are a stupid crook and we are really [only] chasing the stupid crooks.'

One clear benefit from the new legislation seems to be increased harmonisation of data retention rules across the EU. At the moment, up to 15 member states do not have any such legislation whatsoever. The UK, for example, has had only a voluntary code until now. Harmonising data retention would at least ensure that police investigators could be certain to find the necessary information, no matter where the criminal was located at the time.

However, while all EU members will now have some form of data retention, the harmonisation has been kept at a very basic level. It is thus up to member states to decide which serious crimes will be covered by the directive, and unsuccessful calls will only retained where these records are already available. Moreover, each country will also choose independently whether to reimburse operators or not for the additional costs incurred by the legislation.

The issue of the precise period that data will be stored is particularly controversial. The directive gives individual countries the freedom to choose any length of time between six months and two years. However, Professor Steve Peers points out in a report for the civil rights group Statewatch that both the text of the directive itself and the general principles of the European internal market weaken the apparent constraints on member states' ability to store data. Thus, Article 11a of the directive allows member states to extend the retention period if they are 'facing particular circumstances', as long as this does not distort the internal market. As the directive is governed by internal market legislation, the existing Article 95 EC lets member states 'maintain national provisions on grounds of major needs', which include public security. Poland has already announced it will try to retain data for a period of fifteen years.

The result of this legislation, then, is partial rather than complete harmonisation. The narrowing of differences in national practices in data retention seems likely to be much smaller than it could have been with a directive that allowed for less flexibility. In addition, these differences could lead to competitive disadvantages for telecommunications companies based in countries with a long retention period and no state reimbursement of costs.

Overall, it is far from clear that the data retention directive will be of significant practical use, while harmonisation will only take place to a very limited extent. The benefits of this legislation, then, are limited, but what are the costs involved?

Paying the Bill

Two issues are central to the debate on the costs that will arise as a result of this directive. First, how much will data retention cost? Second, who will pay for it?

Implementing this new directive will impose costs on telecommunications

companies. However, at the moment there is little clarity on how this directive will be transposed into national law, so estimates on costs vary considerably. According the UK Internet Service Providers' Association, it has been estimated that the data retention envisaged in the directive would cost a large ISP around £35 million a year, while Carl Mühlner, the head of Tiscali Germany, said that operating costs for his large ISP could increase by several million euros a year. European communications service providers have stated simply that the new rules would be 'hugely expensive', arguing that the EU should have carried out a cost-benefit analysis of the new measures.

Perhaps unsurprisingly, the providers have lobbied for state reimbursement of the costs of data retention. Indeed, the relevant EP committee argued that EU governments and not telecommunications companies should pay for the new rules. This decision was, however, overturned by the Council with the support from the EP leaders of the Party of European Socialists (PES) and the European People's Party (EPP). Germany has already announced that it will make companies pay for data retention, while Charles Clarke has said he would consult with industry representatives.

As the extent of the directive was reduced in the legislative process – with requirements for unsuccessful calls and internet data watered down – the costs incurred will be far lower than initially feared by telecommunications companies. Nevertheless, there is currently a great deal of uncertainty about how much the implementation of this new directive will cost and to what extent some countries' providers will be put at a competitive disadvantage if their government declines to fund reimbursement. It is far from clear that the financial consequences of the legislation were clearly considered by its proposers or those who adopted it.

Personal Liberty

Beyond the balance of practical benefits and monetary costs, the data retention directive has faced opposition from civil rights groups across Europe. They fear that the new arrangements will increase surveillance to an unacceptable level while giving citizens no power to find out what the data gathered has been used for. They also point out that the EU's law goes far beyond rules in other countries such as the United States.

In response to the directive, Statewatch has declared that 'mandatory data retention will place all the communications of everyone under surveillance'. All communications via telephones and the internet will be noted and can be accessed by police. The legislation is unusually far-reaching, in that it stores all data, no matter whether it is required or not. Every user's right to privacy is interfered with, but with benefits that are as yet uncertain.

This interferes with established principles of human rights. The report of Article 29 Working Party notes: 'Freedom and confidentiality of correspondence and all other forms of communication are among the pillars of modern democratic societies...Traffic data retention interferes with the fundamental right to confidential communications guaranteed to the individuals by Article 8 of the European Convention on Human Rights.' The interference with this Article is only justified if it is necessary for national security, but needs to be 'based on a pressing need, should only be allowed in exceptional cases and be the subject of adequate safeguards'.

