27 YEARS
1987-2014

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The dead Directive: What next for data retention in the UK?

Theoretically, the e-Privacy Directive could provide a legal basis for data retention law. But the position is far from clear in the UK, say **Mark Young** and **Philippe Bradley**.

On 8 April 2014, the Court of Justice of the European Union ("CJEU") ruled that the Data Retention Directive 2006/24/EC (the "Directive") was unlawful and invalid, on human rights grounds.[1] The invalidation of a Directive is an unusual event, which has led to questions about the impact of the decision at national level. In the midst of this ambiguity, some Internet service providers have already ceased to comply with national laws that implement the annulled Directive, leading to disputes with authorities.

This article summarises the Directive, analyses the CJEU's decision in the *Digital Rights Ireland* case, and discusses the likely implications under national law, with a focus on the UK. It concludes that the current legal basis for data retention across the EU and in the UK is now weak, but that if challenged, the UK government may find alternate legal means to mandate retention, at least until an EU-level replacement is agreed.

Recap on the Data Retention Directive

The Directive required Member States to ensure that communications

Continued on p.3

Issue 73 **May 2014**

UNITED KINGDOM
report

ISSUE NO 73 **MAY 2014**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

LEGAL EDITOR
Valerie Taylor
valerie.taylor@privacylaws.com

SUB EDITOR
Tom Cooper

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Mark Young
Covington & Burling LLP

Philippe Bradley
Covington & Burling LLP

Alison Deighton
TLT solicitors

Peter Gooch
Deloitte

Dugie Standeford
PL&B Correspondent

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Unsettled time for EU privacy

As the Data Retention Directive has been scrapped, one has to ask whether it was doomed to failure because of the Directive's text, or the controversial national implementation which has been debated in several constitutional courts in the EU. In the UK, the government wants to retain a huge amount of data to fight terrorism. However, in its decision to invalidate the Directive, the Court of Justice of the European Union stated that there was no differentiation between different types of communications data, and the overwhelming majority of the data that was to be retained was not relevant to criminal investigations or prosecutions. Read an analysis of this unusual decision on p.1.

Anonymisation is clouded in uncertainty. Privacy experts do not seem quite satisfied that data can be completely anomymised. Read the guidance of the EU Art. 29 DP Working Party, and UK experts, on p.18. An area that is perhaps easier to manage with careful planning and auditing is managing third parties. Read useful tips and insights on p.10.

Consumers are becoming more privacy savvy; a recent study indicates that 85% of people are happy to share information if they know it is used only by the first party (p.9). But the online environment changes fast, and even privacy lawyers have to run hard to keep up with new developments, such as custom audiences marketing. See p.6.

Our Legal Editor reports on a Court of Appeal decision which states that the Criminal Records Bureau disclosure system is contrary to Article 8 of the European Convention on Human Rights (p.14). The newly appointed Surveillance Camera Commissioner is keen to work with the ICO to ensure that their codes of practice can be integrated to avoid confusion, particularly as 95% of CCTV cameras are outside the scope of the police and local authorities and the norms of democratic accountability (p.13).

PL&B's 27th Annual International Conference, *New Horizons ~ New Risks*, 30 June to 2 July, will feature presentations by both Simon Hughes MP, Justice Minister, and Christopher Graham, Information Commissioner and two members of his staff. See www.privacylaws.com/programme

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Data Retention... from p.1

service providers ("CSPs"), i.e., primarily companies providing telephone and Internet connectivity, retain certain data necessary to identify subscribers or users in relation to every communication carried ("metadata") — although not the content of communications. The Directive required data to be retained for the purpose of investigating, detecting and prosecuting "serious crime", as defined by national law. This requirement was an exception to EU data protection laws, particularly Directive 2002/58/EC (the "e-Privacy Directive"), which required CSPs to erase or anonymise such metadata as soon as it was no longer useful for billing purposes.

