Transposition of Directive 2006/24/EC

Response of the Open Rights Group

Detail of Respondents

Prepared by:	Becky Hogge
Responding on behalf of:	The Open Rights Group
Address:	Open Rights Group 7th Floor 100 Grays Inn Road London WC1X 8TY United Kingdom
Telephone:	+44 (0)20 7096 1079
Email:	info@openrightsgroup.org
Website:	http://www.openrightsgroup.org

The Data Retention Directive is a bad piece of law. We take this opportunity to voice our concerns over the final transposition of this law onto UK statue books in terms of its questionable relationship with basic human rights (focussing, for now, on the period of retention specified in the draft SI), and the uncertainty it will bring into UK law. We note that other EU Member States, such as Austria, have so far refused to implement this directive, and we urge the Home Office to do the same.

Human Rights

The period of retention specified by the statute will be vital in determining if the regulations are proportional and necessary, thus meeting Data Protection and Human Rights criteria for legality. We note that the period of retention the Home Office has chosen to specify is 12 months. This is double the statutory minimum imposed by the Directive. We believe that the case has not been made for this retention period, and that, as such, the UK's proposed transposition of this directive may not pass the proportionality test.

There is a lack of empirical evidence around the age of communications data generally required by law enforcement agencies in the course of their investigations. Although the Government have conducted a number of studies in this area, they do not tend to separate communications data requested from ISPs to data requested from other communications service providers such as telephone companies. We read with interest para 5.5 of the Home Office consultation document:

> "A two week survey of communications data obtained by the police in the UK was conducted by the Association of Chief Police Officers (ACPO) Data Communications Group in May 2005. During the survey, there were 231 requests for data relating to communications that had taken place between 6 and 12 months earlier. 60% of these requests were in support of murder and terrorism investigations

> and 26% of the requests were in support of other forms of serious crime including armed robbery and firearms offences"

We suggest that if ACPO wish to meaningfully contribute to the evidence base on data retention in the public domain, it would be helpful to indicate what percentage of total requests for data these 231 requests represent.

We further note that we have received anecdotal evidence from Communications Service Providers signed up to the Home Office Voluntary Code of Practice on Data Retention[1] that police tended to request older data not because of long-running serious terror/crime investigations, but because police did not get around to asking for the data until some time had elapsed. We suggest that increasing police resources so that they were able to make consistently timely requests would be preferable to specifying an over-long and unproven retention period, and could even constitute an alternative method that brought less Human Rights implications.

We do not believe that it is proportionate to invade individuals' privacy to the extent of retaining their communications data in order to investigate minor infractions of the law. We suggest that the Directive, if transposed at all, is transposed with a savings provision that data compulsorily retained for national security purposes may only be accessed under RIPA for such purposes, by the intelligence and law enforcement agencies, and not, for example, by local authorities pursuing more minor infractions of the law. We note that in 2007 1,707 requests were made by local authorities using RIPA powers for communications data retained under the Voluntary Code. We do not wish to see that figure increase[2].

Rule of Law

We note reports that Government has told Internet Service Providers (ISPs) that if they are not notified by the Home Office that they need to retain, they need not comply with the proposed statute[3]. We understand that the reason for this confusing situation is a lack of government funds available to help all all ISPs comply, since the UK government (unlike most EU Member States), has undertaken to reimburse ISPs for costs of initial retention, storage, and, more significantly, later retrieval.

In all likelihood, the Home Office will only ask larger ISPs who are already complying with the Home Office's Voluntary Code to put retention apparatus in place. We understand that small ISPs who buy bandwidth wholesale from BT will be excluded to avoid paying for so-called "double retention". This situation presents a serious problem of legal uncertainty, especially for small to medium (SME) ISPs wishing to accept that such Home Office statements provide adequate protection for not actually fulfilling the demands of law.

SME ISPs could take comfort from the fact that retained data would only be requested under Regulation of Investigatory Powers Act (RIPA) powers. The logic goes that since only government departments can require retained data to be handed over, it is unlikely that Government will bring suit against an SME ISP they have advised to ignore the law. Further, any suit from the Commission over poor transposition will be directed at Government and not at small ISPs.