Some protection has been built into the directive. Access to data will not be entirely up to law enforcement agencies, as they will have to request information on a case-by-case basis and will not obtain the entire database. Moreover, each country will have to set up an independent authority that will monitor the correct use of retained data. Nevertheless, there is significant concern that law enforcement agencies will not be accountable enough in their use of retained data. Statewatch thus argues that a wide range of civil society groups are certain that the powers given by the directive 'will, on occasion, be misused and abused'. Two specific causes for concern cited by Statewatch are, first, the fact that citizens cannot find out how data on them has been used, except if they have been charged, and second, that information can be shared among all 25 member states because of the 'principle of availability'.

Echoing the concerns of civil rights groups, the Article 29 Working Party and the European Data Protection Supervisor called for a one-year limit on data retention, as there is no evidence that further storage will bring any benefits that can compensate for the invasion of citizens' privacy. As noted above, Professor Peers has pointed out that even the two-year limit included in the directive is by no means watertight. This stands in clear contrast to the recommendation of the Article 29 Working Party that the retention period to be 'as short as possible' in order to reduce the interference of the directive with the right to privacy.

The legislation goes further than equivalent laws in the United States. A report by the civil liberties group Privacy International shows how EU anti-terrorism legislation has been much tougher than the US's efforts. In the US, there is no equivalent to the directive on data retention. The report of the EP's industry committee stated in November 2005 that no other democratic country has such far-reaching laws concerning data retention.

Storing phone numbers, basic information on e-mails and internet addresses may at first seem like a small incursion into citizens' human rights. However, they do represent a significant incursion into each individual's private sphere, while the directive goes further than necessary and the openness and accountability of state authorities remain limited.

Democratic Scrutiny

Most worrying, however, is the way in which this directive came into being. Democratic oversight over the process was insufficient, with EU governments forcing a speedy agreement on a controversial matter. The EP committees were largely cut out of the search for a compromise, and most changes proposed by them were weakened significantly in the final agreement. Moreover, outside observers were not given the possibility to scrutinise the proposals in detail before they were passed.

The final compromise on the content of the directive was reached by the leaders of the PES and the EPP in consultation with the Council of Ministers. The text was agreed at the Justice and Home Affairs Council on 2 December 2005. In the Parliamentary vote on 14 December, 378 MEPs, mainly from the EPP and the PES, were in favour of the directive, with 197 votes against. Unusually, this majority was sufficient to ensure that the directive was passed by the European Parliament at first reading. The Parliament was clearly acting under significant pressure from the Council, and in particular from the UK Presidency to reach a decision before the end of 2005.

The compromise discarded most of the proposed amendments made by the EP's civil liberties committee. Thus, the committee's report, adopted with 33 to 8

votes in favour with 5 abstentions, had argued for state reimbursement of costs and a retention period of only up to 12 months. The proposal had also included increased privacy protection and would have prevented future expansions of the data retention period upon request. While the final proposal did make some concessions to the committee's concerns, the EP as a whole fell far short of being an efficient protector of civil liberties in the face of pressure from EU governments. After the vote, Alexander Nuno Alvaro MEP, the author of the civil liberties committee's report, summed up the situation in these words: 'By voting as we did today, we create a precedent where Council need only say 'jump' and Parliament cries "how high?"'

Indeed, it is a pity that the EP did not manage to play a stronger part in the process. After all, it had fought hard to have a say in the formulation of the directive, persuading the Council to pass the law under the co-decision rather than the consultation procedure. However, pressure from member state governments to adopt the directive quickly led the EP Group leadership of the EPP and the PES to forge a compromise with the Council that can only be seen as unsatisfactory. Thus, the proper co-decision process that the EP had fought for was discarded in favour of a more secretive process. The sudden urgency on the part of member states came as a surprise to Statewatch, who pointed out that the first steps towards data retention were taken in late 2001. If the legislation was indeed urgent, why did it take so long to come to fruition?

It was not only the bulk of the EP that was effectively excluded from the latter stages of the legislative process. As the directive was negotiated so quickly by a small number of participants, civil rights groups, industry representatives and national parliaments had no chance to find out what would be decided. As we have seen, the final directive ignored wide-ranging criticism from a coalition of interest groups and non-governmental organisations without a significant attempt to address publicly the perceived shortcomings of the law.