National implementations of the Directive varied significantly.[2] Member States were given wide discretion to mandate retention for anywhere between six and 24 months. Definitions of "serious crime" also varied between countries; several Member States expanded the scope of retention to include the prevention of crime in general, the protection of public security, and/or the preservation of state security.[3] Access safeguards, which the Directive did not set out, were also not uniform; only 14 Member States required judicial authorisation of requests, six countries authorised tax and/or customs authorities to access the metadata, and the UK permitted access by other public authorities.[4]

All of these issues added to resistance to the law that had been present from the outset. By 2010, the European Data Protection Supervisor was openly referring to the Directive as "*without doubt the most privacy invasive instrument ever adopted by the EU*".[5] The European Commission took action against several countries for missing the national implementation deadline, including Austria, Belgium, Germany, Greece, Ireland, Romania and Sweden. Both Sweden and Germany eventually faced fines for their continued failure to comply. National implementing laws faced significant legal challenges in their national courts, which suspended or annulled national implementations of the Directive in Bulgaria, Cyprus, the Czech Republic, Germany, and Romania. Ultimately, two such national challenges, in Ireland and Austria, were referred to the CJEU, where they succeeded in securing the invalidation of the Directive.

The ruling of the Court in Digital Rights Ireland

Which fundamental rights were engaged?: In *Digital Rights Ireland*, the CJEU held that the Directive violated Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the "Charter"), which protect the right to respect for private life and to protection of personal data. The CJEU noted that retaining metadata interferes with the right to private life as it permits very precise conclusions to be drawn about individuals' private lives, including about their daily habits, movements and social relationships (regardless of whether or not that individual is inconvenienced by the retention). The Court also found that access to the retained data by authorities was an additional interference with Article 7, and that storing or accessing metadata constitutes processing of personal data, thus engaging Article 8.

Prompted by the Austrian referring court, the CJEU also stated that it was "not inconceivable" that indiscriminate data retention might also have a chilling effect on free speech (a right protected under Article 11 of the Charter), but did not find it necessary to explore the point.

Lawfulness of the interference with fundamental rights under the Charter: Applying the test of "strict necessity", the CJEU ruled that there were three key flaws that meant that the Directive constituted a disproportionate interference with fundamental rights.

First, data from all subscribers and registered users was retained without limitation, differentiation or exception, entailing "*an interference with the fundamental rights of practically the entire European population*".

Second, procedural protections were lacking, so access was not restricted to what was strictly necessary; for example, access did not require prior review by a court or independent administrative body.

Third, the data must be retained for at least six months, without any distinction being made as to its type or utility; there should have been objective criteria to ensure that retention times were limited to what is strictly necessary.

The CJEU added two potentially far-reaching objections in relation to the protection of personal data under the Charter. It criticised the latitude given by the Directive to take into account economic factors when deciding on the level of security that a CSP should provide. Further, the Court suggested that Article 8 requires that data remain under the control of EU data protection authorities, deeming this to be an "essential component of the protection of individuals". Academics have suggested that this view may be "particularly explosive", as it seems to suggest that data should not be permitted to leave the EU.[6] This would be an extreme position, analogous to one that was recently explored, but rejected, by Brazilian legislators.[7]

Outcome for Telecoms and Internet Service Providers

Impact on national laws: The CJEU declined to suspend the effects of its invalidation of the Directive until an improved version of the law was passed, ignoring the previous suggestion of Advocate General Cruz Villalón. The ruling thus voided the Directive *ab initio* - i.e., the Directive does not and has never represented a valid law.

Theoretically, in the Directive's absence, the e-Privacy Directive would have had primacy. Article 15(1) of the e-Privacy Directive allows Member States to introduce data retention laws, but "*subject to the general principles of Community law*" and only if they are "*a necessary, appropriate and proportionate measure within a democratic society*".

This would suggest that any national law that is not consistent with these limited grounds has therefore been, and continues to be, unlawful under EU law, in which case national courts would have to refuse to enforce it.[8]

It would be tempting to assume that the CJEU's analysis in *Digital Rights Ireland* also applies to national data retention laws that now have to rely on the e-Privacy Directive for their legal basis. Yet it is unclear whether that is

the case. Commentators have disputed whether the Charter applies to those laws, as those laws are, in principle, a voluntary measure by Member States, not an EU obligation.[9]

Despite the ambiguity, shortly after the CJEU's ruling, some Swedish Internet service providers announced that they would cease complying with Sweden's national implementation of the Directive. Sweden's regulator admitted that it would have difficulty enforcing the national law and would not seek to do so.[10] Companies in other countries may look to follow the Swedish example, although caution is advised: their prospect of success might depend on both local law and politics. Indeed, some regulators in the EU have said that they will stand by their national data retention laws.[11]