1 See http://www.opsi.gov.uk/si/si2003/draft/5b.pdf
2 http://www.official-documents.gov.uk/document/hc0708/hc09/0947/0947.pdf
3 See http://www.theregister.co.uk/2008/10/13/home_office_eudrd/

Nonetheless, this situation is far from clear, given uncertainties raised by the recent European Court of Justice (ECJ) decision on *Promiscae vs Telefonica*[4] over whether retained data should be accessible to those initiating civil proceedings, for example in cases related to the civil infringement of intellectual property. If data is, by law, is supposed to be retained by all ISPs, rightsholders might seek disclosure of that data in civil proceedings using a Norwich Pharmacal order. If that data is not being retained by, say, an SME ISP who has received assurances from the Home Office that they are safe to ignore this new law, damages might still be awarded by the court since the civil litigant has possibly suffered loss as a result of failure to retain. Although we accept that issues of title may come into play here (as not every ordinary member of public can enforce duties imposed by public statutes) we do not find these issues reassuring enough to dismiss this potential threat to SME ISPs, and to the Home Office's plan to control costs.

To avoid this outcome we would suggest that the Directive, if it is transposed at all, is transposed with a saving provision that data retained is only to be disclosed using RIPA powers and not to be made available in ordinary civil litigation. In this instance, statute should trump common law.

All this not withstanding, we observe that it is a bad idea in terms of rule of law for an Executive to unilaterally and without clear statutory discretion announce that the law will be enforced in respect of some ISPs and not others.

We further note uncertainties around what other communications service providers might fall under the jurisdiction of the transposed Directive exist in respect of shifting definitions around so-called “Public Electronic Communications Services” thanks to ongoing Telecoms Package negotiations such as those surrounding the Electronic Communications Privacy Directive. Some currently excluded networks, such as University networks and internet cafés, are currently being re-examined as they may not be in scope for certain privacy protections. Amendments have been tabled that try to add a definition of a "publicly available private network". While the concerns about privacy may be well-motivated the risk is that this they will redraw the boundaries to include a broader range of access networks, and that this broader definition could be adopted for other pieces of legislation like data retention.

Function Creep

This issue of announcing that the law will be enforced in respect of some ISPs and not others is also a matter of practicality – if the aim of the law is to be able to interrogate the communications activity of terrorists and serous criminals, then surely the Government understands that such people will take advantage of the informal exemptions the Executive is granting and migrate their communications activity to SME ISPs?

Not only is it the case that malevolent communications services users are likely to take advantage of the ad hoc exemptions being proffered to SME ISPs by the Executive, they are also likely to take advantage of communications services and mediums not covered by the Directive. The

4 See http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en&newform=newform&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&alldocrec=alldocrec&docj=docj&docor=docor&docop=docop&docav=docav&docsom=docsom&docinf=docinf&alldocnorec=alldocnorec&docnoj=docnoj&docnoor=docnoor&typeord=ALLTYP&allcommjo=allcommjo&affint=affint&affclose=affclose&numaff=&ddatefs=&mdatefs=&ydatefs=&ddatefe=&mdatefe=&ydatefe=&nomusuel=Promusicae&domaine=&mots=&resmax=100&Submit=Submit

Government has to a certain extent recognised this. At the beginning of October, Home Secretary Jacqui Smith delivered a speech to ippr where she stated that:

> "The challenge is the changing technology and the way it is possible to collect communication data."

It is clear to us that the Data Retention Directive signals the beginning, and not the end of this Government's desire to access communications data. Given the issues surrounding this Directive's relationship to the basic human right to privacy, we note that any further extension of surveillance and monitoring powers of state authorities, at least in the context of blanket retention (and even blanket access) are highly questionable.

Costs estimated, for implementing a centralised government-controlled store of communications traffic data rumoured to be part of the Home Office's Intercept Modernisation Programme have been put by insiders at around £12 billion[5]. We direct the Home Office to recent research published in the US by the National Academy of Sciences that makes clear that pattern-seeking data-mining methods are of limited usefulness[6], and question whether, especially in this time of economic crisis, a new multi-billion pound IT project is the most cost-efficient way to combat the terrorist threat.

About the Open Rights Group

The Open Rights Group is a grassroots digital rights advocacy group based in the UK. It aims to increase awareness of digital rights issues, help foster grassroots activity and preserve civil liberties in the digital age. It is funded by individual donations and small grants.

5 See http://www.theregister.co.uk/2008/10/07/detica_interception_modernisation/

6 See http://www.nap.edu/catalog.php?record_id=12452