Conclusion

In the EP debate on the directive, Edith Mastenbroek MEP gave a succinct summary of the data retention directive: 'It is indisputable that this directive is intrusive. It is questionable whether it will help. On the internet side, it is even technically unfeasible.' The benefits of this new legislation are indeed uncertain, especially as far as retention of internet data is concerned. Even harmonisation, one of the main goals of the legislation, is partial rather than complete.

The costs, most of which will have to be shouldered by telecommunications companies, may well be considerable, but at the very least law-makers cannot have been sure of the size of the burden they would be imposing on communications providers. On a practical level, then, the directive is of uncertain benefit and unclear cost.

Civil liberties will be interfered with by this directive, as most telephonic and internet communication will now be monitored. Such interference can of course be justified for reasons of national security, but it is not clear that the legislation will be effective, while its provisions are more sweeping than is necessary. This directive thus exemplifies the general pattern of EU governments consistently pursuing restrictive anti-terrorist legislation at the European level.

Finally, democratic oversight over the law-making process was, in this case, highly limited, as the role of the EP and especially of its committees in scrutinising legislation was not respected. The amendments suggested by the committee report would have changed several aspects of the law criticised by both industry and human rights groups while ensuring more complete harmonisation. There is no reason why data retention would have been less effective under the suggestions made by the EP committees, while civil liberties and industry interests would have been better respected. In addition, interest groups and civil rights organisations were not given enough opportunity to make their concerns heard effectively.

If the EP had insisted on playing its full normal role in the legislative process, the resulting directive would thus not only have satisfied principles of democratic oversight, it would also have been of better quality. However, pressure from member state governments led the leaders of the large parties in the EP to force a consensus that undid much of the improvements made to the directive made at the committee stage. The data retention directive has shown that the EP, if it is prepared to insist on its independence, can be an important actor in justice and home affairs at the European level and play a vital role in securing democratic scrutiny and protecting civil liberties. But the lesson for the Parliament to draw from recent events is that this independence must be fought for and cannot be taken for granted.

Markus Wagner
The Federal Trust

Sources

Civil Liberties Committee Report, Rapporteur: Alexander Nuno Alvaro MEP, 28 November 2005, available at: http://www.statewatch.org/news/2005/nov/ep-dat-ret-rep-28-11-05.pdf

European Parliament Debate, 13 December 2005, available at: http://www.europarl.eu.int/omk/sipade3?PUBREF=-//EP//TEXT+PV+20051213+ITEM-012+DOC+XML+V0//EN&L=EN&LEVEL=1&NAV=S&LSTDOC=Y&LSTDOC=N

Justice and Home Affairs Council Conclusions, 2 December 2005, available at: http://www.fco.gov.uk/Files/kfile/JHA_Conclusions_1-2Dec.pdf

Article 29 Working Party Opinion, 21 October 2005, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf

Gus Hosein, 'Threatening the Open Society: Comparing Anti-terror Policies and Strategies in the U.S. and Europe', Privacy International Report, 13 December 2005, available at: http://www.privacyinternational.org/issues/terrorism/rpt/comparativeterrorreportdec2005.pdf

Statewatch's Observatory of the Surveillance of Telecommunications in the EU, http://www.statewatch.org/eu-data-retention.htm

Steve Peers, 'The European Parliament and data retention: Chronicle of a 'sell-out' foretold?, Statewatch Analysis, December 2005, available at: http://www.statewatch.org/news/2005/dec/sp_dataret_dec05.pdf

European Competitive Telecommunications Association, press release, 7 December 2005, available at: http://www.ectaportal.com/en/upload/File/Press%20Releases/Dataretention071205.pdf

European Confederation of Police, press release, 2 June 2005, available at: http://www.eurocop-police.org/pressreleases/2005/05-06-02%20PRESS%20JHA%20Council_E.pdf

Wendy Grossman, 'Will logging your e-mail combat terrorism in Europe', *The Guardian*, 12 January 2005, available at: http://technology.guardian.co.uk/weekly/story/0,16376,1683944,00.html

Kevin J. O'Brien, 'Data law passed in EU seen as restrictive', *International Herald Tribune*, 15 December 2005, available at: http://www.iht.com/bin/print_ipub.php?file=/articles/2005/12/14/business/data.php