The position is even less clear regarding the UK implementing law. The Data Retention (EC Directive) Regulations 2009[12] were passed into UK law as secondary legislation pursuant to section 2(2) of the European Communities Act 1972, which allows government ministers to introduce laws in order to implement EU Directives. If, in the eyes of the law, there is no Directive to implement, the UK law is arguably *ultra vires*. This appears to accord with the view of several legal academics[13] and to be in line with a ruling of Lord Hoffmann in the *Imperial Tobacco* case before the UK House of Lords, in which he stated that "*s 2(2) of the [European Communities] Act makes the validity of the regulations dependent upon the existence of a Community obligation*" (such as a Directive).[14]

Compensation: A further interesting question arises from the judgment: if the Directive never "existed", and national data retention laws are now unlawful under the e-Privacy Directive, are affected companies and individuals entitled to sue the State for financial compensation?

The established principle of *Francovich* liability entitles persons harmed by a Member State's improper implementation of EU law to claim damages, under certain conditions.[15] Under established case law, such compensation may not be payable if the breach of Community law by the Member State is excusable. Factors include the clarity and precision of the rule breached, whether the infringement and the damage caused was unintentional or involuntary, and whether the position taken by a Community institution may have contributed to the breach.[16] It seems likely that Member States would be able to argue that their technical breach of Community law prior to the Directive's annulment was excusable.

What may be harder to excuse, however, are damages accruing after a clear CJEU ruling that retention of metadata that is not strictly necessary for law enforcement purposes is unlawful. The national cases in Ireland and Austria will now resume, and these will provide an early glimpse of how national courts apply the CJEU's ruling. Even though financial compensation is being sought in the Irish case, the applicant is suing from the perspective of a service user whose data was unlawfully retained; different

REFERENCES

1 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*; available at http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=en
2 See European Commission, 'Proposal for a review of the Directive 2006/24/EC (Data Retention)', July 2001, available at http://ec.europa.eu/smart-regulation/impact/planned_ia/docs/2011_home_006_data_retention_2012_en.pdf
3 See European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', p.6
4 See European Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', p.6 ; and www.statewatch.org/news/2013/dec/secile-data-retention-directive-in-europe-a-case-study.pdf, pp 17-18
5 See Speech by Peter Hustinx, European Data Protection Supervisor 'The moment of truth for the Data Retention Directive', Brussels, 3 December 2010, available at www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf
6 See Daithi Mac Sithigh and Judith Rauhofer 'The Data Retention Directive Never Existed' (2014) SCRIPT-ed 11(1) 118-127; available at http://script-ed.org/?p=1480
7 See Philippe Bradley, Dan Cooper, 'Brazil Enacts "Marco Civil" Internet Civil Rights Bill', 28 April 2014, available at www.insideprivacy.com/international/brazil-enacts-marco-civil-internet-civil-rights-bill/
8 Case C-184/89 *Helga Nimz v Freie und Hansestadt Hamburg*, § 19, and Case 106/77 Amministrazione delle Finanze dello Stato v Simmenthal [1978] ECR 629
9 Steve Peers, 'Are national data retention laws within the scope of the Charter?', available at http://eulawanalysis.blogspot.co.uk/2014/04/are-national-data-retention-laws-within.html
10 Liam Tung, 'Four of Sweden's telcos stop storing customer data after EU retention directive overthrown', available at www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/
11 Jabeen Bhatti et al, 'EU Member State Privacy Regulators Ponder Response to End of Data Retention Directive', 28 April 2014, available at http://www.bna.com/eu-member-state-n17179889937/
12 The Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859), available at http://www.legislation.gov.uk/uksi/2009/859/contents/made
13 See for example T.A.J.A. Vandamme, "The invalid directive: the legal authority of a union act requiring domestic law making", University of Amsterdam Faculty of Law, 2005, p. 252, available at http://dare.uva.nl/document/102647
14 *R v Secretary of State for Health and others*, *ex parte Imperial Tobacco Ltd and others* - [2001] 1 All ER 850; available at www.publications.parliament.uk/pa/ld200001/ldjudgmt/jd001207/tobacc-2.htm
15 Joined Cases C-6/90 and C-9/90 *Francovich and Bonifaci v Italy* [1991] ECR I-5357, [1992] IRLR 84, ECJ
16 Joined cases C-46/93 and C-48/93 *Brasserie du Pêcheur SA v Germany, R v Secretary of State for Transport, ex p Factortame Ltd* [1996] All ER (EC) 301
17 Council of Europe Convention on Cybercrime; available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
18 *Big Brother Watch and Others v. the United Kingdom* (App. No. 58170/13)
19 Jabeen Bhatti *et al, supra n*. 11

considerations will apply in respect of CSPs forced to take measures that were costly and unlawful. CSPs may have to await the outcome of alternative test cases before their ability to recover damages is clarified.

Likely reforms

Many Member States are likely to wait for discussions at EU level about introducing a new law to replace the Data Retention Directive before they instigate national reforms. The CJEU has provided relatively detailed guidance on what such a new law should look like, but it remains to be seen if and how that will be implemented. We may, for instance, see a renewed interest in "quick freeze" data preservation, as found in the Council of Europe's Convention on Cybercrime.[17] However, given the impending European Parliamentary elections and subsequent Commission reshuffle, the ongoing reform of the general EU data protection framework, and a pending case before the European Court of Human Rights concerning the mass collection of communications metadata by Western intelligence agencies,[18] the wait could be lengthy.

It is possible that some other countries, such as the UK, may instead rush to unilaterally shore up their national laws; the UK Home Office has come out strongly in support of data retention, despite the CJEU's ruling.[19] If the UK's implementation of the Directive proves unreliable, the UK government may try to fall back on older laws such as Part 11 of the Anti-Terrorism, Crime and Security Act 2001 or the Telecommunications Act 1984 (particularly section 94). Alternatively, it might press forward with plans for a Communications Data Bill that mandates even broader data retention. Given the political climate engendered by Edward Snowden's disclosures and this ruling, the latter may be particularly difficult to achieve.

AUTHORS

Mark Young, Special Counsel and Philippe Bradley, Trainee, Covington & Burling LLP. Mark Young, previously an Associate in Covington's London IP and Data Protection team, was promoted to Special Counsel in April.
Emails: myoung@cov.com
pbradley@cov.com

Your Subscription **includes**

1. Six Reports a year
The *Privacy Laws & Business (PL&B) United Kingdom Report* ranges beyond the Data Protection Act to include the Freedom of Information Act, related aspects of the Human Rights Act and the Regulation of Investigatory Powers Act. It also covers Jersey, Guernsey and the Isle of Man. It complements the *Privacy Laws & Business International Report*, which has been the leading data protection and privacy publication for 27 years.

2. Online search function
Subscribers can conduct detailed research by key words on the *Privacy Laws & Business* website to access: back issues since 2000 for the UK Report; special reports on specific subjects, such as Big Data; and materials from *PL&B* events, slides, videos and audio recordings.

3. Regular e-news
Subscribers receive updates about relevant news as and when it happens.

4. Helpline Enquiry Service
Subscribers can request information about the current status of legislation and other information.

5. Index
An index is at www.privacylaws.com/Publications/report_index/

Electronic Option
The electronic PDF format enables you to: receive the Report as soon as it is published; click-through from email and web addresses in the document; and follow links from the contents page to articles.

Subscription Discounts
Discounts for 2-4 users or 5-25 users and 2 years (10%) or 3 years (15%). See www.privacylaws.com/subscribe

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists; and 10 of the Global Top 20 in the* Fortune *list.*

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

Single User Access

❑ *PL&B UK* Report Subscription **£400**

❑ *UK/International* Reports Combined Subscription **£800**

Subscription Discounts

Discounts for 2-4 users or 5-25 users

Number of years: 2 (10% discount) or 3 (15%)

Go to www.privacylaws.com/subscribe

Special academic rate – 50% discount on above prices – contact the *PL&B* office

Subscription Includes:

Six reports a year, on-line access to back issues, special reports, and event documentation.

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: info@privacylaws.com 9/05

www.privacylaws.com

Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.